M2 Series Switches

SONiC_1.3.6 Command Reference

Applicable products: M2-W6510-32C, M2-W6510-48GT4V, M2-W6510-48V8C, M2-W6520-24DC8QC, M2-W6910-64C, M2-W6920-4S, M2-W6920-32QC2X, M2-W6930-64QC

There may be descriptions available for other products provided only for reference purposes.

Document version: V1.0
Date: March 12, 2024

Copyright

Disclaimer

The purchased products, services, and features are stipulated by the contract made between Micas Networks and the customers. All or part of the products, services, and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees, or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Micas Networks reserves the rights to change the content without any notice or warning.

This document is used only for reference. Micas Networks endeavors to ensure that the content in this document is accurate and reliable, but cannot ensure that no error or omission exists. All information in this document does not constitute any expressed or implied warranty.

Micas

Website: https://www.micasnetworks.com/

Customer service email: support@micasnetworks.com

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Technical Support

Official Website: https://www.micasnetworks.com/support/

Conventions

Convention	Description
Bold font	Commands, command options, and keywords are in **bold** font.
Italic font	Arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
&<1-n>	The argument before the sign (&) can be input for consecutive 1- n times.
//	Double slashes at the beginning of a line of code indicate a comment line.

Signs

The signs used in this document are described as follows:

Warning

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

Caution

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

Note

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

Specification

An alert that contains a description of product or version support.

Note

- The port type involved in this manual may be different from the actual situation. Please proceed with configuration according to the port type supported by the product.
- The display information involved in this manual may contain the content of other products (such as model and description). Please refer to the actual display information.
- The routers and router product icons involved in this manual represent common routers and Layer 3 switches capable of routing protocols.

M2 Series Switches SONiC_1.3.6

Command Reference

---

18. VRF Commands
19. ACL Commands
20. QoS Commands
21. IGMP Snooping Commands
22. AAA Commands
23. RADIUS Commands
24. TACACS Commands
25. RSTP Commands
26. SSH Commands
27. CoPP Commands
28. M-LAG Commands
29. VRRP Commands
30. BFD Commands
31. ECMP Commands
32. Mirroring Commands
33. sFlow Commands
34. NTP Commands
35. FTP Server Commands
36. FTP Client Commands
37. SNMP Commands
38. RESTCONF Commands
39. Telemetry Commands
40. VXLAN Commands
41. Vnet Commands
42. RDMA Commands

43. Troubleshooting Commands
44. System State Commands
45. Static routing Commands
46. Console Commands
47. Drop Counters Commands
48. Feature Commands
49. Flow Counters Commands
50. GearBox Commands
51. Kubernetes Commands
52. Linux Kernel Dump Commands
53. Loading, Reloading And Saving Configuration Commands
54. MAC Address FDB Commands
55. Muxcable Commands
56. NDP Commands
57. PBH Commands
58. Routing Stack Commands
59. Watermark Commands
60. Rollback Commands

1 ZTP Commands

Command	Function
config ztp enable	Enable ZTP administrative mode.
config ztp disable	Disable ZTP administrative mode.
config ztp run	Manually restart a new ZTP session.
show ztp status	Display the current ZTP configuration of the switch.

1.1 config ztp enable

Function

Run the **config ztp enable** command to enable ZTP administrative mode.

Syntax

config ztp enable

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
root@sonic:/home/admin# config ztp enable
Running command: ztp enable
```

1.2 config ztp disable

Function

Run the **config ztp disable** command to disable ZTP administrative mode.

Syntax

config ztp disable [**-y**]

Parameter Description

N/A

Usage Guidelines

This command can also be used to abort a current ZTP session and load the factory default switch configuration.

Examples

```
root@sonic:/home/admin# config ztp disable
Active ZTP session will be stopped and disabled, continue? [y/N]: y
Running command: ztp disable -y
```

1.3 config ztp run

Function

Run the **config ztp run** command to manually restart a new ZTP session.

This command deletes the existing */etc/sonic/config_db.json* file and stats ZTP service. It also erases the previous ZTP session data. ZTP configuration is loaded on to the switch and ZTP discovery is performed.

Syntax

config ztp run [**-y**]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
root@sonic:/home/admin# config ztp run
ZTP will be restarted. You may lose switch data and connectivity, continue? [y/N]: y
Running command: ztp run -y
```

1.4 show ztp status

Function

Run the **show ztp status** command to display the current ZTP configuration of the switch.

Syntax

show ztp status [**--verbose**]

Parameter Description

N/A

Usage Guidelines

It also displays detailed information about current state of a ZTP session. It displays information related to all configuration sections as defined in the switch provisioning information discovered in a particular ZTP session.

Examples

```
root@B1-SP1-7712:/home/admin# show ztp status
ZTP Admin Mode : True
ZTP Service          : Inactive
ZTP Status            : SUCCESS
ZTP Source            : dhcp-opt67 (eth0)
Runtime                  : 05m 31s
Timestamp              : 2019-09-11 19:12:24 UTC

ZTP Service is not running
```

```
01-configdb-json: SUCCESS
02-connectivity-check: SUCCESS
```

Use the verbose option to display more detailed information.

```
root@B1-SP1-7712:/home/admin# show ztp status --verbose
Command: ztp status --verbose
=======================================
ZTP
=======================================
ZTP Admin Mode : True
ZTP Service          : Inactive
ZTP Status            : SUCCESS
ZTP Source            : dhcp-opt67 (eth0)
Runtime                  : 05m 31s
Timestamp              : 2019-09-11 19:12:16 UTC
ZTP JSON Version : 1.0

ZTP Service is not running

---------------------------------------
01-configdb-json
---------------------------------------
Status                     : SUCCESS
Runtime                    : 02m 48s
Timestamp                  : 2019-09-11 19:11:55 UTC
Exit Code                : 0
Ignore Result       : False

---------------------------------------
02-connectivity-check
---------------------------------------
Status                     : SUCCESS
Runtime                    : 04s
Timestamp                  : 2019-09-11 19:12:16 UTC
Exit Code                : 0
Ignore Result       : False
```

Table 1-1 Output Fields of the show ztp status –verbose command

Field	Description
ZTP Admin Mode	Displays if the ZTP feature is administratively enabled or disabled. Possible values are True or False. This value is configurable using "config ztp enabled" and "config ztp disable" commands.

Field	Description
ZTP Service	Displays the ZTP service status. The following are possible values this field can display: ● Active Discovery: ZTP service is operational and is performing DHCP discovery to learn switch provisioning information ● Processing: ZTP service has discovered switch provisioning information and is processing it
ZTP Status	Displays the current state and result of ZTP session. The following are possible values this field can display: ● IN-PROGRESS: ZTP session is currently in progress. ZTP service is processing switch provisioning information. ● SUCCESS: ZTP service has successfully processed the switch provisioning information. ● FAILED: ZTP service has failed to process the switch provisioning information. ● Not Started: ZTP service has not started processing the discovered switch provisioning information.
ZTP Source	Displays the DHCP option and then interface name from which switch provisioning information has been discovered.
Runtime	Displays the time taken for ZTP process to complete from start to finish. For individual configuration sections it indicates the time taken to process the associated configuration section.
Timestamp	Displays the date/time stamp when the status field has last changed.
ZTP JSON Version	Version of ZTP JSON file used for describing switch provisioning information.
Status	Displays the current state and result of a configuration section. The following are possible values this field can display: ● IN-PROGRESS: Corresponding configuration section is currently being processed. ● SUCCESS: Corresponding configuration section was processed successfully. ● FAILED: Corresponding configuration section failed to execute successfully. ● Not Started: ZTP service has not started processing the corresponding configuration section. ● DISABLED: Corresponding configuration section has

Field	Description
	been marked as disabled and will not be processed.
Exit Code	Displays the program exit code of the configuration section executed. Non-zero exit code indicates that the configuration section has failed to execute successfully.
Ignore Result	If this value is True, the result of the corresponding configuration section is ignored and not used to evaluate the overall ZTP result.
Activity String	In addition to above information an activity string is displayed indicating the current action being performed by the ZTP service and how much time it has been performing the mentioned activity. Below is an example.

1 Syslog Commands

Command	Function
config syslog add	Add a SYSLOG server to the syslog server list. Note that more that one syslog server can be added in the device.
config syslog delete	Delete the syslog server configured.

1.1 config syslog add

Function

Run the **config syslog add** command to add a SYSLOG server to the syslog server list. Note that more that one syslog server can be added in the device.

Syntax

config syslog add [*syslog-ip-address*] [*syslog-ip-address*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config syslog add 1.1.1.1
Syslog server 1.1.1.1 added to configuration
Restarting rsyslog-config service...
```

1.2 config syslog delete

Function

Run the **config syslog delete** command to delete the syslog server configured.

Syntax

config syslog del [*syslog-ip-address*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config syslog del 1.1.1.1
Syslog server 1.1.1.1 removed from configuration
Restarting rsyslog-config service...
```

1 SoNIC Platform Commands

Command	Function
config hostname	Configure the system hostname.
config platform firmware install	Install a platform component firmware.
config platform firmware update	Update a platform component firmware from current/next SONiC image.
config set_timezone	Set the timezone.
show timezone-list	Display the full list of timezones available.
show boot	Display the current OS image, the image to be loaded on next reboot, and lists all the available images installed on the device.
show clock	Display the current date and time configured on the system.
show environment	Display the platform environmentals, such as voltages, temperatures and fan speeds.
show logging	Display all the currently stored log messages.
show platform fan	Display the status of the device's fans.
show platform firmware status	Display platform components firmware status information.
show platform firmware updates	Display platform components firmware updates information.
show platform firmware version	Display platform components firmware utility version.
show platform pcieinfo	Display the status of pcie.
show platform psustatus	Display the status of the device's power supply units.
show platform ssdhealth	Display health parameters of the device's SSD.

show platform summary	Display a summary of the device's hardware platform.
show platform syseeprom	Display information stored on the system EEPROM.
show platform temperature	Display the status of the device's thermal sensors.
show reboot-cause	Display the cause of the previous reboot.
show reboot-cause history	Display the history of the previous reboots up to 10 entry.
show uptime	Display the current system uptime.
show users	Display a list of users currently logged in to the device.
show version	Display software component versions of the currently running SONiC image.
sonic-installer cleanup	Remove all unused images from the device, leaving only the currently active image and the image which will be booted into next (if different) installed.
sonic-installer install	Install a new image on the alternate image partition.
sonic-installer list	Display information about currently installed images.
sonic-installer remove	Remove the unused SONiC image from the disk.
sonic-installer set_default	Change the image which can be loaded by default in all the subsequent reboots.
sonic-installer set_next_boot	Change the image that can be loaded in the next reboot only.
show interfaces transceiver	Display information for all the interfaces for the transceiver requested or a specific interface if the optional "interface-name" is specified.
sonic-package-manager install	Pull and installs a package on SONiC host.
sonic-package-manager list	List all available SONiC packages, their description, installed version and installation status.

sonic-package-manager repository add	Add a new repository as source for SONiC packages to the database.
sonic-package-manager repository remove	Remove a repository as source for SONiC packages from the database.
sonic-package-manager reset	Reset the package by reinstalling it to its default version.
sonic-package-manager show package changelog	Fetches the changelog from the package manifest and displays it.
sonic-package-manager show package manifest	Fetch the package manifest and displays it.
sonic-package-manager show package versions	Retrieve a list of all available versions for the given package from the configured upstream repository.
sonic-package-manager uninstall	Uninstall package from SONiC host. User needs to stop the feature prior to uninstalling it.

1.1 config hostname

Function

Run the **config hostname** command to configure the system hostname.

Syntax

config hostname *hostname*

Parameter Description

N/A

Usage Guidelines

After the system hostname is configured, you need to re-enter the terminal to take effect.

Examples

```
admin@sonic:~$ sudo config hostname CSW06
Please note loaded setting will be lost after system reboot. To preserve setting, run config save.
```

1.2 config platform firmware install

Function

Run the **config platform firmware install** command to install a platform component firmware.

Both modular and non modular chassis platforms are supported.

Syntax

config platform firmware install chassis component *component-name* **fw** *fw-path* [**-y** | **--yes**]

config platform firmware install module *module-name* **component** *component-name* **fw** *fw-path* [**-y** | **--yes**]

Parameter Description

-y | **--yes**: automatic yes to prompts. Assume "yes" as answer to all prompts and run non-interactively.

Usage Guidelines

fw-path can be absolute path or URL.

Examples

```
admin@sonic:~$ sudo config platform firmware install chassis component BIOS fw
/usr/local/lib/firmware/chassis1/bios.bin
Warning: Immediate cold reboot is required to complete BIOS firmware update.
```

```
New firmware will be installed, continue? [y/N]: y
Installing firmware:
    /usr/local/lib/firmware/chassis1/bios.bin
```

1.3 config platform firmware update

Function

Run the **config platform firmware update** command to update a platform component firmware from current/next SONiC image.

Both modular and non modular chassis platforms are supported.

Syntax

config platform firmware update chassis component *component-name* **fw** [**-y** | **--yes**] [**-f** | **--force**] [**-i** | **--image**]

config platform firmware update module *module-name* **component** *component-name* **fw** [**-y** | **--yes**] [**-f** | **--force**] [**-i** | **--image**]

Parameter Description

-y | **--yes**: automatic yes to prompts. Assume "yes" as answer to all prompts and run non-interactively.

-f | **--force**: update FW regardless the current version.

-i | **--image**: update FW using current/next SONiC image.

Usage Guidelines

FW update requires `platform_components.json` to be created and placed at:

sonic-buildimage/device/<platform_name>/<onie_platform>/platform_components.json.

Example:

1. Non modular chassis platform

```
{
    "chassis": {
        "Chassis1": {
            "component": {
                "BIOS": {
                    "firmware":
"/usr/local/lib/firmware/<platform_name>/<onie_platform>/chassis1/bios.bin",
                    "version": "<bios_version>"
                },
                "CPLD": {
                    "firmware":
"/usr/local/lib/firmware/<platform_name>/<onie_platform>/chassis1/cpld.bin",
                    "version": "<cpld_version>"
                },
```

```
                    "FPGA": {
                        "firmware":
"/usr/local/lib/firmware/<platform_name>/<onie_platform>/chassis1/fpga.bin",
                        "version": "<fpga_version>"
                    }
                }
            }
        }
}
```

2. Modular chassis platform

```
{
    "chassis": {
        "Chassis1": {
            "component": {
                "BIOS": {
                    "firmware":
"/usr/local/lib/firmware/<platform_name>/<onie_platform>/chassis1/bios.bin",
                    "version": "<bios_version>"
                },
                "CPLD": {
                    "firmware":
"/usr/local/lib/firmware/<platform_name>/<onie_platform>/chassis1/cpld.bin",
                    "version": "<cpld_version>"
                },
                "FPGA": {
                    "firmware":
"/usr/local/lib/firmware/<platform_name>/<onie_platform>/chassis1/fpga.bin",
                    "version": "<fpga_version>"
                }
            }
        }
    },
    "module": {
        "Module1": {
            "component": {
                "CPLD": {
                    "firmware":
"/usr/local/lib/firmware/<platform_name>/<onie_platform>/module1/cpld.bin",
                    "version": "<cpld_version>"
                },
                "FPGA": {
                    "firmware":
"/usr/local/lib/firmware/<platform_name>/<onie_platform>/module1/fpga.bin",
                    "version": "<fpga_version>"
                }
```

```
            }
        }
    }
}
```

FW update will be disabled if component definition is not provided (e.g., 'BIOS': { }).

FW version will be read from image if version field is not provided.

current/next values for -i|-image are taken from sonic-installer list.

Examples

```
admin@sonic:~$ sudo config platform firmware update chassis component BIOS fw
Warning: Immediate cold reboot is required to complete BIOS firmware update.
New firmware will be installed, continue? [y/N]: y
Updating firmware:
    /usr/local/lib/firmware/broadcom/x86_64-micas_m2-w6520-24dc8qc-r0/chassis1/bios.bin

admin@sonic:~$ sudo config platform firmware update module Module1 component BIOS fw
Warning: Immediate cold reboot is required to complete BIOS firmware update.
New firmware will be installed, continue? [y/N]: y
Updating firmware:
/usr/local/lib/firmware//broadcom/x86_64-micas_m2-w6520-24dc8qc-r0/module1/bios.bin

admin@sonic:~$ sudo sonic-installer list
  Current: SONiC-OS-202012.0-fb89c28c9
  Next: SONiC-OS-201911.0-2bec3004e
  Available:
  SONiC-OS-202012.0-fb89c28c9
  SONiC-OS-201911.0-2bec3004e
```

1.4 config set_timezone

Function

Run the **config set_timezone** command to set the timezone.

Syntax

sudo config set_timezone *timezone-name*

Parameter Description

timezone-name: Timezone name obtained by using show timezone-list command.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config set_timezone America/New_York
set sonic timezone to America/New_York success!
admin@sonic:~$ show clock
Mon 20 Mar 2023 10:45:18 AM EDT
```

1.5 show timezone-list

Function

Run the **show timezone-list** command to display the full list of timezones available.

Syntax

show timezone-list

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show timezone-list
Africa/Abidjan
Africa/Accra
Africa/Algiers
Africa/Bissau
Africa/Cairo
...
```

1.6 show boot

Function

Run the **show boot** command to display the current OS image, the image to be loaded on next reboot, and lists all the available images installed on the device.

Syntax

show boot

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show boot
Current: SONiC-OS-20181130.31
Next: SONiC-OS-20181130.31
Available:
SONiC-OS-20181130.31
```

1.7 show clock

Function

Run the **show clock** command to display the current date and time configured on the system.

Syntax

show clock

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show clock
Mon Mar 25 20:25:16 UTC 2019
```

1.8 show environment

Function

Run the **show environment** command to display the platform environmentals, such as voltages, temperatures and fan speeds.

Syntax

show environment

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show environment
coretemp-isa-0000
Adapter: ISA adapter
Core 0:         +28.0 C  (high = +98.0 C, crit = +98.0 C)
Core 1:         +28.0 C  (high = +98.0 C, crit = +98.0 C)
Core 2:         +28.0 C  (high = +98.0 C, crit = +98.0 C)
Core 3:         +28.0 C  (high = +98.0 C, crit = +98.0 C)
SMF_Z9100_ON-isa-0000
Adapter: ISA adapter
CPU XP3R3V_EARLY:                +3.22 V
<... few more things ...>
Onboard Temperature Sensors:
CPU:                             30 C
BCM56960 (PSU side):              35 C
<... few more things ...>

Onboard Voltage Sensors:
CPU XP3R3V_EARLY                  3.22 V
<... few more things ...>

Fan Trays:
Fan Tray 1:
   Fan1 Speed:      6192 RPM
   Fan2 Speed:      6362 RPM
   Fan1 State:         Normal
   Fan2 State:         Normal
   Air Flow:            F2B
<... few more things ...>

PSUs:
   PSU 1:
      Input:           AC
<... few more things ...>
```

Note
The show output has got lot of information; only the sample output is given in the above example. Though the displayed output slightly differs from one platform to another platform, the overall content will be similar to the example mentioned above.

1.9 show logging

Function

Run the **show logging** command to display all the currently stored log messages.

All the latest processes and corresponding transactions are stored in the "syslog" file.

This file is saved in the path `/var/log` and can be viewed by giving the command ` sudo cat syslog` as this requires root login.

Syntax

show logging [{ *process-name* [**-l** | **--lines** *number-of-lines*] } | { **-f** | **--follow** }]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show logging
```

It can be useful to pipe the output from **show logging** to the command **more** in order to examine one screenful of log messages at a time.

```
admin@sonic:~$ show logging | more
```

Optionally, you can specify a process name in order to display only log messages mentioning that process.

```
admin@sonic:~$ show logging sensord
```

Optionally, you can specify a number of lines to display using the **-l** or **--lines** option. Only the most recent N lines will be displayed. Also note that this option can be combined with a process name.

```
admin@sonic:~$ show logging --lines 50
admin@sonic:~$ show logging sensord --lines 50
```

Optionally, you can follow the log live as entries are written to it by specifying the **-f** or **--follow** flag.

```
admin@sonic:~$ show logging --follow
```

1.10 show platform fan

Function

Run the **show platform fan** command to display the status of the device's fans.

Syntax

show platform fan

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show platform fan
          FAN      Speed     Direction     Presence     Status          Timestamp
-----------  --------  -----------  ----------  --------  -----------------
         fan1       34%       intake      Present        OK  20200302 06:58:56
         fan2       43%       intake      Present        OK  20200302 06:58:56
         fan3       38%       intake      Present        OK  20200302 06:58:56
         fan4       49%       intake      Present        OK  20200302 06:58:57
         fan5       38%      exhaust      Present        OK  20200302 06:58:57
         fan6       48%      exhaust      Present        OK  20200302 06:58:57
         fan7       39%      exhaust      Present        OK  20200302 06:58:57
         fan8       48%      exhaust      Present        OK  20200302 06:58:57
```

1.11 show platform firmware status

Function

Run the **show platform firmware status** command to display platform components firmware status information.

Syntax

show platform firmware status

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo show platform firmware status
Chassis Module Component    Version                 Description
-----   -----  ------   -------------------   -------------------------
M2XXX     N/A       ONIE     2020.11-5.2.0022-9600       ONIE - Open Network Install Environment
                    SSD      0202-000                    SSD - Solid-State Drive
                    BIOS     0ACLH004_02.02.008_9600     BIOS - Basic Input/Output System
                    CPLD1    CPLD000120_REV0900          CPLD - Complex Programmable Logic Device
                    CPLD2    CPLD000165_REV0500          CPLD - Complex Programmable Logic
Device
                    CPLD3    CPLD000166_REV0300          CPLD - Complex Programmable Logic Device
                    CPLD4    CPLD000167_REV0100          CPLD - Complex Programmable Logic Device
```

1.12 show platform firmware updates

Function

Run the **show platform firmware updates** command to display platform components firmware updates information.

Syntax

show platform firmware updates [**-i** | **--image**]

Parameter Description

-i | **--image**: show updates using current/next SONiC image

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo show platform firmware updates
Chassis      Module      Component      Firmware                                          Version
(Current/Available)                              Status
---------  --------  -----------  ----------------------------------------  --------------
-----------------------------------  ------------------
M2XXX        N/A         ONIE             /usr/local/lib/firmware/onie.bin
2020.11-5.2.0022-9600 / 2020.11-5.2.0024-9600         update is required
                         SSD              /usr/local/lib/firmware/ssd.bin
0202-000 / 0204-000                                     update is required
                         BIOS             /usr/local/lib/firmware/bios.bin     0ACLH004_02.02.008_9600 /
0ACLH004_02.02.010_9600    update is required
                         CPLD1            /usr/local/lib/firmware/cpld.mpfa    CPLD000120_REV0900 /
CPLD000120_REV0900                 up-to-date
                         CPLD2            /usr/local/lib/firmware/cpld.mpfa    CPLD000165_REV0500 /
CPLD000165_REV0500                 up-to-date
                         CPLD3            /usr/local/lib/firmware/cpld.mpfa    CPLD000166_REV0300 /
CPLD000166_REV0300                 up-to-date
                         CPLD4            /usr/local/lib/firmware/cpld.mpfa    CPLD000167_REV0100 /
CPLD000167_REV0100                 up-to-date
```

1.13 show platform firmware version

Function

Run the **show platform firmware version** command to display platform components firmware utility version.

Syntax

show platform firmware version

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show platform firmware version
fwutil version 2.0.0.0
```

1.14 show platform pcieinfo

Function

Run the **show platform pcieinfo** command to display the status of pcie.

Syntax

show platform pcieinfo

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show platform pcieinfo
==============================Display PCIe
Device==============================
bus:dev.fn 00:00.0 - dev_id=0x6f00, Host bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3
v4/Xeon D DMI2 (rev 05)
bus:dev.fn 00:01.0 - dev_id=0x6f02, PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3
v4/Xeon D PCI Express Root Port 1 (rev 05)
bus:dev.fn 00:01.1 - dev_id=0x6f03, PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3
v4/Xeon D PCI Express Root Port 1 (rev 05)
bus:dev.fn 00:02.0 - dev_id=0x6f04, PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3
v4/Xeon D PCI Express Root Port 2 (rev 05)
bus:dev.fn 00:02.2 - dev_id=0x6f06, PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3
v4/Xeon D PCI Express Root Port 2 (rev 05)
bus:dev.fn 00:02.3 - dev_id=0x6f07, PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3
v4/Xeon D PCI Express Root Port 2 (rev 05)
bus:dev.fn 00:03.0 - dev_id=0x6f08, PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3
v4/Xeon D PCI Express Root Port 3 (rev 05)
```

bus:dev.fn 00:03.1 - dev_id=0x6f09, PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 3 (rev 05)
bus:dev.fn 00:03.2 - dev_id=0x6f0a, PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 3 (rev 05)
bus:dev.fn 00:03.3 - dev_id=0x6f0b, PCI bridge: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI Express Root Port 3 (rev 05)
bus:dev.fn 00:04.0 - dev_id=0x6f20, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Crystal Beach DMA Channel 0 (rev 05)
bus:dev.fn 00:04.1 - dev_id=0x6f21, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Crystal Beach DMA Channel 1 (rev 05)
bus:dev.fn 00:04.2 - dev_id=0x6f22, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Crystal Beach DMA Channel 2 (rev 05)
bus:dev.fn 00:04.3 - dev_id=0x6f23, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Crystal Beach DMA Channel 3 (rev 05)
bus:dev.fn 00:04.4 - dev_id=0x6f24, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Crystal Beach DMA Channel 4 (rev 05)
bus:dev.fn 00:04.5 - dev_id=0x6f25, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Crystal Beach DMA Channel 5 (rev 05)
bus:dev.fn 00:04.6 - dev_id=0x6f26, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Crystal Beach DMA Channel 6 (rev 05)
bus:dev.fn 00:04.7 - dev_id=0x6f27, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Crystal Beach DMA Channel 7 (rev 05)
bus:dev.fn 00:05.0 - dev_id=0x6f28, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Map/VTd_Misc/System Management (rev 05)
bus:dev.fn 00:05.1 - dev_id=0x6f29, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO Hot Plug (rev 05)
bus:dev.fn 00:05.2 - dev_id=0x6f2a, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO RAS/Control Status/Global Errors (rev 05)
bus:dev.fn 00:05.4 - dev_id=0x6f2c, PIC: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D I/O APIC (rev 05)
bus:dev.fn 00:05.6 - dev_id=0x6f39, Performance counters: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IO Performance Monitoring (rev 05)
bus:dev.fn 00:06.0 - dev_id=0x6f10, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO Debug (rev 05)
bus:dev.fn 00:06.1 - dev_id=0x6f11, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO Debug (rev 05)
bus:dev.fn 00:06.2 - dev_id=0x6f12, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO Debug (rev 05)
bus:dev.fn 00:06.3 - dev_id=0x6f13, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO Debug (rev 05)
bus:dev.fn 00:06.4 - dev_id=0x6f14, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO Debug (rev 05)
bus:dev.fn 00:06.5 - dev_id=0x6f15, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO Debug (rev 05)
bus:dev.fn 00:06.6 - dev_id=0x6f16, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO Debug (rev 05)

bus:dev.fn 00:06.7 - dev_id=0x6f17, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO Debug (rev 05)
bus:dev.fn 00:07.0 - dev_id=0x6f18, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO Debug (rev 05)
bus:dev.fn 00:07.1 - dev_id=0x6f19, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO Debug (rev 05)
bus:dev.fn 00:07.2 - dev_id=0x6f1a, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO Debug (rev 05)
bus:dev.fn 00:07.3 - dev_id=0x6f1b, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO Debug (rev 05)
bus:dev.fn 00:07.4 - dev_id=0x6f1c, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D IIO Debug (rev 05)
bus:dev.fn 00:14.0 - dev_id=0x8c31, USB controller: Intel Corporation 8 Series/C220 Series Chipset Family USB xHCI (rev 05)
bus:dev.fn 00:16.0 - dev_id=0x8c3a, Communication controller: Intel Corporation 8 Series/C220 Series Chipset Family MEI Controller #1 (rev 04)
bus:dev.fn 00:16.1 - dev_id=0x8c3b, Communication controller: Intel Corporation 8 Series/C220 Series Chipset Family MEI Controller #2 (rev 04)
bus:dev.fn 00:1d.0 - dev_id=0x8c26, USB controller: Intel Corporation 8 Series/C220 Series Chipset Family USB EHCI #1 (rev 05)
bus:dev.fn 00:1f.0 - dev_id=0x8c54, ISA bridge: Intel Corporation C224 Series Chipset Family Server Standard SKU LPC Controller (rev 05)
bus:dev.fn 00:1f.2 - dev_id=0x8c02, SATA controller: Intel Corporation 8 Series/C220 Series Chipset Family 6-port SATA Controller 1 [AHCI mode] (rev 05)
bus:dev.fn 00:1f.3 - dev_id=0x8c22, SMBus: Intel Corporation 8 Series/C220 Series Chipset Family SMBus Controller (rev 05)
bus:dev.fn 04:00.0 - dev_id=0x15ab, Ethernet controller: Intel Corporation Ethernet Connection X552 10 GbE Backplane
bus:dev.fn 04:00.1 - dev_id=0x15ab, Ethernet controller: Intel Corporation Ethernet Connection X552 10 GbE Backplane
bus:dev.fn 05:00.0 - dev_id=0x15ab, Ethernet controller: Intel Corporation Ethernet Connection X552 10 GbE Backplane
bus:dev.fn 05:00.1 - dev_id=0x15ab, Ethernet controller: Intel Corporation Ethernet Connection X552 10 GbE Backplane
bus:dev.fn 06:00.0 - dev_id=0xb780, Ethernet controller: Broadcom Inc. and subsidiaries Device b780 (rev 01)
bus:dev.fn 07:00.0 - dev_id=0x1537, Ethernet controller: Intel Corporation I210 Gigabit Backplane Connection (rev 03)
bus:dev.fn 08:00.0 - dev_id=0x7011, Memory controller: Xilinx Corporation Device 7011
bus:dev.fn ff:0b.0 - dev_id=0x6f81, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D R3 QPI Link 0/1 (rev 05)
bus:dev.fn ff:0b.1 - dev_id=0x6f36, Performance counters: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D R3 QPI Link 0/1 (rev 05)
bus:dev.fn ff:0b.2 - dev_id=0x6f37, Performance counters: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D R3 QPI Link 0/1 (rev 05)

bus:dev.fn ff:0b.3 - dev_id=0x6f76, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D R3 QPI Link Debug (rev 05)
bus:dev.fn ff:0c.0 - dev_id=0x6fe0, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 05)
bus:dev.fn ff:0c.1 - dev_id=0x6fe1, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 05)
bus:dev.fn ff:0c.2 - dev_id=0x6fe2, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 05)
bus:dev.fn ff:0c.3 - dev_id=0x6fe3, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 05)
bus:dev.fn ff:0f.0 - dev_id=0x6ff8, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 05)
bus:dev.fn ff:0f.4 - dev_id=0x6ffc, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 05)
bus:dev.fn ff:0f.5 - dev_id=0x6ffd, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 05)
bus:dev.fn ff:0f.6 - dev_id=0x6ffe, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Caching Agent (rev 05)
bus:dev.fn ff:10.0 - dev_id=0x6f1d, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D R2PCIe Agent (rev 05)
bus:dev.fn ff:10.1 - dev_id=0x6f34, Performance counters: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D R2PCIe Agent (rev 05)
bus:dev.fn ff:10.5 - dev_id=0x6f1e, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Ubox (rev 05)
bus:dev.fn ff:10.6 - dev_id=0x6f7d, Performance counters: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Ubox (rev 05)
bus:dev.fn ff:10.7 - dev_id=0x6f1f, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Ubox (rev 05)
bus:dev.fn ff:12.0 - dev_id=0x6fa0, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Home Agent 0 (rev 05)
bus:dev.fn ff:12.1 - dev_id=0x6f30, Performance counters: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Home Agent 0 (rev 05)
bus:dev.fn ff:12.2 - dev_id=0x6f70, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Home Agent 0 Debug (rev 05)
bus:dev.fn ff:13.0 - dev_id=0x6fa8, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Target Address/Thermal/RAS (rev 05)
bus:dev.fn ff:13.1 - dev_id=0x6f71, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Target Address/Thermal/RAS (rev 05)
bus:dev.fn ff:13.2 - dev_id=0x6faa, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel Target Address Decoder (rev 05)
bus:dev.fn ff:13.3 - dev_id=0x6fab, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel Target Address Decoder (rev 05)
bus:dev.fn ff:13.4 - dev_id=0x6fac, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel Target Address Decoder (rev 05)
bus:dev.fn ff:13.5 - dev_id=0x6fad, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel Target Address Decoder (rev 05)

bus:dev.fn ff:13.6 - dev_id=0x6fae, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D DDRIO Channel 0/1 Broadcast (rev 05)
bus:dev.fn ff:13.7 - dev_id=0x6faf, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D DDRIO Global Broadcast (rev 05)
bus:dev.fn ff:14.0 - dev_id=0x6fb0, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel 0 Thermal Control (rev 05)
bus:dev.fn ff:14.1 - dev_id=0x6fb1, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel 1 Thermal Control (rev 05)
bus:dev.fn ff:14.2 - dev_id=0x6fb2, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel 0 Error (rev 05)
bus:dev.fn ff:14.3 - dev_id=0x6fb3, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel 1 Error (rev 05)
bus:dev.fn ff:14.4 - dev_id=0x6fbc, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D DDRIO Channel 0/1 Interface (rev 05)
bus:dev.fn ff:14.5 - dev_id=0x6fbd, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D DDRIO Channel 0/1 Interface (rev 05)
bus:dev.fn ff:14.6 - dev_id=0x6fbe, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D DDRIO Channel 0/1 Interface (rev 05)
bus:dev.fn ff:14.7 - dev_id=0x6fbf, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D DDRIO Channel 0/1 Interface (rev 05)
bus:dev.fn ff:15.0 - dev_id=0x6fb4, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel 2 Thermal Control (rev 05)
bus:dev.fn ff:15.1 - dev_id=0x6fb5, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel 3 Thermal Control (rev 05)
bus:dev.fn ff:15.2 - dev_id=0x6fb6, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel 2 Error (rev 05)
bus:dev.fn ff:15.3 - dev_id=0x6fb7, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Memory Controller 0 - Channel 3 Error (rev 05)
bus:dev.fn ff:1e.0 - dev_id=0x6f98, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Power Control Unit (rev 05)
bus:dev.fn ff:1e.1 - dev_id=0x6f99, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Power Control Unit (rev 05)
bus:dev.fn ff:1e.2 - dev_id=0x6f9a, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Power Control Unit (rev 05)
bus:dev.fn ff:1e.3 - dev_id=0x6fc0, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Power Control Unit (rev 05)
bus:dev.fn ff:1e.4 - dev_id=0x6f9c, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Power Control Unit (rev 05)
bus:dev.fn ff:1e.7 - dev_id=0x6f9f, System peripheral: Intel Corporation Device 6f9f (rev 05)
bus:dev.fn ff:1f.0 - dev_id=0x6f88, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Power Control Unit (rev 05)
bus:dev.fn ff:1f.2 - dev_id=0x6f8a, System peripheral: Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D Power Control Unit (rev 05)

1.15 show platform psustatus

Function

Run the **show platform psustatus** command to display the status of the device's power supply units.

Syntax

show platform psustatus

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show platform psustatus
PSU      Model             Serial          HW Rev      Voltage (V)     Current (A)     Power (W)   Status
LED
-----  -------------  ------------  --------  -------------  -------------  -----------  ----
----  -----
PSU 1  MTEF-PSF-AC-A  MT1621X15246  A3                11.97           4.56         54.56  OK
green
```

1.16 show platform ssdhealth

Function

Run the **show platform ssdhealth** command to display health parameters of the device's SSD.

Syntax

show platform ssdhealth [**--vendor**]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show platform ssdhealth
  Device Model : M.2 (S42) 3IE3
  Health       : 99.665%
```

```
  Temperature   : 30C
```

1.17 show platform summary

Function

Run the **show platform summary** command to display a summary of the device's hardware platform.

Syntax

show platform summary

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show platform summary
  Platform: x86_64-micas_m2-w6520-24dc8qc-r0
  HwSKU: M2-W6520-24DC8QC
  ASIC: broadcom
  ASIC Count: 1
  Serial Number: 0000000000000
  Model Number: 01019APZ
  Hardware Revision: 105
```

1.18 show platform syseeprom

Function

Run the **show platform syseeprom** command to display information stored on the system EEPROM.

Note that the output of this command is not the same for all vendor's platforms.

Couple of example outputs are given below.

Syntax

show platform syseeprom

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show platform syseeprom
TlvInfo Header:
  Id String:       TlvInfo
  Version:         1
  Total Length: 193
  TLV Name                Code        Len    Value
-------------------   ------   -----   --------------------------------
Product Name             0x21         16    M2-W6520-24DC8QC
Part Number              0x22          8    01019APZ
Serial Number            0x23         13    0000000000000
Base MAC Address         0x24          6    EC:B9:70:B4:4C:2B
Manufacture Date         0x25         19    07/26/2023 16:05:42
Device Version           0x26          1    105
Label Revision           0x27          3    R01
Platform Name            0x28         32    x86_64-micas_m2-w6520-24dc8qc-r0
ONIE Version             0x29          7    2023.02
MAC Addresses            0x2A          2    3
Manufacturer             0x2B          5    Micas
Manufacture Country      0x2C          3    USA
Vendor Name              0x2D          5    Micas
Diag Version             0x2E          8    0.1.0.15
Service Tag              0x2F         21    www.micasnetworks.com
Vendor Extension         0xFD          6
CRC-32                   0xFE          4    0x9FCB07E3

(checksum valid)
```

1.19 show platform temperature

Function

Run the **show platform temperature** command to display the status of the device's thermal sensors.

Syntax

show platform temperature

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show platform temperature
                      NAME       Temperature     High Th     Low Th     Crit High Th     Crit Low Th
Warning              Timestamp
----------------------  -------------  ---------  --------  --------------  -------------  --
-------  -----------------
       Ambient ASIC Temp             37.0        100.0      N/A          120.0            N/A
False    20200302 06:58:57
 Ambient Fan Side Temp               28.5        100.0      N/A          120.0            N/A
False    20200302 06:58:57
Ambient Port Side Temp              31.0        100.0      N/A          120.0            N/A
False    20200302 06:58:57
          CPU Core 0 Temp           36.0         87.0      N/A          105.0            N/A
False    20200302 06:59:57
          CPU Core 1 Temp           38.0         87.0      N/A          105.0            N/A
False    20200302 06:59:57
            CPU Pack Temp           38.0         87.0      N/A          105.0            N/A
False    20200302 06:59:57
                PSU-1 Temp          28.0        100.0      N/A          120.0            N/A
False    20200302 06:59:58
                PSU-2 Temp          28.0        100.0      N/A          120.0            N/A
False    20200302 06:59:58
      xSFP module 1 Temp            31.5         70.0      N/A           90.0            N/A
False    20200302 06:59:57
      xSFP module 2 Temp            35.0         70.0      N/A           90.0            N/A
False    20200302 06:59:57
      xSFP module 3 Temp            32.0         70.0      N/A           90.0            N/A
False    20200302 06:59:57
      xSFP module 4 Temp            33.5         70.0      N/A           90.0            N/A
False    20200302 06:59:57
      xSFP module 5 Temp            34.0         70.0      N/A           90.0            N/A
False    20200302 06:59:57
      xSFP module 6 Temp            36.0         70.0      N/A           90.0            N/A
False    20200302 06:59:57
      xSFP module 7 Temp            33.5         70.0      N/A           90.0            N/A
False    20200302 06:59:57
      xSFP module 8 Temp            33.0         70.0      N/A           90.0            N/A
False    20200302 06:59:57
      xSFP module 9 Temp            32.0         70.0      N/A           90.0            N/A
False    20200302 06:59:57
     xSFP module 10 Temp            38.5         70.0      N/A           90.0            N/A
False    20200302 06:59:57
     xSFP module 11 Temp            38.0         70.0      N/A           90.0            N/A
False    20200302 06:59:57
```

xSFP module 12 Temp	39.0	70.0	N/A	90.0	N/A
False 20200302 06:59:57					
xSFP module 13 Temp	35.5	70.0	N/A	90.0	N/A
False 20200302 06:59:57					
xSFP module 14 Temp	37.0	70.0	N/A	90.0	N/A
False 20200302 06:59:57					
xSFP module 15 Temp	36.0	70.0	N/A	90.0	N/A
False 20200302 06:59:57					
xSFP module 16 Temp	36.5	70.0	N/A	90.0	N/A
False 20200302 06:59:57					
xSFP module 17 Temp	32.0	70.0	N/A	90.0	N/A
False 20200302 06:59:57					
xSFP module 18 Temp	34.5	70.0	N/A	90.0	N/A
False 20200302 06:59:57					
xSFP module 19 Temp	30.0	70.0	N/A	90.0	N/A
False 20200302 06:59:57					
xSFP module 20 Temp	31.5	70.0	N/A	90.0	N/A
False 20200302 06:59:57					
xSFP module 21 Temp	34.0	70.0	N/A	90.0	N/A
False 20200302 06:59:57					
xSFP module 22 Temp	34.4	70.0	N/A	90.0	N/A
False 20200302 06:59:57					
xSFP module 23 Temp	34.0	70.0	N/A	90.0	N/A
False 20200302 06:59:57					
xSFP module 24 Temp	35.6	70.0	N/A	90.0	N/A
False 20200302 06:59:57					
xSFP module 25 Temp	38.0	70.0	N/A	90.0	N/A
False 20200302 06:59:57					
xSFP module 26 Temp	32.2	70.0	N/A	90.0	N/A
False 20200302 06:59:58					
xSFP module 27 Temp	39.0	70.0	N/A	90.0	N/A
False 20200302 06:59:58					
xSFP module 28 Temp	30.1	70.0	N/A	90.0	N/A
False 20200302 06:59:58					
xSFP module 29 Temp	32.0	70.0	N/A	90.0	N/A
False 20200302 06:59:58					
xSFP module 30 Temp	35.3	70.0	N/A	90.0	N/A
False 20200302 06:59:58					
xSFP module 31 Temp	31.0	70.0	N/A	90.0	N/A
False 20200302 06:59:58					
xSFP module 32 Temp	39.5	70.0	N/A	90.0	N/A
False 20200302 06:59:58					

1.20 show reboot-cause

Function

Run the **show reboot-cause** command to display the cause of the previous reboot.

Syntax

show reboot-cause

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show reboot-cause
User issued reboot command [User: admin, Time: Mon Mar 25 01:02:03 UTC 2019]
```

1.21 show reboot-cause history

Function

Run the **show reboot-cause history** command to display the history of the previous reboots up to 10 entry.

Syntax

show reboot-cause history

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show reboot-cause history
Name                 Cause          Time                          User      Comment
-------------------  -----------  ----------------------------  ------  ---------
2020_10_09_02_33_06  reboot         Fri Oct  9 02:29:44 UTC 2020  admin
2020_10_09_01_56_59  reboot         Fri Oct  9 01:53:49 UTC 2020  admin
2020_10_09_02_00_53  fast-reboot    Fri Oct  9 01:58:04 UTC 2020  admin
2020_10_09_04_53_58  warm-reboot    Fri Oct  9 04:51:47 UTC 2020  admin
```

1.22 show uptime

Function

Run the **show uptime** command to display the current system uptime.

Syntax

show uptime

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show uptime
  up 2 days, 21 hours, 30 minutes
```

1.23 show users

Function

Run the **show users** command to display a list of users currently logged in to the device.

Syntax

show users

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show users
admin    pts/9        Mar 25 20:31 (100.127.20.23)

admin@sonic:~$ show users
admin    ttyS1        2019-03-25 20:31
```

1.24 show version

Function

Run the **show version** command to display software component versions of the currently running SONiC image.

This includes the SONiC image version as well as Docker image versions.

This command is used to display relevant information as the SONiC and Linux kernel version being utilized, as well as the ID of the commit used to build the SONiC image. The second section of the output displays the various docker images and their associated IDs.

Syntax

show version

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show version

SONiC Software Version: SONiC_1.3.5_20231201033518
Distribution: Debian 11.8
Kernel: 5.10.0-8-2-amd64
Build commit: eb6f0fcaa
Build date: Thu Nov 30 19:47:18 UTC 2023
Built by: ngcf@sonic-114

Platform: x86_64-micas_m2-w6930-64qc-r0
HwSKU: M2-W6930-64QC
ASIC: broadcom
ASIC Count: 1
Serial Number: 0000000000000
Model Number: 01019AQ0
Hardware Revision: 105
Uptime: 01:56:39 up 2 days, 23:48,  1 user,  load average: 1.97, 1.98, 2.11

Docker images:
REPOSITORY                 TAG                                 IMAGE ID       SIZE
docker-syncd-brcm          SONiC_1.3.6_20231201033518     dca4b32dfe24     741MB
docker-syncd-brcm          latest                              dca4b32dfe24     741MB
docker-gbsyncd-credo       SONiC_1.3.6_20231201033518     8ca879183bf0     471MB
docker-gbsyncd-credo       latest                              8ca879183bf0     471MB
```

```
docker-macsec                SONiC_1.3.6_20231201033518     88b65a5e9418     437MB
docker-macsec                latest                         88b65a5e9418     437MB
docker-l2mcd                 SONiC_1.3.6_20231201033518     b0dba9e6fb88     452MB
docker-l2mcd                 latest                         b0dba9e6fb88     452MB
docker-fpm-frr               SONiC_1.3.6_20231201033518     94415c4a208f     452MB
docker-fpm-frr               latest                         94415c4a208f     452MB
docker-iccpd                 SONiC_1.3.6_20231201033518     a5cf29dedab2     434MB
docker-iccpd                 latest                         a5cf29dedab2     434MB
docker-dhcp-relay            latest                         f0a300bf2656     431MB
docker-teamd                 SONiC_1.3.6_20231201033518     c66765cb3bda     433MB
docker-teamd                 latest                         c66765cb3bda     433MB
docker-stp                   SONiC_1.3.6_20231201033518     d8102ab1219c     456MB
docker-stp                   latest                         d8102ab1219c     456MB
docker-snmp                  SONiC_1.3.6_20231201033518     f9f9613320f5     510MB
docker-snmp                  latest                         f9f9613320f5     510MB
docker-sonic-telemetry       SONiC_1.3.6_20231201033518     3dea78a5d131     563MB
docker-sonic-telemetry       latest                         3dea78a5d131     563MB
docker-sonic-mgmt-framework  SONiC_1.3.6_20231201033518     0ee611058c6e     657MB
docker-sonic-mgmt-framework  latest                         0ee611058c6e     657MB
docker-sflow                 SONiC_1.3.6_20231201033518     9eac54af4cfb     434MB
docker-sflow                 latest                         9eac54af4cfb     434MB
docker-router-advertiser     SONiC_1.3.6_20231201033518     b92c95b83283     417MB
docker-router-advertiser     latest                         b92c95b83283     417MB
docker-platform-monitor      SONiC_1.3.6_20231201033518     40edccee910b     678MB
docker-platform-monitor      latest                         40edccee910b     678MB
docker-reup                  SONiC_1.3.6_20231201033518     d0f5018dc39e     482MB
docker-reup                  latest                         d0f5018dc39e     482MB
docker-orchagent             SONiC_1.3.6_20231201033518     b0ad64277121     449MB
docker-orchagent             latest                         b0ad64277121     449MB
docker-nat                   SONiC_1.3.6_20231201033518     1662cf2b43a4     434MB
docker-nat                   latest                         1662cf2b43a4     434MB
docker-lldp                  SONiC_1.3.6_20231201033518     28bf2b377b1e     455MB
docker-lldp                  latest                         28bf2b377b1e     455MB
docker-database              SONiC_1.3.6_20231201033518     269329a8cac1     415MB
docker-database              latest                         269329a8cac1     415MB
docker-mux                   SONiC_1.3.6_20231201033518     4323b930ddad     467MB
docker-mux                   latest                         4323b930ddad     467MB
```

1.25 sonic-installer cleanup

Function

Run the **sonic-installer cleanup** command to remove all unused images from the device, leaving only the currently active image and the image which will be booted into next (if different) installed.

If there are no images which can be removed, the command will output “No image(s) to remove”.

Syntax

sonic-installer cleanup [**-y** | **--yes**]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo sonic-installer cleanup
  Remove images which are not current and next, continue? [y/N]: y
  No image(s) to remove
```

1.26 sonic-installer install

Function

Run the **sonic-installer install** command to install a new image on the alternate image partition.

This command takes a path to an installable SONiC image or URL and installs the image.

Syntax

sonic-installer install *image-file-path*

Parameter Description

image-file-path: A path of installable SONiC image or the URL to download the image.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo sonic-installer install https://sonic-
jenkins.westus.cloudapp.azure.com/job/xxxx/job/buildimage-xxxx-all/xxx/artifact/target/sonic-
xxxx.bin
New image will be installed, continue? [y/N]: y
Downloading image...
...100%, 480 MB, 3357 KB/s, 146 seconds passed
Command: /tmp/sonic_image
Verifying image checksum ... OK.
Preparing image archive ... OK.
ONIE Installer: platform: XXXX
```

```
onie_platform:
Installing SONiC in SONiC
Installing SONiC to /host/image-xxxx
Directory /host/image-xxxx/ already exists. Cleaning up...
Archive:  fs.zip
   creating: /host/image-xxxx/boot/
  inflating: /host/image-xxxx/boot/vmlinuz-3.16.0-4-amd64
  inflating: /host/image-xxxx/boot/config-3.16.0-4-amd64
  inflating: /host/image-xxxx/boot/System.map-3.16.0-4-amd64
  inflating: /host/image-xxxx/boot/initrd.img-3.16.0-4-amd64
   creating: /host/image-xxxx/platform/
 extracting: /host/image-xxxx/platform/firsttime
  inflating: /host/image-xxxx/fs.squashfs
  inflating: /host/image-xxxx/dockerfs.tar.gz
Log file system already exists. Size: 4096MB
Installed SONiC base image SONiC-OS successfully

Command: cp /etc/sonic/minigraph.xml /host/

Command: grub-set-default --boot-directory=/host 0

Done
```

Installing a new image using the sonic-installer will keep using the packages installed on the currently running SONiC image and automatically migrate those. In order to perform clean SONiC installation use the -skip-package-migration option.

```
admin@sonic:~$ sudo sonic-installer install https://sonic-
jenkins.westus.cloudapp.azure.com/job/xxxx/job/buildimage-xxxx-all/xxx/artifact/target/sonic-
xxxx.bin --skip-package-migration
```

1.27 sonic-installer list

Function

Run the **sonic-installer list** command to display information about currently installed images.

It displays a list of installed images, currently running image and image set to be loaded in next reboot.

Syntax

sonic-installer list

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo sonic-installer list
  Current: SONiC-OS-HEAD.XXXX
  Next: SONiC-OS-HEAD.XXXX
  Available:
  SONiC-OS-HEAD.XXXX
  SONiC-OS-HEAD.YYYY
```

Note
This output can be obtained without evelated privileges by running the **show boot** command.

1.28 sonic-installer remove

Function

Run the **sonic-installer remove** command to remove the unused SONiC image from the disk.

Note
It's not allowed to remove currently running image.

Syntax

sonic-installer remove [**-y** | **--yes**] *image-name*

Parameter Description

image-name: SONiC image name installed on the device.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo sonic-installer remove SONiC-OS-HEAD.YYYY
Image will be removed, continue? [y/N]: y
Updating GRUB...
Done
Removing image root filesystem...
Done
Command: grub-set-default --boot-directory=/host 0
```

```
Image removed
```

1.29 sonic-installer set_default

Function

Run the **sonic-installer set_default** command to change the image which can be loaded by default in all the subsequent reboots.

Syntax

sonic-installer set_default *image-name*

Parameter Description

image-name: SONiC image name installed on the device.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo sonic-installer set_default SONiC-OS-HEAD.XXXX
```

1.30 sonic-installer set_next_boot

Function

Run the **sonic-installer set_next_boot** command to change the image that can be loaded in the next reboot only.

Note
That it will fallback to current image in all other subsequent reboots after the next reboot.

Syntax

sonic-installer set_next_boot *image-name*

Parameter Description

image-name: SONiC image name installed on the device.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo sonic-installer set_next_boot SONiC-OS-HEAD.XXXX
```

1.31 show interfaces transceiver

Function

Run the **show interfaces transceiver** command to display information for all the interfaces for the transceiver requested or a specific interface if the optional "interface-name" is specified.

Syntax

show interfaces transceiver { **eeprom** [**-d** | **--dom**] | **lpmode** | **presence** | **error-status** [**-hw** | **--fetch-from-hardware**] } [*interface-name*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
Decode and display information stored on the EEPROM of SFP transceiver connected to Ethernet0.
admin@sonic:~$ show interfaces transceiver eeprom --dom Ethernet0
Ethernet0: SFP detected
    Connector : No separable connector
    Encoding : Unspecified
    Extended Identifier : Unknown
    Extended RateSelect Compliance : QSFP+ Rate Select Version 1
    Identifier : QSFP+
    Length Cable Assembly(m) : 1
    Specification compliance :
            10/40G Ethernet Compliance Code : 40GBASE-CR4
            Fibre Channel Speed : 1200 Mbytes/Sec
            Fibre Channel link length/Transmitter Technology : Electrical inter-enclosure (EL)
            Fibre Channel transmission media : Twin Axial Pair (TW)
    Vendor Date Code(YYYY-MM-DD Lot) : 2015-10-31
    Vendor Name : XXXXX
    Vendor OUI : XX-XX-XX
    Vendor PN : 1111111111
    Vendor Rev :
    Vendor SN : 111111111
    ChannelMonitorValues:
            RX1Power: -1.1936dBm
            RX2Power: -1.1793dBm
            RX3Power: -0.9388dBm
            RX4Power: -1.0729dBm
            TX1Bias: 4.0140mA
            TX2Bias: 4.0140mA
```

```
            TX3Bias: 4.0140mA
            TX4Bias: 4.0140mA
    ModuleMonitorValues :
              Temperature : 1.1111C
              Vcc : 0.0000Volts
```

Display status of low-power mode of SFP transceiver connected to Ethernet100.

```
admin@sonic:~$ show interfaces transceiver lpmode Ethernet100
Port            Low-power Mode
----------  ----------------
Ethernet100   On
```

Display presence of SFP transceiver connected to Ethernet100.

```
admin@sonic:~$ show interfaces transceiver presence Ethernet100
Port            Presence
----------  ----------
Ethernet100   Present
```

Display error status of SFP transceiver connected to Ethernet100.

```
admin@sonic:~$ show interfaces transceiver error-status Ethernet100
Port            Error Status
----------  --------------
Ethernet100   OK
```

1.32 sonic-package-manager install

Function

Run the **sonic-package-manager install** command to pull and installs a package on SONiC host.

Note
This command requires elevated (root) privileges to run.

Syntax

sonic-package-manager install [*OPTIONS*] [*package-expr*]

Parameter Description

OPTIONS:

- --enable:

  Set the default state of the feature to enabled and enable feature right after installation. NOTE: user needs to execute "config save -y" to make this setting persistent.

- --set-owner [local | kube]:

Default owner configuration setting for a feature.

- --from-repository TEXT:

  Fetch package directly from image registry repository.

Note
This argument is mutually exclusive with arguments: [from-tarball, package-expr].

- --from-tarball FILE:

  Fetch package from saved image tarball.

Note
This argument is mutually exclusive with arguments: [package-expr, from-repository].

- -f, --force:

  Force operation by ignoring package dependency tree and package manifest validation failures.

- -y, --yes:

  Automatically answer yes on prompts.

- -v, --verbosity LVL:

  Either CRITICAL, ERROR, WARNING, INFO or DEBUG.

  Default is INFO.

- --skip-host-plugins:

  Do not install host OS plugins provided by the package (CLI, etc).

Note
In case when package host OS plugins are set as mandatory in package manifest this option will fail the installation.

- --allow-downgrade:

  Allow package downgrade. By default an attempt to downgrade the package will result in a failure since downgrade might not be supported by the package, thus requires explicit request from the user.

- --help:

  Show this message and exit..

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo sonic-package-manager install dhcp-relay=1.0.2
```

```
admin@sonic:~$ sudo sonic-package-manager install dhcp-relay@latest
admin@sonic:~$ sudo sonic-package-manager install dhcp-
relay@sha256:9780f6d83e45878749497a6297ed9906c19ee0cc48cc88dc63827564bb8768fd
admin@sonic:~$ sudo sonic-package-manager install --from-repository azure/sonic-cpu-
report:latest
admin@sonic:~$ sudo sonic-package-manager install --from-tarball sonic-docker-image.gz
```

1.33 sonic-package-manager list

Function

Run the **sonic-package-manager list** command to list all available SONiC packages, their description, installed version and installation status.

SONiC package status can be "Installed", "Not installed" or "Built-In". "Built-In" status means that a feature is built-in to SONiC image and can't be upgraded or uninstalled.

Syntax

sonic-package-manager list

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sonic-package-manager list
Name              Repository                    Description                    Version      Status
--------------    ---------------------------   ----------------------------   ---------    ------
--------
cpu-report        azure/cpu-report              CPU report package             N/A          Not
Installed
database          docker-database               SONiC database package         1.0.0        Built-In
dhcp-relay        azure/docker-dhcp-relay       SONiC dhcp-relay package       1.0.0        Installed
fpm-frr           docker-fpm-frr                SONiC fpm-frr package          1.0.0        Built-In
lldp              docker-lldp                   SONiC lldp package             1.0.0        Built-In
macsec            docker-macsec                 SONiC macsec package           1.0.0        Built-
In
mgmt-framework    docker-sonic-mgmt-framework   SONiC mgmt-framework package   1.0.0
Built-In
nat               docker-nat                    SONiC nat package              1.0.0        Built-In
pmon              docker-platform-monitor       SONiC pmon package             1.0.0        Built-In
radv              docker-router-advertiser      SONiC radv package             1.0.0        Built-In
sflow             docker-sflow                  SONiC sflow package            1.0.0        Built-In
snmp              docker-snmp                   SONiC snmp package             1.0.0        Built-In
```

swss	docker-orchagent	SONiC swss package	1.0.0	Built-In
syncd	docker-syncd-mlnx	SONiC syncd package	1.0.0	Built-In
teamd	docker-teamd	SONiC teamd package	1.0.0	Built-In
telemetry	docker-sonic-telemetry	SONiC telemetry package	1.0.0	Built-In

1.34 sonic-package-manager repository add

Function

Run the **sonic-package-manager repository add** command to add a new repository as source for SONiC packages to the database.

Note
This command requires elevated (root) privileges to run.

Syntax

sonic-package-manager repository add [*OPTIONS*] *name repository*

Parameter Description

add: Add a new repository to database.

OPTIONS:

- --default-reference TEXT:

  Default installation reference. Can be a tag or sha256 digest in repository.
- --description TEXT:

  Optional package entry description.
- --help:

  Show this message and exit.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo sonic-package-manager repository add cpu-report azure/sonic-cpu-report --default-reference 1.0.0
```

1.35 sonic-package-manager repository remove

Function

Run the **sonic-package-manager repository remove** command to remove a repository as source for SONiC packages from the database.

The package has to be *Not Installed* in order to be removed from package database.

Note
This command requires elevated (root) privileges to run.

Syntax

sonic-package-manager repository remove [*OPTIONS*] *name*

Parameter Description

remove: Remove repository from database.

OPTIONS:

- --help: Show this message and exit.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo sonic-package-manager repository remove cpu-report
```

1.36 sonic-package-manager reset

Function

Run the **sonic-package-manager reset** command to reset the package by reinstalling it to its default version.

Note
This command requires elevated (root) privileges to run.

Syntax

sonic-package-manager reset [*OPTIONS*] *name*

Parameter Description

reset: Reset package to the default version.

OPTIONS:

- -f, --force:

  Force operation by ignoring package dependency tree and package manifest validation failures.

- -y, --yes:

  Automatically answer yes on prompts.

- -v, --verbosity LVL:

Either CRITICAL, ERROR, WARNING, INFO or DEBUG. Default is INFO.

- --skip-host-plugins Do not install host OS plugins provided by the package (CLI, etc).

Note
In case when package host OS plugins are set as mandatory in package manifest this option will fail the installation.

- --help:

  Show this message and exit.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo sonic-package-manager reset dhcp-relay
```

1.37 sonic-package-manager show package changelog

Function

Run the **sonic-package-manager show package changelog** command to fetches the changelog from the package manifest and displays it.

Note
The package changelog can be retrieved from registry or read from image tarball without installing it.

Syntax

sonic-package-manager show package changelog [*OPTIONS*] [*package-expr*]

Parameter Description

OPTIONS:

- --from-repository TEXT:

  Fetch package directly from image registry repository.

Note
This argument is mutually exclusive with arguments: [from-tarball, package-expr].

- --from-tarball FILE:

  Fetch package from saved image tarball.

Note
This argument is mutually exclusive with arguments: [package-expr, from-repository].

- --help:

  Show this message and exit.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sonic-package-manager show package changelog dhcp-relay
  1.0.0:

    Initial release

      Author (author@email.com) Mon, 25 May 2020 12:25:00 +0300
```

1.38 sonic-package-manager show package manifest

Function

Run the **sonic-package-manager show package manifest** command to fetch the package manifest and displays it.

Note
The package manifest can be retrieved from registry or read from image tarball without installing it.

Syntax

sonic-package-manager show package manifest [*OPTIONS*] [*package-expr*]

Parameter Description

OPTIONS:

- --from-repository TEXT:

  Fetch package directly from image registry repository.

Note
This argument is mutually exclusive with arguments: [from-tarball, package-expr].

- --from-tarball FILE:

  Fetch package from saved image tarball.

Note
This argument is mutually exclusive with arguments: [package-expr, from-repository].

- -v, --verbosity LVL:

  Either CRITICAL, ERROR, WARNING, INFO or DEBUG.

- --help:

  Show this message and exit.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sonic-package-manager show package manifest dhcp-relay=2.0.0
{
  "version": "1.0.0",
  "package": {
    "version": "2.0.0",
    "depends": [
      "database>=1.0.0,<2.0.0"
    ]
  },
  "service": {
    "name": "dhcp_relay"
  }
}
```

1.39 sonic-package-manager show package versions

Function

Run the **sonic-package-manager show package versions** command to retrieve a list of all available versions for the given package from the configured upstream repository.

Syntax

sonic-package-manager show package versions [*OPTIONS*] *name*

Parameter Description

OPTIONS:

- --all:

  Show all available tags in repository.

- --plain:

  Plain output.

- --help:

  Show this message and exit.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sonic-package-manager show package versions dhcp-relay
    1.0.0
    1.0.2
    2.0.0
admin@sonic:~$ sonic-package-manager show package versions dhcp-relay --plain
   1.0.0
   1.0.2
   2.0.0
admin@sonic:~$ sonic-package-manager show package versions dhcp-relay --all
    1.0.0
    1.0.2
    2.0.0
    latest
```

1.40 sonic-package-manager uninstall

Function

Run the **sonic-package-manager uninstall** command to uninstall package from SONiC host. User needs to stop the feature prior to uninstalling it.

Note
This command requires elevated (root) privileges to run.

Syntax

sonic-package-manager uninstall [*OPTIONS*] *NAME*

Parameter Description

uninstall: Uninstall package.

OPTIONS:

- -f, --force:

  Force operation by ignoring package dependency tree and package manifest validation failures.

- -y, --yes:

  Automatically answer yes on prompts.

- -v, --verbosity LVL:
  Either CRITICAL, ERROR, WARNING, INFO or DEBUG. Default is INFO.
- --help:
  Show this message and exit.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo sonic-package-manager uninstall dhcp-relay
```

1 Container Warm Restart Commands

Command	Function
bgp graceful-restart	Enable the function of global BGP graceful restart (GR).
config warm_restart	Enable or disable the warm_restart for a particular service that supports warm reboot.
config warm_restart bgp_timer	Set the bgp_timer value for warm_restart of BGP service.
config warm_restart neighsyncd_timer	Set the neighsyncd_timer value for warm_restart of "swss" service.
config warm_restart teamsyncd_timer	Set the teamsyncd_timer value for warm_restart of teamd service.
show warm_restart config	Display all the configuration related to warm_restart.
show warm_restart state	Display the warm_restart state.
warm reboot	Initiates a warm reboot of the device.

1.1 bgp graceful-restart

Function

Run the **bgp graceful-restart** command to enable the function of global BGP graceful restart (GR).

Note
That during a warm restart, certain BGP fast convergence feature and black hole avoidance feature should either be disabled or be set to a lower preference to avoid conflicts with BGP graceful restart.

Syntax

bgp graceful-restart

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ vtysh
sonic# configure terminal
sonic(config)# router bgp 65000
sonic(config-router)# bgp graceful-restart
Graceful restart configuration changed, reset all peers to take effect
```

1.2 config warm_restart

Function

Run the **config warm_restart** command to enable or disable the warm_restart for a particular service that supports warm reboot.

Syntax

config warm_restart [{ **-s** | **--redis-unix-socket-path** } *socket-path*] { **enable** | **disable** } [*module-name*]

Parameter Description

module-name: Can be either system or swss or bgp or teamd. If "module-name" argument is not specified, it will enable "system" module.

Usage Guidelines

Following four services support warm reboot. When user restarts the particular service using "systemctl restart", this configured value will be checked for whether it is enabled or disabled.

If this configuration is enabled for that service, it will perform warm reboot for that service. Otherwise, it will do cold restart of the service.

Examples

Set warm_restart as "enable" for the "system" service.

```
admin@sonic:~$ sudo config warm_restart enable
```

Set warm_restart as "enable" for the "swss" service. When user does "systemctl restart swss", it will perform warm reboot instead of cold reboot.

```
admin@sonic:~$ sudo config warm_restart enable swss
```

Set warm_restart as "enable" for the "teamd" service. When user does "systemctl restart teamd", it will perform warm reboot instead of cold reboot.

```
admin@sonic:~$ sudo config warm_restart enable teamd
```

Set warm_restart as "enable" for the "syncd" service. When user does "systemctl restart syncd", it will perform warm reboot instead of cold reboot.

```
admin@sonic:~$ sudo config warm_restart enable syncd
```

1.3 config warm_restart bgp_timer

Function

Run the **config warm_restart bgp_timer** command to set the bgp_timer value for warm_restart of BGP service.

Syntax

config warm_restart [{ **-s** | **--redis-unix-socket-path** } *socket-path*] **bgp_timer** *seconds*

Parameter Description

bgp_timer: The parameter is the timer used for “bgp” service during the warm restart.

seconds: Range from 1 to 3600.

Usage Guidelines

Timer is started after the BGP table is restored to internal data structures. BGP services then start to read all Linux kernel entries and mark the entries in the data structures accordingly. Once the timer is expired, reconciliation is done and the delta is pushed to appDB Valid value is 1-3600. 0 is invalid.

Examples

```
admin@sonic:~$ sudo config warm_restart bgp_timer 2000
```

1.4 config warm_restart neighsyncd_timer

Function

Run the **config warm_restart neighsyncd_timer** command to set the neighsyncd_timer value for warm_restart of "swss" service.

Syntax

config warm_restart [{ **-s** | **--redis-unix-socket-path** } *socket-path*]
neighsyncd_timer *seconds*

Parameter Description

seconds: Range from 1 to 9999.

Usage Guidelines

The neighsyncd_timer is the timer used for "swss" (neighsyncd) service during the warm restart.

Timer is started after the neighborTable is restored to internal data structures.

neighborsyncd then starts to read all Linux kernel entries and mark the entries in the data structures accordingly.

Once the timer is expired, reconciliation is done and the delta is pushed to appDB.

Examples

```
admin@sonic:~$ sudo config warm_restart neighsyncd_timer 2000
```

1.5 config warm_restart teamsyncd_timer

Function

Run the **config warm_restart teamsyncd_timer** command to set the teamsyncd_timer value for warm_restart of teamd service.

Syntax

config warm_restart [{ **-s**| **--redis-unix-socket-path** } *socket-path*]
teamsyncd_timer *seconds*

Parameter Description

teamsyncd_timer: teamsyncd_timer holds the time interval utilized by teamsyncd during warm-restart episodes.

seconds: Range from 1 to 3600.

Usage Guidelines

The timer is started when teamsyncd starts. During the timer interval, teamsyncd will preserve all LAG interface changes, but it will not apply them. The changes will only be applied when the timer expires. When the changes are applied, the stale LAG entries will be removed, the new LAG entries will be created. Supported range: 1-3600. 0 is invalid.

Examples

```
admin@sonic:~$ sudo config warm_restart teamsyncd_timer 3000
```

1.6 show warm_restart config

Function

Run the **show warm_restart config** command to display all the configuration related to warm_restart.

Syntax

show warm_restart config

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show warm_restart config
    name         enable         timer_name         timer_duration         eoiu_enable
    ------    --------    ------------    ----------------    -------------
    bgp           true             NULL                   NULL                          NULL
    swss         true            NULL                  NULL                         NULL
    syncd       true           NULL                 NULL                        NULL
    teamd       true            NULL                   NULL                          NULL
```

1.7 show warm_restart state

Function

Run the **show warm_restart state** command to display the warm_restart state.

Syntax

show warm_restart state

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show warm_restart state
    name                        restore_count     state
    ----------     ---------------     ----------
    bgp                                       1     reconciled
    fdbsyncd                                  2     replayed
    intfmgrd                                  2     reconciled
    neighsyncd                                2     reconciled
    orchagent                                 2     reconciled
    portsyncd                                 2     reconciled
    syncd                                     1     reconciled
    teamsyncd                                 1     reconciled
    vlanmgrd                                  2     reconciled
    vrfmgrd                                   2     reconciled
    vxlanmgrd                                 2     reconciled
```

1.8 warm reboot

Function

Run the **warm reboot** command to initiates a warm reboot of the device.

Syntax

warm-reboot [**-h** | **-?** | **-v** | **-f** | **-I** | **-d** | **-r** | **-k** | **-x** | **-c** *control plane assistant IP list* | **-s** | **-t** | **-D**]

Parameter Description

-h,**-?** : get this help

-v: turn on verbose mode

-f: force execution - ignore Orchagent RESTARTCHECK failure

-i: force execution - ignore ASIC MD5-checksum-verification

-d: force execution - ignore database integrity check

-r: reboot with /sbin/reboot

-k: reboot with /sbin/kexec -e [default]

-x: execute script with -x flag

-c: specify control plane assistant IP list

-s: strict mode: do not proceed without:

control plane assistant IP list.

-t: Don't tag the current kube images as latest

-D: detached mode - closing terminal will not cause stopping reboot

Usage Guidelines

Warm-reboot command doesn't require setting warm restart configuration. The

Command will setup everything needed to perform warm reboot.

This command requires root privilege.

Examples

```
admin@sonic:~$ sudo warm-reboot -v
    Mon 20 Mar 2023 09:55:11 AM UTC Saving counters folder before warmboot...
    Mon 20 Mar 2023 09:55:15 AM UTC Pausing orchagent ...
    Mon 20 Mar 2023 09:55:15 AM UTC Collecting logs to check ssd health before warm-reboot...
    Mon 20 Mar 2023 09:55:15 AM UTC Stopping lldp.timer ...
    Mon 20 Mar 2023 09:55:15 AM UTC Stopped lldp.timer ...
    Mon 20 Mar 2023 09:55:15 AM UTC Stopping mgmt-framework.timer ...
    Mon 20 Mar 2023 09:55:15 AM UTC Stopped mgmt-framework.timer ...
    Mon 20 Mar 2023 09:55:15 AM UTC Stopping pmon.timer ...
    Mon 20 Mar 2023 09:55:15 AM UTC Stopped pmon.timer ...
    Mon 20 Mar 2023 09:55:15 AM UTC Stopping snmp.timer ...
    Mon 20 Mar 2023 09:55:15 AM UTC Stopped snmp.timer ...
    Mon 20 Mar 2023 09:55:15 AM UTC Stopping telemetry.timer ...
    Mon 20 Mar 2023 09:55:15 AM UTC Stopped telemetry.timer ...
    Mon 20 Mar 2023 09:55:15 AM UTC Stopping lldp ...
    Mon 20 Mar 2023 09:55:17 AM UTC Stopped lldp
    Mon 20 Mar 2023 09:55:17 AM UTC Stopping radv ...
    Mon 20 Mar 2023 09:55:17 AM UTC Stopped radv
    Mon 20 Mar 2023 09:55:17 AM UTC Stopping bgp ...
    Mon 20 Mar 2023 09:55:22 AM UTC Stopped bgp
    Mon 20 Mar 2023 09:55:22 AM UTC Stopping swss ...
    Mon 20 Mar 2023 09:55:29 AM UTC Stopped swss
    Mon 20 Mar 2023 09:55:29 AM UTC Initialize pre-shutdown ...
    Mon 20 Mar 2023 09:55:30 AM UTC Requesting pre-shutdown ...
    Mon 20 Mar 2023 09:55:30 AM UTC Waiting for pre-shutdown ...
    Mon 20 Mar 2023 09:55:30 AM UTC Pre-shutdown succeeded, state: pre-shutdown-succeeded ...
    Mon 20 Mar 2023 09:55:30 AM UTC Backing up database ...
    Mon 20 Mar 2023 09:55:31 AM UTC Stopping teamd ...
    Mon 20 Mar 2023 09:55:31 AM UTC Stopped teamd
    Mon 20 Mar 2023 09:55:31 AM UTC Stopping syncd ...
    Mon 20 Mar 2023 09:55:41 AM UTC Stopped syncd
    Mon 20 Mar 2023 09:55:41 AM UTC Stopping all remaining containers ...
    Mon 20 Mar 2023 09:55:44 AM UTC Stopped all remaining containers ...
    Mon 20 Mar 2023 09:55:46 AM UTC Enabling Watchdog before warm-reboot
```

```
    Mon 20 Mar 2023 09:55:46 AM UTC Rebooting with /sbin/kexec -e to SONiC-OS-
SONiC_1.3.0_20230320003403 ...
```

1 Ethernet Interface Commands

Command	Function
config interface advertised-speeds	Set port advertised speed.
config interface arp	Configure the ARP aging time and gratuitous ARP.
config interface autoneg	Set port auto negotiation mode.
config interface breakout	Set active breakout mode available for user-specified interface based on the platform-specific port configuration file(i.e. platform.json) and the current mode set for the interface.
config interface carrier_delay	Set the carrier-delay time for a specified interface.
config interface description	Set the description for a specified interface.
config interface error_down	Recover the interface link status.
config interface fastlink	Enable or disable fastlink.
config interface fec	Set the fec mode for a specified interface.
config interface fec-bypass	Configure interface fec-bypass mode.
config interface ip add	Add the IP address for an interface.
config interface ip remove	Remove the IP address for an interface.
config interface ipv6 enable use-link-local-only	Enable an interface to forward L3 traffic with out configuring an address. This command creates the routing interface based on the auto generated IPv6 link-local address. This command can be used even if an address is configured on the interface.
config interface ipv6 disable use-link-local-only	Disable use-link-local-only configuration on an interface.
config interface ip-statistics	Enable or disable the IP packet counter specific to the interface.

config interface lacp-port-priority	Set the LACP port priority for a specified interface.
config interface link_dither	Disable an interface when flapping occurs.
config interface mediatype	Set the media type for a specified interface.
config interface mpls add	Add MPLS operation on the interface.
config interface mpls remove	Remove MPLS operation on the interface.
config interface mtu	Configure the mtu for the Physical interface. Use the value 1500 for setting max transfer unit size to 1500 bytes.
config interface pfc asymmetric	Set the asymmetric PFC for an interface to either "on" or "off".
config interface pfc priority	Set PFC on a given priority of a given interface to either "on" or "off". Once it is successfully configured, it will show current losses priorities on the given interface. Otherwise, it will show error information.
config interface shutdown	Administratively shut down either the Physical interface or port channel interface. Once if it is configured, use "show interfaces status" to check the same.
config interface speed	Configure the speed for the Physical interface.
config interface startup	Administratively bringing up the Physical interface or port channel interface.
config interface storm_control	Configure storm control for a specified interface.
config interface switchmode	Configure the switchport mode.
config interface tpid	Configure the TPID for the Physical/PortChannel interface.
config interface transceiver lpmode	Enable or disable low-power mode for an SFP transceiver.
config interface transceiver reset	Reset an SFP transceiver.

config interface_naming_mode	Change the interface naming mode.
config ipv6 enable link-local	Enable use-link-local-only command on all the interfaces globally.
config ipv6 disable link-local	Disable use-link-local-only command on all the interfaces globally.
config loopback	Add or delete loopback interfaces.
config subinterface	Add or delete loopback interfaces.
show subinterfaces status	Display all the subinterfaces that are configured on the device and its current status.
show interfaces alias	Display name and alias of the interface. For a single interface, provide the interface name with the sub-command.
show interfaces autoneg	Display name and alias of the interface. For a single interface, provide the interface name with the sub-command.
show interfaces breakout	Display the port capability for all interfaces i.e. index, lanes, default_brkout_mode, breakout_modes(i.e. available breakout modes) and brkout_mode (i.e. current breakout mode). To display current breakout mode, "current-mode" subcommand can be used.For a single interface, provide the interface name with the sub-command.
show interfaces counters	Display packet counters for all interfaces since the last time the counters were cleared. To display l3 counters "rif" subcommand can be used. There is no facility to display counters for one specific l2 interface. For l3 interfaces a single interface output mode is present. Optional argument "-a" provides two additional columns - RX-PPS and TX_PPS.
show interfaces description	Display the key fields of the interfaces such as Operational Status, Administrative Status, Alias and Description.
show interfaces errdisable	Display the error disable information such as status and reason.

show interfaces fec-bypass	Displays the configuration of interfaces fec-bypass mode.
show interfaces info	Display the interface information such as description, status, line protocol status, MAC address, speed, bandwidth, admin FEC, oper FEC, MTU, interface IP address, interface IPv6 address, VLAN, link up delay, link down delay, and statistics.
show interfaces ip-statisitcs	Display the status of IP packet counter specific to the interface.
show interfaces media	Display the interface media type.
show interfaces mpls	Display the configured MPLS state for the list of configured interfaces.
show interfaces naming_mode	Display the current interface naming mode.
show interfaces neighbor	Display the list of expected neighbors for all interfaces (or for a particular interface) that is configured.
show interfaces portchannel	Display information regarding port-channel interfaces.
show interfaces status	Display some more fields such as Lanes, Speed, MTU, Type, Asymmetric PFC status and also the operational and administrative status of the interfaces.
show interfaces storm_control	Display broadcast, multicast, and unicast storm control configuration.
show interfaces tpid	Display the key fields of the interfaces such as Operational Status, Administrative Status, Alias and TPID.
show interfaces transceiver	Explain here.
show interfaces vlan-info	Display VLAN interface configuration.
show ipv6 link-local-mode	Display the link local mode of all the interfaces.

1.1 config interface advertised-speeds

Function

Run the **config interface advertised-speeds** command to set port advertised speed.

Syntax

sudo config interface advertised-speeds *interface-name speed-list*

Parameter Description

interface_name: Interface name, for example, Ethernet1

speed_list: Auto-negotiation advertising speed list

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface advertised-speeds Ethernet0 all
admin@sonic:~$ sudo config interface advertised-speeds Ethernet0 50000,100000
```

1.2 config interface arp

Function

Run the **config interface arp** command to configure the ARP aging time and gratuitous ARP.

Syntax

config interface arp { **adv-gratuitous** { **disable** | **enable** } | **adv-gratuitous-interval** *interval* | **gratuitous** { **disable** | **enable** } | **reachable-time** *reachable-time* | **stale-time** *stale-time* }

Parameter Description

adv-gratuitous: Enable/Disable advertising gratuitous_arp to the interface

adv-gratuitous-interval *interval*: Set advertising gratuitous_arp interval time to the interface

gratuitous: Enable/Disable gratuitous_arp to the interface

reachable-time *reachable-time*: Add arp reachable_time to the interface

stale-time *stale-time*: Add arp aging_time to the interface

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface arp adv-gratuitous Ethernet22 enabled
admin@sonic:~$ sudo config interface arp adv-gratuitous-interval Ethernet22 10
admin@sonic:~$ sudo config interface arp gratuitous Ethernet22 enabled
admin@sonic:~$ sudo config interface arp reachable-time Ethernet30 1800
admin@sonic:~$ sudo config interface arp stale-time Ethernet30 60
```

1.3 config interface autoneg

Function

Run the **config interface autoneg** command to set port auto negotiation mode.

Syntax

sudo config interface autoneg *interface-name mode*

Parameter Description

interface_name: Interface name, for example, Ethernet1

mode: disabled or enabled

Usage Guidelines

NOTE:

- The product M2-W6920-4S uses an external PHY and does not support the specified port auto-negotiation capability.
- When using copper cables for ports with a speed greater than 25G, it is recommended to enable auto-negotiation. After enabling the auto-negotiation function, you need to set the interface media type to copper at the same time.

Examples

```
admin@sonic:~$ sudo config interface autoneg Ethernet0 enabled
admin@sonic:~$ sudo config interface autoneg Ethernet0 disabled
```

1.4 config interface breakout

Function

Run the **config interface breakout** command to set active breakout mode available for user-specified interface based on the platform-specific port configuration file(i.e. platform.json) and the current mode set for the interface.

Syntax

sudo config interface breakout *interface-name mode* [**-f**] [**-l**] [**-y**] [**-v**]

Parameter Description

interface_name: Interface name, for example, Ethernet1

mode: Breakout modes supported by the interface

Usage Guidelines

NOTE**:**

- Port split support details can be viewed through the “show interface breakout” command
- In the scenario of enabling ZTP, the port cannot be split, because the splitting configuration is not loaded into the database. You need to disable ZTP before splitting the port.
- Port splitting will delete the port and then create it, so the newly created port will lack the configuration of certain services bound to the port when the device is powered on. You are advised to run the “sudo config save -y” command to save the configuration, then restart the device and rebind the startup configuration to the split port.
- Splitting an interface will remove its associated configuration. It requires reconfiguration after the split is successful.

Examples

```
admin@sonic:~$ sudo config interface breakout Ethernet0 <tab><tab>
<tab provides option for breakout mode>
1x100G[40G]    2x50G          4x25G[10G]
This command also provides "--force-remove-dependencies/-f" option to CLI, which will
automatically determine and remove the configuration dependencies using Yang models.
admin@sonic:~$ sudo config interface breakout    Ethernet0 4x25G[10G] -f -l -v -y
```

1.5 config interface carrier_delay

Function

Run the **config interface carrier_delay** command to set the carrier-delay time for a specified interface.

Syntax

config interface carrier_delay { **down** | **up** } *interface-name delay-time*

Parameter Description

down: set interface down delay time

up: set interface up delay time

interface-name: Interface name, for example, Ethernet1

delay-time: Delay time

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface carrier_delay down Ethernet22 100
admin@sonic:~$ sudo config interface carrier_delay up Ethernet22 100
```

1.6 config interface description

Function

Run the **config interface description** command to set the description for a specified interface.

Syntax

config interface description *interface-name description*

Parameter Description

interface-name: Interface name, for example, Ethernet1

description: Interface description

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface description Ethernet44 "Example"
```

1.7 config interface error_down

Function

Run the **config interface error_down** command to recover the interface link status.

Syntax

config interface error_down { **auto_recovery** [**disable** | **enable** | **interval** *interval*]| **recovery link_dither** }

Parameter Description

auto_recovery: rror down auto_recovery configuration

recovery: Error down recovery configuration

interval *interval*: Errdisable recovery interval

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface error_down auto_recovery enable
admin@sonic:~$ sudo config interface error_down auto_recovery disable
admin@sonic:~$ sudo config interface error_down auto_recovery interval 100
admin@sonic:~$ sudo config interface error_down recovery link_dither
```

1.8 config interface fastlink

Function

Run the **config interface fastlink** command to enable or disable fastlink.

Syntax

config interface fastlink { **disable** | **enable** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo cconfig interface fastlink enable
admin@sonic:~$ sudo config interface fastlink disable
```

1.9 config interface fec

Function

Run the **config interface fec** command to set the fec mode for a specified interface.

Syntax

config interface fec *interface-name* [**fc** | **none** | **rs**]

Parameter Description

interface-name: Interface name, for example, Ethernet1

Usage Guidelines

NOTE:

- The fec configuration command cannot specify a specific RS type. The device will match the RS-FEC mode based on the port type.

- In product M2-W6930-64QC-R0, when the port speed is reduced to 40G, the port fec only supports configuration of none.

Examples

```
admin@sonic:~$ sudo config interface fec Ethernet23 rs
```

1.10 config interface fec-bypass

Function

Run the **config interface fec-bypass** command to configure interface fec-bypass mode.

Syntax

config interface fec-bypass *interface_name* { **enable** | **disable** }

Parameter Description

interface-name: Interface name, for example, Ethernet1

Usage Guidelines

Support products: M2-W6510-48V8C、M2-W6510-32C、M2-W6920、M2-W6510-48GT4V、M2-W6920-32QC2X

Examples

```
admin@sonic:~$ sudo config interface fec-bypass Ethernet1 enable
```

1.11 config interface ip add

Function

Run the **config interface ip add** command to add the IP address for an interface.

IP address for either physical interface or for portchannel or for VLAN interface or for Loopback interface can be configured using this command. While configuring the IP address for the management interface "eth0", users can provide the default gateway IP address as an optional parameter from release 201911.

Syntax

config interface ip add [*interface-name*] [*ip-addr/mask*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface ip add Ethernet63 10.11.12.13/24
admin@sonic:~$ sudo config interface ip add eth0 20.11.12.13/24 20.11.12.254
```

1.12 config interface ip remove

Function

Run the **config interface ip remove** command to remove the IP address for an interface.

IP address for either physical interface or for portchannel or for VLAN interface or for Loopback interface can be configured using this command. While configuring the IP address for the management interface "eth0", users can provide the default gateway IP address as an optional parameter from release 201911.

Syntax

config interface ip remove [*interface-name*] [*ip-addr/mask*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface ip remove Ethernet63 10.11.12.13/24
admin@sonic:~$ sudo config interface ip remove eth0 20.11.12.13/24
```

1.13 config interface ipv6 enable use-link-local-only

Function

Run the **config interface ipv6 enable use-link-local-only** command to enable an interface to forward L3 traffic with out configuring an address. This command creates the routing interface based on the auto generated IPv6 link-local address. This command can be used even if an address is configured on the interface.

Syntax

config interface ipv6 enable use-link-local-only [*interface-name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface ipv6 enable use-link-local-only Vlan206
admin@sonic:~$ sudo config interface ipv6 enable use-link-local-only PortChannel007
admin@sonic:~$ sudo config interface ipv6 enable use-link-local-only Ethernet52
```

1.14 config interface ipv6 disable use-link-local-only

Function

Run the **config interface ipv6 disable use-link-local-only** command to disable use-link-local-only configuration on an interface.

Syntax

config interface ipv6 disable use-link-local-only [*interface-name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface ipv6 disable use-link-local-only Vlan206
admin@sonic:~$ sudo config interface ipv6 disable use-link-local-only PortChannel007
admin@sonic:~$ sudo config interface ipv6 disable use-link-local-only Ethernet52
```

1.15 config interface ip-statistics

Function

Run the **config interface ip-statistics** command to enable or disable the IP packet counter specific to the interface.

Syntax

config interface ip-statistics { *interface-name* | **all** } { **disable** | **enable** }

Parameter Description

interface_name: Interface name, for example, Ethernet1

all: All interfaces

Usage Guidelines

NOTE:

- In products M2-W6930-64QC、M2-W6920-32QC2X and M2-W6510-48GT4C, for multicast and broadcast messages without layer 3 headers, the chip cannot count the

corresponding registers, and the counting statistics are incorrect.

- In products M2-W6930-64QC、M2-W6920-32QC2X and M2-W6510-48GT4C, export MTU statistics do not take effect.
- The IP traffic statistics function uses ACL resources. Configuring the IP traffic statistics function may cause the ACL capacity resources to be full, affecting ACL business functions. If necessary, you can release ACL resources by disabling the IP traffic statistics function.

Examples

```
admin@sonic:~$ sudo config interface ip-statistics all enable
admin@sonic:~$ sudo config interface ip-statistics Ethernet12 enable
admin@sonic:~$ sudo config interface ip-statistics Ethernet12 disable
```

1.16 config interface lacp-port-priority

Function

Run the **config interface lacp-port-priority** command to set the LACP port priority for a specified interface.

Syntax

config interface lacp-port-priority [**-v**]*interface-name priority*

Parameter Description

-v: Enable verbose output

interface_name: Interface name, for example, Ethernet1

priority: Member interface priority negotiated through LACP

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface lacp-port-priority Ethernet44 1000
```

1.17 config interface link_dither

Function

Run the **config interface link_dither** command to disable an interface when flapping occurs.

Syntax

config interface link_dither { **disable** | **enable** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface link_dither disable
admin@sonic:~$ sudo config interface link_dither enable
```

1.18 config interface mediatype

Function

Run the **config interface mediatype** command to set the media type for a specified interface.

Syntax

config interface mediatype *interface-name mediatype*

Parameter Description

-v: Enable verbose output

interface_name: Interface name, for example, Ethernet1

mediatype: Media types supported by the interface

Usage Guidelines

NOTE:

- If the configured media type is inconsistent with the actual access type, the interface will become unavailable.
- In product M2-W6510-48GT4V, if the port is connected to a copper cable, currently only copper cables within 3M can be guaranteed to work normally, and copper cables exceeding 3M cannot be guaranteed to work properly.

Examples

```
admin@sonic:~$ sudo config interface mediatype Ethernet44 fiber
```

1.19 config interface mpls add

Function

Run the **config interface mpls add** command to add MPLS operation on the interface.

MPLS operation for either physical, portchannel, or VLAN interface can be configured using this command.

Syntax

sudo config interface mpls add *interface-name*

Parameter Description

interface_name: Interface name, for example, Ethernet1

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface mpls add Ethernet4
```

1.20 config interface mpls remove

Function

Run the **config interface mpls remove** command to remove MPLS operation on the interface.

MPLS operation for either physical, portchannel, or VLAN interface can be configured using this command.

Syntax

sudo config interface mpls remove *interface-name*

Parameter Description

interface_name: Interface name, for example, Ethernet1

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface mpls remove Ethernet4
```

1.21 config interface mtu

Function

Run the **config interface mtu** command to configure the mtu for the Physical interface. Use the value 1500 for setting max transfer unit size to 1500 bytes.

Syntax

config interface mtu [*interface-name*] [mtu]

Parameter Description

interface_name: Interface name, for example, Ethernet1

mtu: MTU value, valid range [68, 9216]

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface mtu Ethernet64 1500
```

1.22 config interface pfc asymmetric

Function

Run the **config interface pfc asymmetric** command to set the asymmetric PFC for an interface to either "on" or "off".

Once if it is configured, use "show interfaces status" to check the same.

Syntax

config interface pfc asymmetric [*interface-name*] { **on** | **off** }

Parameter Description

interface-name: Interface name, for example, Ethernet1.

on | **off**: Asymmetric PFC is enabled or disabled

Usage Guidelines

NOTE:

- When the asymmetric PFC mode is enabled on an interface, the PFC function is enabled for all queues at the ingress of the interface and whether it is enabled at the egress depends on the bitmap.
- When the asymmetric PFC mode is disabled on an interface, the PFC function can be enabled at the ingress and egress of the interface based on the configuration.

Examples

```
admin@sonic:~$ sudo config interface pfc asymmetric Ethernet60 on
```

1.23 config interface pfc priority

Function

Run the **config interface pfc priority** command to set PFC on a given priority of a given interface to either "on" or "off". Once it is successfully configured, it will show current losses priorities on the given interface. Otherwise, it will show error information.

Syntax

config interface pfc priority [*interface-name*] *priority* { **on** | **off** }

Parameter Description

interface-name: Interface name, for example, Ethernet1.

priority: PFC priority, valid range 0~7

on | **off**: PFC priority is enabled or disabled

Usage Guidelines

NOTE:

- If PFC priority is disabled on a PFC-enabled interface, PFC frames received by the interface will not be counted.
- When the PFC sampling period is set to 1 second, it will result in a significant error in PFC frame rate counting.
- When the interface rate changes, the PFC counters of the corresponding interface are cleared.
- Interface queue priority takes effect only after tc-to-queue mapping is configured for QoS.
- The priorities of the PFC-enabled interfaces in the inbound direction apply to all interfaces. For example: Configuration: Interface A: 1; Interface B: 2, 3; Interface C: 3, 4; Interface D: N/A Actual value: Interfaces A, B, and C: 1, 2, 3, 4; Interface D: N/A
- Before configuring PFC for a priority group on an interface, enable tc-to-pg mapping and apply it on the interface. Command for configuring tc-to-pg mapping: sudo config qos map add tc-to-pg tc-to-pg-name tc-value pg-value Command for applying tc-to-pg mapping to a port: sudo config qos map apply tc-to-pg interface-name tc-to-pg-name

Examples

```
admin@sonic:~$ sudo config interface pfc priority Ethernet0 3 off
Interface          Lossless priorities
-----------   ---------------------
Ethernet0                          4
admin@sonic:~$ sudo config interface pfc priority Ethernet0 8 off
Usage: pfc config priority [OPTIONS] STATUS INTERFACE PRIORITY
Error: Invalid value for "priority": invalid choice: 8. (choose from 0, 1, 2, 3, 4, 5, 6, 7)
admin@sonic:~$ sudo config interface pfc priority Ethernet101 3 off
Cannot find interface Ethernet101
admin@sonic:~$ sudo config interface pfc priority Ethernet0 3 on
Interface       Lossless priorities
-----------   ---------------------
Ethernet0       3,4
```

1.24 config interface shutdown

Function

Run the **config interface shutdown** command to administratively shut down either the Physical interface or port channel interface. Once if it is configured, use "show interfaces status" to check the same.

Syntax

config interface shutdown [*interface-name*] { **on** | **off** }

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface shutdown Ethernet63
```

1.25 config interface speed

Function

Run the **config interface speed** command to configure the speed for the Physical interface.

Use the value 40000 for setting it to 40G and 100000 for 100G. Users need to know the device to configure it properly.

Syntax

config interface speed [*interface-name*] [*speed_value*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

speed_value: Speed supported by the interface

Usage Guidelines

NOTE: - In products M2-W6510-32C and M2-W6510-48V8C, when the product configures the speed of the 25G interface, it will change the speed of four adjacent 25G interfaces at the same time. If there are members of the aggregate interface among the four adjacent 25G interfaces, the speed configuration will not take effect. - In product M2-W6920-4S, when the product configures the interface speed, it will change the speed of four adjacent interfaces at the same time. If there are members of the aggregate interface among the four adjacent interfaces, the speed configuration cannot take effect. - In products M2-W6510-32C、M2-W6510-48V8C、M2-W6920-4S、M2-W6930-64QC and M2-W6520-24DC8QC, changing the speed will clear the port queue statistics. - In products M2-W6520-24DC8QC、M2-W6920-32QC2X and M2-W6930-64QC, configuring speed reduction will

reduce the number of lanes. For the actual number of lanes, refer to the Lns display content in bcmcmd ps.

Examples

```
admin@sonic:~$ sudo config interface speed Ethernet63 40000
```

1.26 config interface startup

Function

Run the **config interface startup** command to administratively bringing up the Physical interface or port channel interface.

Once it is configured, use "show interfaces status" to check the same.

Syntax

config interface startup [*interface-name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface startup Ethernet63
```

1.27 config interface storm_control

Function

Run the **config interface storm_control** command to configure storm control for a specified interface.

Syntax

config interface storm_control [*interface_name*] { **broadcast** | **multicast** | **unicast** } { kbps | level | pps } storm_value

Parameter Description

interface-name: Interface name, for example, Ethernet1.

broadcast: broadcast storm control

multicast: Multicast storm control

unicast: Unicast storm control

kbps: Enter suppression level in Mbits/sec

level: Set storm suppression level on this interface

pps: Suppression level in packets per second

storm_value: Storm control value

Usage Guidelines

In products M2-W6930-64QC and M2-W6920-32QC2X, port storm control is implemented using the ACL solution. After configuring the command, the chip will reserve resources for the storm control function and cannot be used when the ACL resources are full. In the scenario of using ACL, you need to judge whether you need to use this function based on the ACL resources.

Examples

```
admin@sonic:~$ sudo config interface storm_control Ethernet44 broadcast kbps 1214
admin@sonic:~$ sudo config interface storm_control Ethernet43 broadcast level 20
admin@sonic:~$ sudo config interface storm_control Ethernet42 broadcast pps 1214
```

1.28 config interface switchmode

Function

Run the **config interface switchmode** command to configure the switchport mode.

Syntax

config interface switchmode { **access** *vlan-id* | **no-access** | **no-trunk** | **trunk** { **no-vlan-range** *no-vlan-range* | **pvid** *vlan-id* | **vlan-range** *vlan-list* } } *interface-name*

Parameter Description

access: Set interface access mode.

vlan-id: VLAN ID, for example, 20.

no-access: Set interface default access mode.

no-trunk: Remove interface all trunk configuration.

trunk: Set interface trunk mode.

no-vlan-range: Remove interface tagged vlan.

no-vlan-range: List of VLANs that the interface needs to exit

pvid: Set interface trunk mode native vlan.

vlan-range: Set interface tagged vlan.

vlan-range: List of VLANs to which the interface will be added

interface-name: Interface name, for example, Ethernet1

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface switchmode access 100 Ethernet22
admin@sonic:~$ sudo config interface switchmode no-access Ethernet22
admin@sonic:~$ sudo config interface switchmode trunk pvid 20 Ethernet22
admin@sonic:~$ sudo config interface switchmode trunk vlan-range 100-104 Ethernet22
admin@sonic:~$ sudo config interface switchmode trunk no-vlan-range 100-101 Ethernet22
admin@sonic:~$ sudo config interface switchmode no-trunk Ethernet22
```

1.29 config interface tpid

Function

Run the **config interface tpid** command to configure the TPID for the Physical/PortChannel interface.

Default is 0x8100. Other allowed values if supported by HW SKU (0x9100, 0x9200, 0x88A8).

Syntax

config interface tpid [*interface_name*] [*tpid_value*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

tpid_value: TPID value

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface tpid Ethernet64 0x9200
```

1.30 config interface transceiver lpmode

Function

Run the **config interface transceiver lpmode** command to enable or disable low-power mode for an SFP transceiver.

Syntax

- **config interface transceiver lpmode** [*interface-name*] { **enable** | **disable** }

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
user@sonic~$ sudo config interface transceiver lpmode Ethernet0 enable
Enabling low-power mode for port Ethernet0...  OK
user@sonic~$ sudo config interface transceiver lpmode Ethernet0 disable
Disabling low-power mode for port Ethernet0...  OK
```

1.31 config interface transceiver reset

Function

Run the **config interface transceiver reset** command to reset an SFP transceiver.

Syntax

config interface transceiver reset [*interface-name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface transceiver reset Ethernet0
```

1.32 config interface_naming_mode

Function

Run the **config interface_naming_mode** command to change the interface naming mode.

Users can select between default mode (SONiC interface names) or alias mode (Hardware vendor names). The user must log out and log back in for changes to take effect. Note that the newly-applied interface mode will affect all interface-related show/config commands.

Syntax

config interface_naming_mode { **default** | **alias** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces naming_mode
default

admin@sonic:~$ show interface status Ethernet0
  Interface       Lanes      Speed      MTU              Alias      Oper      Admin
-----------  --------  -------  -----  ---------------  ------  -------
  Ethernet0    101,102        40G     9100    fortyGigE1/1/1        up          up

admin@sonic:~$ sudo config interface_naming_mode alias
Please logout and log back in for changes take effect.
```

- After user logs out and logs back in again, interfaces will then referenced by hardware vendor aliases:

```
admin@sonic:~$ show interfaces naming_mode
alias

admin@sonic:~$ sudo config interface fortyGigE1/1/1 shutdown
admin@sonic:~$ show interface status fortyGigE1/1/1
  Interface       Lanes      Speed      MTU              Alias      Oper      Admin
-----------  --------  -------  -----  ---------------  ------  -------
  Ethernet0    101,102        40G     9100    fortyGigE1/1/1      down       down
```

1.33 config ipv6 enable link-local

Function

Run the **config ipv6 enable link-local** command to enable use-link-local-only command on all the interfaces globally.

Syntax

sudo config ipv6 enable link-local

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config ipv6 enable link-local
```

1.34 config ipv6 disable link-local

Function

Run the **config ipv6 disable link-local** command to disable use-link-local-only command on all the interfaces globally.

Syntax

sudo config ipv6 disable link-local

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config ipv6 disable link-local
```

1.35 config loopback

Function

Run the **config loopback** command to add or delete loopback interfaces.

Syntax

config loopback { **add** | **del** } *loopback-name*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

Create the loopback with name "Loopback11"

```
admin@sonic:~$ sudo config loopback add Loopback11
```

1.36 config subinterface

Function

Run the **config subinterface** command to add or delete loopback interfaces.

Syntax

config subinterface { **add** | **del** } *subinterface-name* [*vlan-id*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

Create the subinterfces with name "Ethernet0.100"

```
admin@sonic:~$ sudo config subinterface add Ethernet0.100
```

Create the subinterfces with name "Eth64.100"

```
admin@sonic:~$ sudo config subinterface add Eth64.100 100
```

Delete the subinterfces with name "Ethernet0.100"

```
admin@sonic:~$ sudo config subinterface del Ethernet0.100
```

Delete the subinterfces with name "Eth64.100"

```
admin@sonic:~$ sudo config subinterface del Eth64.100 100
```

1.37 show subinterfaces status

Function

Run the **show subinterfaces status** command to display all the subinterfaces that are configured on the device and its current status.

Syntax

show subinterfaces status

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show subinterfaces status
Sub port interface    Speed     MTU     Vlan     Admin                    Type
------------------  -------  -----  ------  -------  --------------------
      Eth64.10          100G    9100     100       up   dot1q-encapsulation
      Ethernet0.100     100G    9100     100       up   dot1q-encapsulation
```

1.38 show interfaces alias

Function

Run the **show interfaces alias** command to display name and alias of the interface. For a single interface, provide the interface name with the sub-command.

Syntax

show interfaces alias

show interfaces alias [*interface-name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces alias
Name            Alias
----------   ------------------
Ethernet1    twentyfiveGigE0/1
Ethernet2    twentyfiveGigE0/2
Ethernet3    twentyfiveGigE0/3
Ethernet4    twentyfiveGigE0/4
Ethernet5    twentyfiveGigE0/5
Ethernet6    twentyfiveGigE0/6
Ethernet7    twentyfiveGigE0/7

admin@sonic:~$ show interfaces alias Ethernet54
Name            Alias
----------   --------------
Ethernet54   hundredGigE0/6
```

1.39 show interfaces autoneg

Function

Run the **show interfaces autoneg** command to display name and alias of the interface. For a single interface, provide the interface name with the sub-command.

Syntax

show interfaces autoneg status [*interface_name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces autoneg status
    Interface      Auto-Neg Mode      Speed      Adv Speeds      Type      Adv Types      Oper      Admin
-----------  ---------------  -------  ------------  ------  -----------  ------  -------
    Ethernet0            enabled       25G         10G,25G        CR          CR,CR4        up          up
    Ethernet4           disabled      100G              all       CR4            all         up          up

  admin@sonic:~$ show interfaces autoneg status Ethernet8
    Interface      Auto-Neg Mode      Speed      Adv Speeds      Type      Adv Types      Oper      Admin
-----------  ---------------  -------  ------------  ------  -----------  ------  -------
    Ethernet8           disabled      100G               N/A       CR4            N/A         up          up
```

1.40 show interfaces breakout

Function

Run the **show interfaces breakout** command to display the port capability for all interfaces i.e. index, lanes, default_brkout_mode, breakout_modes(i.e. available breakout modes) and brkout_mode (i.e. current breakout mode). To display current breakout mode, "current-mode" subcommand can be used.For a single interface, provide the interface name with the sub-command.

Syntax

show interfaces breakout (Versions >= 202006)

show interfaces breakout current-mode [*interface_name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@lnos-x1-a-fab01:~$ show interfaces    breakout
{
    "Ethernet0": {
        "index": "1,1,1,1",
        "default_brkout_mode": "1x100G[40G]",
```

```
            "child ports": "Ethernet0",
            "child port speed": "100G",
            "breakout_modes": "1x100G[40G],2x50G,4x25G[10G]",
            "Current Breakout Mode": "1x100G[40G]",
            "lanes": "65,66,67,68",
            "alias_at_lanes": "Eth1/1, Eth1/2, Eth1/3, Eth1/4"
        },... continue
}
```

The "current-mode" subcommand is used to display current breakout mode for all interfaces.

```
admin@lnos-x1-a-fab01:~$ show interfaces    breakout current-mode
+-------------+-------------------------+
| Interface     | Current Breakout Mode     |
+==============+=========================+
| Ethernet0     | 4x25G[10G]                  |
+-------------+-------------------------+
| Ethernet4     | 4x25G[10G]                  |
+-------------+-------------------------+
| Ethernet8     | 4x25G[10G]                  |
+-------------+-------------------------+
| Ethernet12    | 4x25G[10G]                  |
+-------------+-------------------------+

admin@lnos-x1-a-fab01:~$ show interfaces    breakout current-mode Ethernet0
+-------------+-------------------------+
| Interface     | Current Breakout Mode     |
+==============+=========================+
| Ethernet0     | 4x25G[10G]                  |
+-------------+-------------------------+
```

1.41 show interfaces counters

Function

Run the **show interfaces counters** command to display packet counters for all interfaces since the last time the counters were cleared. To display l3 counters "rif" subcommand can be used. There is no facility to display counters for one specific l2 interface. For l3 interfaces a single interface output mode is present. Optional argument "-a" provides two additional columns - RX-PPS and TX_PPS.

Syntax

show interfaces counters [**-a** | **--printall**] [**-p** | **--period** [*period*]]

show interfaces counters errors

show interfaces counters rates

show interfaces counters rif [**-p** | **--period** [*period*]] [**-i** [*interface-name*]]

Parameter Description

-a | **--printall**: Print all statistics

-p | **--period**: Print statistics over a period of time

-i: Interface name, for example, Ethernet1

period: Time required to obtain statistics, in seconds

interface_name: Interface name, for example, Ethernet1

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces counters
      IFACE     STATE              RX_OK         RX_BPS     RX_UTIL     RX_ERR     RX_DRP     RX_OVR
TX_OK         TX_BPS     TX_UTIL     TX_ERR     TX_DRP     TX_OVR
-----------  -------  ---------------  -----------  ---------  --------  --------  --------
---------------  -----------  ---------  --------  --------  --------
  Ethernet0          U   471,729,839,997   653.87 MB/s       12.77%           0     18,682           0
409,682,385,925   556.84 MB/s       10.88%             0           0           0
  Ethernet4          U   453,838,006,636   632.97 MB/s       12.36%           0      1,636           0
388,299,875,056   529.34 MB/s       10.34%             0           0           0
  Ethernet8          U   549,034,764,539   761.15 MB/s       14.87%           0     18,274           0
457,603,227,659   615.20 MB/s       12.02%             0           0           0
Ethernet12           U   458,052,204,029   636.84 MB/s       12.44%           0     17,614           0
388,341,776,615   527.37 MB/s       10.30%             0           0           0
  Ethernet16         U    16,679,692,972    13.83 MB/s        0.27%           0     17,605           0
18,206,586,265    17.51 MB/s        0.34%              0           0           0
  Ethernet20         U    47,983,339,172    35.89 MB/s        0.70%           0      2,174           0
58,986,354,359    51.83 MB/s        1.01%              0           0           0
  Ethernet24         U    33,543,533,441    36.59 MB/s        0.71%           0      1,613           0
43,066,076,370    49.92 MB/s        0.97%              0           0           0

admin@sonic:~$ show interfaces counters -i Ethernet4,Ethernet12-16
      IFACE     STATE              RX_OK         RX_BPS     RX_UTIL     RX_ERR     RX_DRP     RX_OVR
TX_OK         TX_BPS     TX_UTIL     TX_ERR     TX_DRP     TX_OVR
-----------  -------  ---------------  -----------  ---------  --------  --------  --------
---------------  -----------  ---------  --------  --------  --------
  Ethernet4          U   453,838,006,636   632.97 MB/s       12.36%           0      1,636           0
388,299,875,056   529.34 MB/s       10.34%             0           0           0
  Ethernet12         U   458,052,204,029   636.84 MB/s       12.44%           0     17,614           0
388,341,776,615   527.37 MB/s       10.30%             0           0           0
  Ethernet16         U    16,679,692,972    13.83 MB/s        0.27%           0     17,605           0
18,206,586,265    17.51 MB/s        0.34%              0           0           0
```

The "errors" subcommand is used to display the interface errors.

```
admin@str-s6000-acs-11:~$ show interface counters errors
    IFACE      STATE      RX_ERR      RX_DRP      RX_OVR      TX_ERR      TX_DRP      TX_OVR
-----------  -------  ---------  ---------  ---------  ---------  ---------  ---------
  Ethernet0          U          0          4          0          0          0          0
  Ethernet4          U          0          0          0          0          0          0
  Ethernet8          U          0          1          0          0          0          0
  Ethernet12         U          0          0          0          0          0          0
```

The "rates" subcommand is used to display only the interface rates.

```
admin@str-s6000-acs-11:/usr/bin$ show int counters rates
    IFACE      STATE      RX_OK      RX_BPS      RX_PPS      RX_UTIL      TX_OK      TX_BPS      TX_PPS
TX_UTIL
-----------  -------  -------  ---------  ---------  ----------  -------  ---------  ---------  --
-------
  Ethernet0          U     467510         N/A         N/A          N/A    466488         N/A         N/A
N/A
  Ethernet4          U     469679         N/A         N/A          N/A    469245         N/A         N/A
N/A
  Ethernet8          U     466660         N/A         N/A          N/A    465982         N/A         N/A
N/A
  Ethernet12         U     466579         N/A         N/A          N/A    466318         N/A         N/A
N/A
```

The "rif" subcommand is used to display l3 interface counters. Layer 3 interfaces include router interfaces, portchannels and vlan interfaces.

```
admin@sonic:~$ show interfaces counters rif
          IFACE         RX_OK        RX_BPS      RX_PPS     RX_ERR     TX_OK      TX_BPS      TX_PPS
TX_ERR
---------------  -------  ----------  ---------  ---------  -------  ---------  ---------  ------
--
PortChannel0001     62,668          107.81 B/s      1.34/s          3          6    0.02 B/s      0.00/s
0
PortChannel0002     62,645          107.77 B/s      1.34/s          3          2    0.01 B/s      0.00/s
0
PortChannel0003     62,481          107.56 B/s      1.34/s          3          3    0.01 B/s      0.00/s
0
PortChannel0004     62,732          107.88 B/s      1.34/s          2          3    0.01 B/s      0.00/s
0
           Vlan1000          0            0.00 B/s       0.00/s          0          0    0.00 B/s      0.00/s
0
```

Optionally, you can specify a period (in seconds) with which to gather counters over. Note that this function will take `<period>` seconds to execute.

```
admin@sonic:~$ show interfaces counters -p 5
```

```
      IFACE     STATE     RX_OK         RX_BPS     RX_UTIL     RX_ERR     RX_DRP     RX_OVR
TX_OK         TX_BPS     TX_UTIL     TX_ERR     TX_DRP     TX_OVR
-----------  -------  -------  -----------  ---------  --------  --------  --------  -------
-----------  ---------  --------  --------  --------
Ethernet0           U       515    59.14 KB/s       0.00%           0          0          0     1,305   127.60
KB/s         0.00%           0           0           0
Ethernet4           U       305    26.54 KB/s       0.00%           0          0          0       279
39.12 KB/s       0.00%           0           0           0
Ethernet8           U       437    42.96 KB/s       0.00%           0          0          0       182
18.37 KB/s       0.00%           0           0           0
Ethernet12          U       284    40.79 KB/s       0.00%           0          0          0       160
13.03 KB/s       0.00%           0           0           0
Ethernet16          U       377    32.64 KB/s       0.00%           0          0          0       214    18.01
KB/s         0.00%           0           0           0
Ethernet20          U       284    36.81 KB/s       0.00%           0          0          0       138
8758.25 B/s      0.00%           0           0           0
Ethernet24          U       173    16.09 KB/s       0.00%           0          0          0       169    11.39
KB/s         0.00%           0           0           0
```

Interface counters can be cleared by the user with the following command:

```
admin@sonic:~$ sonic-clear counters
```

Layer 3 interface counters can be cleared by the user with the following command:

```
admin@sonic:~$ sonic-clear rifcounters
```

1.42 show interfaces description

Function

Run the **show interfaces description** command to display the key fields of the interfaces such as Operational Status, Administrative Status, Alias and Description.

Syntax

show interfaces description [*interface-name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces description
Interface      Oper      Admin                Alias              Description
-----------  ------  -------  ---------------  --------------------
Ethernet0      down         up    hundredGigE1/1   T0-1:hundredGigE1/30
```

```
Ethernet4      down          up     hundredGigE1/2    T0-2:hundredGigE1/30
Ethernet8      down        down     hundredGigE1/3            hundredGigE1/3
Ethernet12     down        down     hundredGigE1/4            hundredGigE1/4
```

To only display the description for interface Ethernet4

```
admin@sonic:~$ show interfaces description Ethernet4
Interface      Oper      Admin              Alias               Description
-----------  ------   -------   --------------   --------------------
Ethernet4      down          up   hundredGigE1/2   T0-2:hundredGigE1/30
```

1.43 show interfaces errdisable

Function

Run the **show interfaces errdisable** command to display the error disable information such as status and reason.

Syntax

show interfaces errdisable

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces errdisable
Interface            Status          Reason
-----------   -------------   -----------
Ethernet50   Error disable   link-dither
```

1.44 show interfaces fec-bypass

Function

Run the **show interfaces fec-bypass** command to displays the configuration of interfaces fec-bypass mode.

Syntax

show interfaces fec-bypass

show interfaces fec-bypass [*interface_name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces fec-bypass status
Interface          Oper         Admin         Fec-bypass Mode
-----------     ------     -------     -----------------
Ethernet1          down              up                          disable
Ethernet2          down              up                          disable
Ethernet3          down              up                           enable
Ethernet4          down              up                              N/A
Ethernet5          down              up                           enable
Ethernet6          down              up                              N/A
Ethernet7          down              up                              N/A
```

1.45 show interfaces info

Function

Run the **show interfaces info** command to display the interface information such as description, status, line protocol status, MAC address, speed, bandwidth, admin FEC, oper FEC, MTU, interface IP address, interface IPv6 address, VLAN, link up delay, link down delay, and statistics.

Syntax

show interfaces info

show interfaces info [*interface_name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces info
=============== Interface Ethernet1 ===============
  Description:
  Admin status: up
  Line protocol status: down
  MAC: 58:69:6c:fb:20:19
  Speed: 25.0G
  Bandwidth: 25.0G
  Admin FEC: none       Oper FEC: none
  MTU: 9100
```

```
  Interface IP:
  Interface IPv6:
  Vlan:
    Native vlan: 1
  Link up delay:     0 s 0 ms
  Link down delay: 0 s 0 ms
  Statistic:
    RX packets 0    bytes 0 (0.0 B)
    RX errors 0    dropped 0    overruns 0    frame 0
    TX packets 0    bytes 0 (0.0 B)
    TX errors 0    dropped 0 overruns 0    carrier 0    collisions 0
=============== Interface Ethernet2 ===============
  Description:
  Admin status: up
  Line protocol status: down
  MAC: 58:69:6c:fb:20:19
  Speed: 25.0G
  Bandwidth: 25.0G
  Admin FEC: none       Oper FEC: none
  MTU: 9100
  Interface IP:
  Interface IPv6:
  Vlan:
    Native vlan: 1
  Link up delay:     0 s 0 ms
  Link down delay: 0 s 0 ms
  Statistic:
    RX packets 0    bytes 0 (0.0 B)
    RX errors 0    dropped 0    overruns 0    frame 0
    TX packets 0    bytes 0 (0.0 B)
    TX errors 0    dropped 0 overruns 0    carrier 0    collisions 0
```

```
admin@sonic:~$ show interfaces info Ethernet56
=============== Interface Ethernet56 ===============
  Description:
  Admin status: up
  Line protocol status: down
  MAC: 58:69:6c:fb:20:19
  Speed: 100.0G
  Bandwidth: 100.0G
  Admin FEC: none       Oper FEC: none
  MTU: 9100
  Interface IP:
  Interface IPv6:
  Vlan:
```

```
    Native vlan: 1
  Link up delay:     0 s 0 ms
  Link down delay: 0 s 0 ms
  Statistic:
    RX packets 0    bytes 0 (0.0 B)
    RX errors 0    dropped 0    overruns 0    frame 0
    TX packets 0    bytes 0 (0.0 B)
TX errors 0    dropped 0 overruns 0    carrier 0    collisions 0
```

1.46 show interfaces ip-statisitcs

Function

Run the **show interfaces ip-statisitcs** command to display the status of IP packet counter specific to the interface.

Syntax

show interfaces ip-statisitcs state

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces ip-statisitcs state
Interface       ip_statistics state
-----------   ---------------------
  Ethernet1                    disable
  Ethernet2                    disable
  Ethernet3                    disable
  Ethernet4                    disable
  Ethernet5                    disable
  Ethernet6                    disable
  Ethernet7                    disable
```

1.47 show interfaces media

Function

Run the **show interfaces media** command to display the interface media type.

Syntax

show interfaces media

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces media
Media type Configure
+-------------+--------------+
| port name     | media_type     |
+==============+==============+
| Ethernet22    | fiber            |
+-------------+--------------+
```

1.48 show interfaces mpls

Function

Run the **show interfaces mpls** command to display the configured MPLS state for the list of configured interfaces.

Syntax

show interfaces mpls [*interface-name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces mpls
Interface       MPLS State
-----------   ------------
Ethernet0       disable
Ethernet4       enable
Ethernet8       enable
Ethernet12     disable
Ethernet16     disable
Ethernet20     disable
```

To only display the MPLS state for interface Ethernet4

```
admin@sonic:~$ show interfaces mpls Ethernet4
Interface      MPLS State
-----------   ------------
Ethernet4      enable
```

1.49 show interfaces naming_mode

Function

Run the **show interfaces naming_mode** command to display the current interface naming mode.

Syntax

show interfaces naming_mode

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces naming_mode
default
"default" naming mode will display all SONiC interface names in 'show' commands and accept SONiC interface names as parameters in 'config commands
admin@sonic:~$ show interfaces naming_mode
alias
"alias" naming mode will display all hardware vendor interface aliases in 'show' commands and accept hardware vendor interface aliases as parameters in 'config commands
```

1.50 show interfaces neighbor

Function

Run the **show interfaces neighbor** command to display the list of expected neighbors for all interfaces (or for a particular interface) that is configured.

Syntax

show interfaces neighbor expected [*interface-name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces neighbor expected
LocalPort      Neighbor      NeighborPort      NeighborLoopback      NeighborMgmt      NeighborType
-----------  ----------  --------------  ------------------  --------------  --------------
Ethernet112   Router01T1   Ethernet1          None                  10.16.205.100     ToRRouter
Ethernet116   Router02T1   Ethernet1          None                  10.16.205.101     SpineRouter
Ethernet120   Router03T1   Ethernet1          None                  10.16.205.102     LeafRouter
Ethernet124   Router04T1   Ethernet1          None                  10.16.205.103     LeafRouter
```

1.51 show interfaces portchannel

Function

Run the **show interfaces portchannel** command to display information regarding port-channel interfaces.

Syntax

show interfaces portchannel

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces portchannel
Flags: A - active, I - inactive, Up - up, Dw - Down, N/A - not available, S - selected, D - deselected
  No.   Team Dev          Protocol       Ports
-----  -------------  -----------  --------------------------
   24   PortChannel24   LACP(A)(Up)   Ethernet28(S) Ethernet24(S)
   48   PortChannel48   LACP(A)(Up)   Ethernet52(S) Ethernet48(S)
   40   PortChannel40   LACP(A)(Up)   Ethernet44(S) Ethernet40(S)
    0   PortChannel0    LACP(A)(Up)   Ethernet0(S) Ethernet4(S)
    8   PortChannel8    LACP(A)(Up)   Ethernet8(S) Ethernet12(S)
```

1.52 show interfaces status

Function

Run the **show interfaces status** command to display some more fields such as Lanes, Speed, MTU, Type, Asymmetric PFC status and also the operational and administrative status of the interfaces.

Syntax

show interfaces status [*interface-name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

Show interface status of all interfaces

```
admin@sonic:~$ show interfaces status
Interface                Lanes      Speed      MTU               Alias      Oper      Admin      Type      Asym
PFC
-----------  ---------------  -------  -----  ---------------  ------  -------  ------  -----
-----
Ethernet0         49,50,51,52       100G     9100     hundredGigE1/1      down          up       N/A            off
Ethernet4         53,54,55,56       100G     9100     hundredGigE1/2      down          up       N/A
off
Ethernet8         57,58,59,60       100G     9100     hundredGigE1/3      down       down       N/A
off
<contiues to display all the interfaces>
```

To only display the status for interface Ethernet0

```
admin@sonic:~$ show interface status Ethernet0
Interface       Lanes      Speed      MTU               Alias      Oper      Admin
-----------  --------  -------  -----  --------------  ------  -------
Ethernet0     101,102         40G     9100     fortyGigE1/1/1         up          up
```

To only display the status for range of interfaces

```
admin@sonic:~$ show interfaces status Ethernet8,Ethernet168-180
Interface                  Lanes      Speed      MTU               Alias       Oper      Admin      Type
Asym PFC
-----------  -----------------  -------  -----  ---------------  ------  -------  ------  ---
-------
  Ethernet8         49,50,51,52       100G      9100      hundredGigE3       down       down       N/A
N/A
```

```
Ethernet168          9,10,11,12       100G      9100      hundredGigE43      down       down       N/A
N/A
Ethernet172          13,14,15,16      100G      9100      hundredGigE44      down       down       N/A
N/A
Ethernet176    109,110,111,112        100G      9100      hundredGigE45      down       down       N/A
N/A
Ethernet180    105,106,107,108        100G      9100      hundredGigE46      down       down       N/A
N/A
```

1.53 show interfaces storm_control

Function

Run the **show interfaces storm_control** command to display broadcast, multicast, and unicast storm control configuration.

Syntax

show interfaces storm_control

show interfaces storm_control [*interface-name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces storm_control
Interface      Broadcast Control      Multicast Control      Unicast Control
--------------  --------------------  --------------------  -----------------
Ethernet1               Disabled              Disabled             Disabled
Ethernet2               Disabled              Disabled             Disabled
Ethernet3               Disabled              Disabled             Disabled
Ethernet4               Disabled              Disabled             Disabled
Ethernet5               Disabled              Disabled             Disabled
```

```
admin@sonic:~$ show interfaces storm_control Ethernet55
Interface      Broadcast Control        Multicast Control       Unicast Control
-----------  --------------------  --------------------  -----------------
Ethernet55              Disabled              Disabled             Disabled
```

1.54 show interfaces tpid

Function

Run the **show interfaces tpid** command to display the key fields of the interfaces such as Operational Status, Administrative Status, Alias and TPID.

Syntax

show interfaces tpid [*interface-name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces tpid
       Interface                Alias      Oper      Admin      TPID
---------------  ---------------  ------  -------  ------
       Ethernet0    fortyGigE1/1/1        up         up   0x8100
       Ethernet1    fortyGigE1/1/2        up         up   0x8100
       Ethernet2    fortyGigE1/1/3      down       down   0x8100
       Ethernet3    fortyGigE1/1/4      down       down   0x8100
       Ethernet4    fortyGigE1/1/5        up         up   0x8100
       Ethernet5    fortyGigE1/1/6        up         up   0x8100
       Ethernet6    fortyGigE1/1/7        up         up   0x9200
       Ethernet7    fortyGigE1/1/8        up         up   0x88A8
       Ethernet8    fortyGigE1/1/9        up         up   0x8100
       ...
      Ethernet63   fortyGigE1/4/16      down       down   0x8100
PortChannel0001                N/A        up         up   0x8100
PortChannel0002                N/A        up         up   0x8100
PortChannel0003                N/A        up         up   0x8100
PortChannel0004                N/A        up         up   0x8100
```

To only display the TPID for interface Ethernet6

```
admin@sonic:~$ show interfaces tpid Ethernet6
  Interface              Alias      Oper      Admin      TPID
-----------  --------------  ------  -------  ------
  Ethernet6   fortyGigE1/1/7        up         up   0x9200
```

1.55 show interfaces transceiver

Function

Run the **show interfaces transceiver** command to explain here.

Syntax

show interfaces transceiver { **eeprom** | **error-status** | **lpmode** | **presence** } [*interface-name*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces transceiver eeprom
Ethernet1: SFP EEPROM detected
        Application Advertisement: N/A
        Connector: No separable connector
        Encoding: 64B/66B
        Extended Identifier: Power Class 1 Module (1.5W max.), No CLEI code present in Page 02h, No
CDR in TX, No CDR in RX
        Extended RateSelect Compliance: Unknown
        Identifier: QSFP28 or later
        Length Cable Assembly(m): 1.0
        Nominal Bit Rate(100Mbs): 255
        Specification compliance:
                10/40G Ethernet Compliance Code: Unknown
                Extended Specification Compliance: 100GBASE-CR4, 25GBASE-CR CA-25G-L or
50GBASE-CR2 with RS
                Fibre Channel Link Length: Unknown
                Fibre Channel Speed: Unknown
                Fibre Channel Transmission Media: Unknown
                Fibre Channel Transmitter Technology: Unknown
                Gigabit Ethernet Compliant Codes: Unknown
                SAS/SATA Compliance Codes: Unknown
                SONET Compliance Codes: Unknown
        Vendor Date Code(YYYY-MM-DD Lot): 2020-10-09 00
        Vendor Name: LEONI
        Vendor OUI: a8-b0-ae
        Vendor PN: C45593-A502-D10
        Vendor Rev: 00
        Vendor SN: LEO2041G2WX
```

```
admin@sonic:~$ show interfaces transceiver error-status
Port             Error Status
-----------   --------------
Ethernet1      OK
Ethernet5       Unplugged
Ethernet9       Unplugged
Ethernet13     OK
Ethernet17     Unplugged
Ethernet21     OK
Ethernet25      Unplugged

admin@sonic:~$ show interfaces transceiver lpmode
Traceback (most recent call last):
  File "/usr/local/bin/sfputil", line 8, in <module>
    sys.exit(cli())
  File "/usr/local/lib/python3.9/dist-packages/click/core.py", line 764, in __call__
    return self.main(*args, **kwargs)
  File "/usr/local/lib/python3.9/dist-packages/click/core.py", line 717, in main
    rv = self.invoke(ctx)
  File "/usr/local/lib/python3.9/dist-packages/click/core.py", line 1137, in invoke
    return _process_result(sub_ctx.command.invoke(sub_ctx))
  File "/usr/local/lib/python3.9/dist-packages/click/core.py", line 1137, in invoke
    return _process_result(sub_ctx.command.invoke(sub_ctx))
  File "/usr/local/lib/python3.9/dist-packages/click/core.py", line 956, in invoke
    return ctx.invoke(self.callback, **ctx.params)
  File "/usr/local/lib/python3.9/dist-packages/click/core.py", line 555, in invoke
    return callback(*args, **kwargs)
  File "/usr/local/lib/python3.9/dist-packages/sfputil/main.py", line 799, in lpmode
    lpmode = platform_chassis.get_sfp(physical_port).get_lpmode()
  File "/usr/lib/python3/dist-packages/sonic_platform/sfp.py", line 146, in get_lpmode
    return SfpOptoeBase.get_lpmode(self)
  File "/usr/local/lib/python3.9/dist-
packages/sonic_platform_base/sonic_xcvr/sfp_optoe_base.py", line 154, in get_lpmode
    return api.get_lpmode() if api is not None else None
AttributeError: 'Sff8636Api' object has no attribute 'get_lpmode'

admin@sonic:~$ show interfaces transceiver pre
Port             Presence
-----------   -----------
Ethernet1      Present
Ethernet5       Not present
Ethernet9       Not present
Ethernet13     Present
Ethernet17     Not present
```

1.56 show interfaces vlan-info

Function

Run the **show interfaces vlan-info** command to display VLAN interface configuration.

Syntax

show interfaces vlan-info [*vlan-name*]

Parameter Description

vlan-name: Interface name, for example, Vlan20.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces vlan-info
=============== Interface Vlan20 ===============
  Description:
  Admin status: up
  Line protocol status: down
  MAC: 00:22:22:22:22:22
  Interface IP:
    192.168.30.20/24
  Interface IPv6:
=============== Interface Vlan100 ===============
  Description:
  Admin status: up
  Line protocol status: down
  MAC: 58:69:6c:fb:20:19
  Interface IP:
    192.168.20.20/24
  Interface IPv6:
```

```
admin@sonic:~$ show interfaces vlan-info Vlan20
=============== Interface Vlan20 ===============
  Description:
  Admin status: up
  Line protocol status: down
  MAC: 00:22:22:22:22:22
  Interface IP:
    192.168.30.20/24
  Interface IPv6:
```

1.57 show ipv6 link-local-mode

Function

Run the **show ipv6 link-local-mode** command to display the link local mode of all the interfaces.

Syntax

show ipv6 link-local-mode

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
root@sonic:/home/admin# show ipv6 link-local-mode
+------------------+----------+
| Interface Name     | Mode        |
+==================+==========+
| Ethernet16           | Disabled |
+------------------+----------+
| Ethernet18           | Enabled   |
+------------------+----------+
```

1 LAG Interface Commands

Command	Function
config portchannel	Add or delete the portchannel. It is recommended to use portchannel names in the format "PortChannelxxxx", where "xxxx" is number of 1 to 4 digits. Ex: "PortChannel0002".
config portchannel lacp-update	Update portchannel.
config portchannel member	Add or delete a member port to/from the already created portchannel.
show interfaces portchannel	Display all the port channels that are configured in the device and its current status.

1.1 config portchannel

Function

Run the **config portchannel** command to add or delete the portchannel. It is recommended to use portchannel names in the format "PortChannelxxxx", where "xxxx" is number of 1 to 4 digits. Ex: "PortChannel0002".

Syntax

config portchannel { **add** | **del** } [*portchannel_name*] [**--min-links** [*num_min_links*]] [**--fallback** { **true** | **false** }] [**--system-id** [**mac-address as** *xx:xx:xx:xx:xx:xx*]] [**--device-id** *num_id*] [**--system-priority** [*num*]] [**--fast-rate** { **true** | **false** }] [**--mode** { **manual** | **lacp** }]

Parameter Description

add: Add port channel.

del: Remove port channel.

portchannel_name: Aggregate interface name, for example, PortChannel1.

num_min_links: Threshold for the number of Up members required for the aggregate interface to be Up.

mac-address: MAC address as xx:xx:xx:xx:xx:xx.

num_id: Device ID.

num: System priority.

manual: Manual mode.

lacp: Lacp protocol negotiation mode.

Usage Guidelines

If users specify any other name like "pc99", command will succeed, but such names are not supported. Such names are not printed properly in the "show interface portchannel" command. It is recommended not to use such names.

When any port is already member of any other portchannel and if user tries to add the same port in some other portchannel (without deleting it from the current portchannel), the command fails internally. But, it does not print any error message. In such cases, remove the member from current portchannel and then add it to new portchannel.

Command takes two optional arguments given below. 1) min-links - minimum number of links required to bring up the portchannel 2) fallback - true/false. LACP fallback feature can be enabled / disabled. When it is set to true, only one member port will be selected as active per portchannel during fallback mode. Refer https://github.com/Azure/SONiC/blob/master/doc/lag/LACP%20Fallback%20Feature%20for%20SONiC_v0.5.md for more details about fallback feature. 3) system-id - . Identifies an aggregation port, the default is the system MAC. 4) device-id - 0~3. Identify a device. 5) system-priority - Aggregation port priority. 6) fast-rate - true/false. Aggregation port detection link connection, long timeout and short timeout configuration. 7) mode - manual/lacp. Use manual mode or LACP protocol to negotiate the link.

NOTE:

- A port channel can be deleted only if it does not have any members or the members are already deleted. When a user tries to delete a port channel and the port channel still has one or more members that exist, the deletion of port channel is blocked.
- Only full-duplex interfaces can perform LACP aggregation.
- In LACP mode, the rate, flow control, media type of member interfaces, and the Layer 2 and Layer 3 attributes of member interfaces must be consistent for LACP aggregation.
- When an interface is added to an aggregate interface, the attributes of this interface will be replaced by the attributes of the aggregate interface. Therefore, generally, configuration is not allowed on the member interfaces of the aggregate interface, or the configuration takes effect solely on the member interfaces of the aggregate interface. However, there are a few commands or functions that can still be configured on member interfaces of an aggregate interface, and the configuration can take effect. Therefore, when using the member interfaces of an aggregate interface, you need to determine whether it is supported to take effect solely on the member interfaces of the aggregate interface based on specific functional requirements, and configure it correctly.
- Manual aggregation does not have an error detection mechanism. Member interfaces are bound after the status is Up. Therefore, you need to manually ensure the correctness of the topology and the consistency of the negotiated attributes between member interfaces.
- When configuring a Layer 2 port channel interface or a Layer 3 port channel interface, packets with the same fields (source and destination MAC, source and destination IP, and their combination) will only go through one port channel member interface, and the traffic will not be balanced to other port channel member interfaces.

Examples

Create the portchannel with name “PortChannel11

```
admin@sonic:~$ sudo config portchannel add PortChannel11
```

1.2 config portchannel lacp-update

Function

Run the **config portchannel lacp-update** command to update portchannel.

Syntax

config portchannel lacp-update fallback [OPTIONS] portchannel_name { **true** | **false** }

config portchannel lacp-update fast-rate [OPTIONS] portchannel_name { **true** | **false** }

config portchannel lacp-update min-links [OPTIONS] portchannel_name *num_min_links*

Parameter Description

fallback: update lacp fallback.

fast-rate: update lacp fast-rate.

min-links: update lacp min-links.

portchannel_name: Aggregate interface name, for example, PortChannel1

num_min_links: The threshold for the number of up members required for the aggregation

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config portchannel lacp-update fallback PortChannel20 true
```

1.3 config portchannel member

Function

Run the **config portchannel member** command to add or delete a member port to/from the already created portchannel.

Syntax

config portchannel member { **add** | **del** } *portchannel-name member-portname*

Parameter Description

add: Add member to port channel.

del: Remove member from portchannel.

portchannel_name: Aggregate interface name, for example, PortChannel1

member_portname: Name of the members of the aggregate interface

Usage Guidelines

NOTE:

- When the number of member links on a port channel aggregation port is an odd number or is not a power of 2, even if a packet flow whose change number is a multiple of the number of member links is input, it may not be fully evenly distributed among all member links.
- During the change of port channel members, millisecond-level loops may occur.
- After LACP member interfaces are aggregated, modifying the rate, flow control, media type of the interface, and the Layer 2 and 3 attributes of the member interfaces will cause other interfaces in the same aggregation group to be unable to perform LACP aggregation.

- Port channel member ports that are LINK UP and in the LACP SUSP state can receive frames, and the incoming traffic will be in the form of a normal physical port for normal Layer 2 forwarding and address learning.

Examples

```
admin@sonic:~$ sudo config portchannel member add PortChannel0011 Ethernet4
```

1.4 show interfaces portchannel

Function

Run the **show interfaces portchannel** command to display all the port channels that are configured in the device and its current status.

Syntax

show interfaces portchannel

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces portchannel
Flags: A - active, I - inactive, Up - up, Dw - Down, N/A - not available, S - selected, D - deselected
No.    Team Dev           Protocol        Ports
-----   -------------   -----------   --------------------------
24    PortChannel24    LACP(A)(Up)    Ethernet28(S) Ethernet24(S)
48    PortChannel48    LACP(A)(Up)    Ethernet52(S) Ethernet48(S)
40    PortChannel40    LACP(A)(Up)    Ethernet44(S) Ethernet40(S)
0    PortChannel0     LACP(A)(Up)    Ethernet0(S) Ethernet4(S)
8    PortChannel8     LACP(A)(Up)    Ethernet8(S) Ethernet12(S)
```

1 Startup & Running Configuration Commands

Command	Function
show runningconfiguration all	Display the entire running configuration.
show runningconfiguration acl	Display the running configuration of the acls.
show runningconfiguration bgp	Display the running configuration of the BGP module.
show runningconfiguration dhcp_relay	Displays the running configuration of the dhcp relay.
show runningconfiguration dhcp4_client	Show all the interfaces with DHCP4 client function enabled.
show runningconfiguration dhcp6_client	Show all the interfaces with DHCP6 client ia_na or stateless_configuration function enabled.
show runningconfiguration interfaces	Display the running configuration for the "interfaces".
show runningconfiguration ntp	Display the running configuration of the ntp module.
show runningconfiguration ports	Display the running configuration of the ports.
show runningconfiguration snmp	Display the running configuration of the snmp module.
show runningconfiguration spanning-tree	Displays the running configuration of the STP.
show runningconfiguration syslog	Display the running configuration of the syslog module.
show startupconfiguration bgp	Display the startup configuration for the BGP module..

1.1 show runningconfiguration all

Function

Run the **show runningconfiguration all** command to display the entire running configuration.

Syntax

show runningconfiguration all

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration all
```

1.2 show runningconfiguration acl

Function

Run the **show runningconfiguration acl** command to display the running configuration of the acls.

Syntax

show runningconfiguration acl

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration acl
```

1.3 show runningconfiguration bgp

Function

Run the **show runningconfiguration bgp** command to display the running configuration of the BGP module.

Syntax

show runningconfiguration bgp

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration bgp
```

1.4 show runningconfiguration dhcp_relay

Function

Run the **show runningconfiguration dhcp_relay** command to displays the running configuration of the dhcp relay.

Syntax

show runningconfiguration dhcp_relay { **ipv4** | **ipv6** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration dhcp_relay ipv4
----------------------------  -----
DHCPv4 Relay Status:                FALSE
DHCPv4 Relay Option82 Status:   FALSE
----------------------------  -----


admin@sonic:~$ show runningconfiguration dhcp_relay ipv6
-------------------  -----
DHCPv6 Relay Staus:   FALSE
-------------------  -----
+-------------+-------------------------------+-------------------------------+
| Interface     | DHCPv6 Relay Option18 Status     | DHCPv6 Relay Option79 Status     |
+=============+===================================+=======================
==========+
+-------------+-------------------------------+-------------------------------+
```

1.5 show runningconfiguration dhcp4_client

Function

Run the **show runningconfiguration dhcp4_client** command to show all the interfaces with DHCP4 client function enabled.

Syntax

show runningconfiguration dhcp4_client

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration dhcp4_client
+----------------------------+----------------------------+
| dhcp4 client enabled interface | ['Ethernet1', 'Ethernet2'] |
+----------------------------+----------------------------+
```

1.6 show runningconfiguration dhcp6_client

Function

Run the **show runningconfiguration dhcp6_client** command to show all the interfaces with DHCP6 client ia_na or stateless_configuration function enabled.

Syntax

show runningconfiguration dhcp6_client

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration dhcp6_client
+-------------------------------------------------------+----+
| dhcp6 client ia_na enabled interface                  | [] |
+-------------------------------------------------------+----+
| dhcp6 client stateless_configuration enabled interface | [] |
+-------------------------------------------------------+----+
```

1.7 show runningconfiguration interfaces

Function

Run the **show runningconfiguration interfaces** command to display the running configuration for the "interfaces".

Syntax

show runningconfiguration interfaces

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration interfaces
```

1.8 show runningconfiguration ntp

Function

Run the **show runningconfiguration ntp** command to display the running configuration of the ntp module.

Syntax

show runningconfiguration ntp

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration ntp
NTP Servers
-------------
1.1.1.1
2.2.2.2
```

1.9 show runningconfiguration ports

Function

Run the **show runningconfiguration ports** command to display the running configuration of the ports.

Syntax

show runningconfiguration ports [*port-name*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration ports
```

```
admin@sonic:~$ show runningconfiguration ports
```

1.10 show runningconfiguration snmp

Function

Run the **show runningconfiguration snmp** command to display the running configuration of the snmp module.

Syntax

show runningconfiguration snmp

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration snmp
```

1.11 show runningconfiguration spanning-tree

Function

Run the **show runningconfiguration spanning-tree** command to displays the running configuration of the STP.

Syntax

show runningconfiguration spanning-tree

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration spanning-tree
```

1.12 show runningconfiguration syslog

Function

Run the **show runningconfiguration syslog** command to display the running configuration of the syslog module.

Syntax

show runningconfiguration syslog

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration syslog
syslog server       port
---------------   ------
172.31.240.48       514
```

1.13 show startupconfiguration bgp

Function

Run the **show startupconfiguration bgp** command to display the startup configuration for the BGP module..

Syntax

show startupconfiguration bgp

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show startupconfiguration bgp
Routing-Stack is: quagga
!
! ========== Managed by sonic-cfggen DO NOT edit manually! ====================
```

```
! generated by templates/quagga/bgpd.conf.j2 with config DB data
! file: bgpd.conf
!
!
hostname T1-2
password zebra
log syslog informational
log facility local4
! enable password !
!
! bgp multiple-instance
!
route-map FROM_BGP_SPEAKER_V4 permit 10
!
route-map TO_BGP_SPEAKER_V4 deny 10
!
router bgp 65000
   bgp log-neighbor-changes
   bgp bestpath as-path multipath-relax
   no bgp default ipv4-unicast
   bgp graceful-restart restart-time 180
```

Only the partial output is shown here. In actual command, more configuration information will be displayed.

1 Monitor-Link Commands

Command	Function
config monitor-link	Enable or disable a monitor link group.
config monitor-link group	Set a monitor link group.
config monitor-link up-delay	Set the switchover delay for the downlink interfaces in a monitor link group.
config monitor-link up-threshold	Set the switchover threshold for the downlink interfaces in a monitor link group.
config monitor-link { uplink | downlink }	Add an uplink or downlink interface to a monitor link group.
show monitor-link all	Display the monitor link group configuration.

1.1 config monitor-link

Function

Run the **config monitor-link** command to enable or disable a monitor link group.

Syntax

config monitor-link { enable | disable } *id* **(Versions >= 202111)**

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config monitor-link disable 1
admin@sonic:~$ sudo config monitor-link enable 1
```

1.2 config monitor-link group

Function

Run the **config monitor-link group** command to set a monitor link group.

Syntax

config monitor-link group { add | del } *id* **(Versions >= 202111)**

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config monitor-link group add 1
admin@sonic:~$ sudo config monitor-link group del 1
```

1.3 config monitor-link up-delay

Function

Run the **config monitor-link up-delay** command to set the switchover delay for the downlink interfaces in a monitor link group.

Syntax

config monitor-link up-delay *grp-id time* **(Versions >= 202111)**

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config monitor-link up-delay 1 100
```

1.4 config monitor-link up-threshold

Function

Run the **config monitor-link up-threshold** command to set the switchover threshold for the downlink interfaces in a monitor link group.

Syntax

config monitor-link up-threshold *grp-id num-threshold* **(Versions >= 202111)**

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config monitor-link up-threshold 1 1
```

1.5 config monitor-link { uplink | downlink }

Function

Run the **config monitor-link { uplink | downlink }** command to add an uplink or downlink interface to a monitor link group.

Syntax

config monitor-link { uplink | downlink } *id interface-name* **(Versions >= 202111)**

Parameter Description

interface-name: interface name

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config monitor-link uplink add 1 Ethernet12
admin@sonic:~$ sudo config monitor-link downlink add 1 Ethernet13
```

1.6 show monitor-link all

Function

Run the **show monitor-link all** command to display the monitor link group configuration.

Syntax

show monitor-link all

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show monitor-link all
Monitor Link Group Configure
+------------+----------+------------+----------------+
|       group id | is_use       |       up_delay |       up_threshold |
+============+==========+============+================+
|                    1 | true           |               100 |                          1 |
+------------+----------+------------+----------------+
Monitor Link Ports Configure
+------------+-------------+----------+
|       group id | port name       | type           |
+============+=============+==========+
|                    1 | Ethernet12     | uplink       |
+------------+-------------+----------+
|                    1 | Ethernet13     | downlink |
+------------+-------------+----------+
```

1 VLAN Commands

Command	Function
config vlan	Add or delete the vlan.
config vlan proxy_arp	Enable or disable proxy ARP for a VLAN interface.
config vlan proxy_nd	Enable or disable proxy ND for a VLAN interface.
config vlan mac	Configure a MAC address for a VLAN interface.
config vlan member	Add or delete a member port into the already created vlan.
show vlan brief	Display brief information about all the vlans configured in the device. It displays the vlan ID, IP address (if configured for the vlan), list of vlan member ports, whether the port is tagged or in untagged mode, the DHCP Helper Address, and the proxy ARP status
show vlan config	Display all the vlan configuration.

1.1 config vlan

Function

Run the **config vlan** command to add or delete the vlan.

Syntax

config vlan { **add** | **del** } *vlan-id*

Parameter Description

add: Add VLAN

del: Delete VLAN

vlan-id: VLAN ID, for example, 100

Usage Guidelines

N/A

Examples

Create the VLAN "Vlan100" if it does not already exist

```
admin@sonic:~$ sudo config vlan add 100
```

Note

In products M2-W6930-64QC、M2-W6920-32QC2X and M2-W6510 series, there are a few points that need to be paid attention to:

The following points will occupy vlan resources:

- Each routed port needs to occupy 1 vlan resource.
- Each layer 3 aggregation port needs to occupy 1 vlan resource.
- Each time a vlan is created, it occupies a vlan resource.

After the VLAN recources occupied by the routing port are preempted by the user-configured VLAN, it will cause Layer 3 traffic interruption.

The interruption time caused by the preemption of VLAN resources occupied by a single routing port is at the millisecond level. As long as there are remaining VLAN resources in the system, the VLAN resources can be successfully occupied. In other words, you can create N routing ports and (4094 - N) arbitrary vlans.

When creating a VLAN, if the VLAN ressource is already occupied by a routed port, an error message will appear and the VLAN creation fails.

1.2 config vlan proxy_arp

Function

Run the **config vlan proxy_arp** command to enable or disable proxy ARP for a VLAN interface.

Syntax

config vlan proxy_arp *vlan-id* { **enabled** | **disabled** }

Parameter Description

vlan-id: VLAN ID.

enabled: Enable proxy ARP for a VLAN interface.

disabled: Disable proxy ARP for a VLAN interface.

Usage Guidelines

Adding the -u or --untagged flag will set the member in "untagged" mode.

Examples

```
admin@sonic:~$ sudo config vlan proxy_arp 1000 enabled
This command will enable proxy ARP for the interface 'Vlan1000'
```

1.3 config vlan proxy_nd

Function

Run the **config vlan proxy_nd** command to enable or disable proxy ND for a VLAN interface.

Syntax

config vlan proxy_nd *vlan-id* { **enabled** | **disabled** }

Parameter Description

vlan-id: VLAN ID.

enabled: Enable proxy ND for a VLAN interface.

disabled: Disable proxy ND for a VLAN interface.

Usage Guidelines

Adding the -u or --untagged flag will set the member in "untagged" mode.

Examples

```
admin@sonic:~$ sudo config vlan proxy_nd 1000 enabled
This command will enable proxy ND for the interface 'Vlan1000'
```

1.4 config vlan mac

Function

Run the **config vlan mac** command to configure a MAC address for a VLAN interface.

Syntax

config vlan mac *vlan-id* [*mac-address* | **default**]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config vlan mac 100 00:77:cc:12:34:
admin@sonic:~$ sudo config vlan mac 100 default
```

1.5 config vlan member

Function

Run the **config vlan member** command to add or delete a member port into the already created vlan.

Syntax

config vlan member { **add** | **del** } [**-u** | **--untagged**] [*vlan-id*] [*member-portname*]

Parameter Description

add: *Add VLAN member*

del: *Delete VLAN member*

vlan-id: VLAN ID, for example, 100.

member-portname: Vlan member port name.

Usage Guidelines

Adding the -u or --untagged flag will set the member in "untagged" mode.

Examples

```
admin@sonic:~$ sudo config vlan member add 100 Ethernet0
This command will add Ethernet0 as member of the vlan 100

admin@sonic:~$ sudo config vlan member add 100 Ethernet4
This command will add Ethernet4 as member of the vlan 100.
```

1.6 show vlan brief

Function

Run the **show vlan brief** command to display brief information about all the vlans configured in the device. It displays the vlan ID, IP address (if configured for the vlan), list of vlan member ports, whether the port is tagged or in untagged mode, the DHCP Helper Address, and the proxy ARP status

Syntax

show vlan brief

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vlan brief

+-------+----------+---------+--------+--------------------+-------------+
|VLAN ID|IP Address|Ports|Port Tagging| DHCP Helper Address|Proxy ARP      |
+=======+==========+=========+========+====================+==========
===+
|    100 |1.1.2.2/16|Ethernet0|tagged    | 192.0.0.1              | disabled      |
|          |              |Ethernet4|tagged    | 192.0.0.2              |                 |
|          |              |             |            | 192.0.0.3              |                 |
+-------+----------+---------+--------+--------------------+-------------+
```

1.7 show vlan config

Function

Run the **show vlan config** command to display all the vlan configuration.

Syntax

show vlan config

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vlan config
Name          VID   Member       Mode
-------   -----   ---------   ------
Vlan100       100   Ethernet0    tagged
Vlan100       100   Ethernet4    tagged
```

1 LLDP Commands

Command	Function
config lldp mode set	Set the LLDP mode for a specified interface.
show lldp mode	Display the brief summary of all LLDP neighbors.
show lldp neighbors	Display more details about all LLDP neighbors or only the neighbors connected to a specific interface.
show lldp table	Display the brief summary of all LLDP neighbors.

1.1 config lldp mode set

Function

Run the **config lldp mode set** command to set the LLDP mode for a specified interface.

Syntax

config lldp mode set *interface-name* { **rx** | **tx** | **txrx** | **disable** } **(Versions >= 202111)**

Parameter Description

interface-name: Interface name, for example, Ethernet1

rx | **tx** | **txrx** | **disable**: Packet sending and receiving modes supported by LLDP.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config lldp mode set Ethernet44 tx
```

1.2 show lldp mode

Function

Run the **show lldp mode** command to display the brief summary of all LLDP neighbors.

Syntax

show lldp mode [*interface-name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1 .

Usage Guidelines

N/A

Examples

To display all neighbors in all interfaces

```
admin@sonic:~$ show lldp mode
ports          lldp-mode
----------   -----------
Ethernet1     rx-and-tx
Ethernet2     rx-and-tx
Ethernet3     rx-and-tx
Ethernet4     rx-and-tx
Ethernet5     rx-and-tx
```

```
admin@sonic:~$ show lldp mode Ethernet22
  ports          lldp-mode
  ----------   -----------
  Ethernet22   rx-and-tx
```

Note
The LLDP MIB cannot be updated in real time when obtaining LLDP related configurations, and there is a 60s delay.

1.3 show lldp neighbors

Function

Run the **show lldp neighbors** command to display more details about all LLDP neighbors or only the neighbors connected to a specific interface.

Syntax

show lldp neighbors [*interface-name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

To display all neighbors in all interfaces

```
admin@sonic:~$ show lldp neighbors
-------------------------------------------------------------------------------
LLDP neighbors:
-------------------------------------------------------------------------------
Interface:      eth0, via: LLDP, RID: 1, Time: 0 day, 12:21:21
  Chassis:
    ChassisID:      mac 00:01:e8:81:e3:45
    SysName:          swtor-b2lab2-1610
    SysDescr:       SONiC Software Version: SONiC.SONiC_1.3.3_20230925044746 - HwSku: M2-W6510-
48GT4V - Distribution: Debian 11.7 - Kernel: 5.10.0-8-2-amd64
    TTL:              20
    Capability:     Repeater, on
    Capability:     Bridge, on
    Capability:     Router, on
  Port:
    PortID:         ifname GigabitEthernet 0/2
```

```
  VLAN:             162, pvid: yes
--------------------------------------------------------------------------------
Interface:      Ethernet116, via: LLDP, RID: 3, Time: 0 day, 12:20:49
  Chassis:
    ChassisID:      mac 4c:76:25:e7:f0:c0
    SysName:          T1-2
    SysDescr:       Debian GNU/Linux 8 (jessie) Linux 4.9.0-8-amd64 #1 SMP Debian 4.9.110-3+deb9u6
(2015-12-19) x86_64
    TTL:              120
    MgmtIP:           10.11.162.40
    Capability:     Bridge, on
    Capability:     Router, on
    Capability:     Wlan, off
    Capability:     Station, off
  Port:
    PortID:           local hundredGigE1/2
    PortDescr:      T0-2:hundredGigE1/30
```

Optionally, you can specify an interface name in order to display only that particular interface

```
admin@sonic:~$ show lldp neighbors Ethernet112
show lldp neighbors Ethernet112
--------------------------------------------------------------------------------
LLDP neighbors:
--------------------------------------------------------------------------------
Interface:      Ethernet112, via: LLDP, RID: 2, Time: 0 day, 19:24:17
  Chassis:
    ChassisID:      mac 4c:76:25:e5:e6:c0
    SysName:          T1-1
    SysDescr:       Debian GNU/Linux 8 (jessie) Linux 4.9.0-8-amd64 #1 SMP Debian 4.9.110-3+deb9u6
(2015-12-19) x86_64
    TTL:              120
    MgmtIP:           10.11.162.41
    Capability:     Bridge, on
    Capability:     Router, on
    Capability:     Wlan, off
    Capability:     Station, off
  Port:
    PortID:           local hundredGigE1/2
    PortDescr:      T0-2:hundredGigE1/29
--------------------------------------------------------------------------------
```

1.4 show lldp table

Function

Run the **show lldp table** command to display the brief summary of all LLDP neighbors.

Syntax

show lldp table

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show lldp table
Capability codes: (R) Router, (B) Bridge, (O) Other
LocalPort    RemoteDevice     RemotePortID     Capability      RemotePortDescr
---------    ------------   -------------   ------------   --------------------
Ethernet112    T1-1             hundredGigE1/2     BR          T0-2:hundredGigE1/29
Ethernet116    T1-2             hundredGigE1/2     BR          T0-2:hundredGigE1/30
eth0             swtor-b2lab2-1610    GigabitEthernet 0/2    OBR
------------------------------------------------
Total entries displayed:    3
```

1 NAT Commands

Command	Function
config nat add static	Add a static NAT or NAPT entry.
config nat add pool	Create a NAT pool used for dynamic Source NAT or NAPT translations. Pool can be configured in one of the following combinations.
config nat add binding	Create a NAT binding between a pool and an ACL. The following fields are needed for configuring the binding.
config nat add interface	Configure NAT zone on an L3 interface. Default value of NAT zone on an L3 interface is 0. Valid range of zone values is 0-3.
config nat feature	Config nat feature
config nat set	Set the NAT timeout values. Different timeout values can be configured for the NAT entry timeout, NAPT TCP entry timeout, NAPT UDP entry timeout.
config nat statistic	Enable or disable the NAT statistic.
sonic-clear nat translations	Clear the dynamic NAT and NAPT translation entries.
sonic-clear nat statistics	Clear the statistics of all the NAT and NAPT entries.
show nat config	Display the NAT configuration.
show nat statistics	Display the NAT translation statistics for each entry.
show nat translations	Display the NAT translation entries.

1.1 config nat add static

Function

Run the **config nat add static** command to add a static NAT or NAPT entry.

Note

When configuring the Static NAT entry, user has to specify the following fields with 'basic' keyword.

- Global IP address,
- Local IP address,
- NAT type (snat / dnat) to be applied on the Global IP address. Default value is dnat. This is optional argument.
- Twice NAT Id. This is optional argument used in case of twice nat configuration.

When configuring the Static NAPT entry, user has to specify the following fields.

- IP protocol type (tcp / udp)
- Global IP address + Port
- Local IP address + Port
- NAT type (snat / dnat) to be applied on the Global IP address + Port. Default value is dnat. This is optional argument.
- Twicw NAT Id. This is optional argument used in case of twice nat configuration.

Syntax

config nat add static { **basic** *global-ip local-ip* } | { **tcp** | **udp** | **sctp** } *global-ip global-port local-ip local-port* } [**-nat_type { snat** | **dnat** }] [**-twice_nat_id** *value*]

- To delete a static NAT or NAPT entry, use the command below. Giving the all argument deletes all the configured static NAT and NAPT entries.

config nat remove static { **basic** *global-ip local-ip* | { **tcp** | **udp** | **sctp** } *global-ip global-port local-ip local-port>* | **all** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config nat add static basic 65.55.45.1 12.12.12.14 -nat_type dnat
admin@sonic:~$ sudo config nat add static tcp 65.55.45.2 100 12.12.12.15 200 -nat_type dnat

admin@sonic:~$ show nat translations

Static NAT Entries ..... 2
Static NAPT Entries ..... 2
```

```
Dynamic NAT Entries ..... 0
Dynamic NAPT Entries ..... 0
Static Twice NAT Entries ..... 0
Static Twice NAPT Entries ..... 0
Dynamic Twice NAT Entries ..... 0
Dynamic Twice NAPT Entries ..... 0
Total SNAT/SNAPT Entries ..... 2
Total DNAT/DNAPT Entries ..... 2
Total Entries ..... 4

Protocol Source Destination Translated Source Translated
Destination
-------- --------- ---------- ---------- ----------
all 12.12.12.14 --- 65.55.42.1 ---
all --- 65.55.42.1 --- 12.12.12.14
tcp 12.12.12.15:200 --- 65.55.42.2:100 ---
tcp --- 65.55.42.2:100 --- 12.12.12.15:200
```

1.2 config nat add pool

Function

Run the **config nat add pool** command to create a NAT pool used for dynamic Source NAT or NAPT translations. Pool can be configured in one of the following combinations.

Note

Pool can be configured in one of the following combinations.

- Global IP address range (or)
- Global IP address + L4 port range (or)
- Global IP address range + L4 port range.

Syntax

config nat add pool *pool-name global-ip-range* [*global-port-range*]

- To delete a NAT pool, use the command. Pool cannot be removed if it is referenced by a NAT binding. Giving the pools argument removes all the configured pools.

config nat remove { **pool** *pool-name* | **pools** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config nat add pool pool1 65.55.45.2-65.55.45.10
admin@sonic:~$ sudo config nat add pool pool2 65.55.45.3 100-1024

admin@sonic:~$ show nat config pool

Pool Name         Global IP Range                Global Port Range
-----------    ----------------------    -------------------
pool1               65.55.45.2-65.55.45.10    ---
pool2               65.55.45.3                        100-1024
```

1.3 config nat add binding

Function

Run the **config nat add binding** command to create a NAT binding between a pool and an ACL. The following fields are needed for configuring the binding.

Note

The following fields are needed for configuring the binding.

- ACL is an optional argument. If ACL argument is not given, the NAT binding is applicable to match all traffic.
- NAT type is an optional argument. Only DNAT type is supported for binding.
- Twice NAT Id is an optional argument. This Id is used to form a twice nat grouping with the static NAT/NAPT entry configured with the same Id.

Syntax

config nat add binding *binding-name pool-name* [*acl-name*] [**-nat_type** { **snat** | **dnat** }] [**-twice_nat_id** *value*]

- To delete a NAT binding, use the command below. Giving the bindings argument removes all the configured bindings.

config nat remove { **binding** *binding-name* | **bindings** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config nat add binding bind1 pool1 acl1
admin@sonic:~$ sudo config nat add binding bind2 pool2

admin@sonic:~$ show nat config bindings

Binding Name      Pool Name      Access-List      Nat Type      Twice-NAT Id
--------------   -----------   -------------   ----------   --------------
bind1              pool1           acl1              snat           ---
bind2              pool2                             snat           ---
```

1.4 config nat add interface

Function

Run the **config nat add interface** command to configure NAT zone on an L3 interface. Default value of NAT zone on an L3 interface is 0. Valid range of zone values is 0-3.

Syntax

config nat add interface *interface-name* **-nat_zone** *value*

- To reset the NAT zone on an interface, use the command below. Giving the interfaces argument resets the NAT zone on all the L3 interfaces to 0.

config nat remove { **interface** *interface-name*) | **interfaces** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config nat add interface Ethernet28 -nat_zone 1

admin@sonic:~$ show nat config zones

Port              Zone
----------   ------
Ethernet0          0
Ethernet28         1
Ethernet22         0
Vlan2091           0
```

1.5 config nat feature

Function

Run the **config nat feature** command to config nat feature

Syntax

config nat feature { **enable** | **disable** }

Parameter Description

enable: Enbale the NAT feature.

disable: Disable the NAT feature.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config nat feature enable
admin@sonic:~$ sudo config nat feature disable
```

1.6 config nat set

Function

Run the **config nat set** command to set the NAT timeout values. Different timeout values can be configured for the NAT entry timeout, NAPT TCP entry timeout, NAPT UDP entry timeout.

Syntax

config nat set { **tcp-timeout** | **timeout** | **udp-timeout** | **sctp-timeout** } *value*

- To reset the timeout values to the default values, use the command.

config nat reset { **tcp-timeout** | **timeout** | **udp-timeout** | **sctp-timeout** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config nat set tcp-timeout 3600

admin@sonic:~$ show nat config globalvalues
```

```
Admin Mode          : enabled
Global Timeout    : 600 secs
TCP Timeout         : 86400 secs
SCTP Timeout       : 86400 secs
UDP Timeout         : 300 secs
Flow Statistic    : enabled
```

1.7 config nat statistic

Function

Run the **config nat statistic** command to enable or disable the NAT statistic.

Syntax

config nat statistic { **enable** | **disable** }

Parameter Description

disable: Disable the NAT statistic.

enable: Enbale the NAT statistic.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config nat statistic enable
admin@sonic:~$ sudo config nat statistic disable
```

1.8 sonic-clear nat translations

Function

Run the **sonic-clear nat translations** command to clear the dynamic NAT and NAPT translation entries.

Syntax

sonic-clear nat translations

Parameter Description

N/A

Usage Guidelines

N/A

Examples

N/A

1.9 sonic-clear nat statistics

Function

Run the **sonic-clear nat statistics** command to clear the statistics of all the NAT and NAPT entries.

Syntax

sonic-clear nat statistics

Parameter Description

N/A

Usage Guidelines

N/A

Examples

N/A

1.10 show nat config

Function

Run the **show nat config** command to display the NAT configuration.

Syntax

show nat config [**static** | **pool** | **bindings** | **globalvalues** | **zones**]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show nat config static

Nat Type   IP Protocol Global IP        Global L4 Port   Local IP         Local L4 Port   Twice-Nat Id
--------   ----------- ------------   --------------   -------------   -------------   -----------
--
dnat       all         65.55.45.5       ---              10.0.0.1        ---             ---
dnat       all         65.55.45.6       ---              10.0.0.2        ---             ---
dnat       tcp          65.55.45.7       2000             20.0.0.1        4500            1
snat       tcp          20.0.0.2         4000             65.55.45.8      1030            1
```

```
admin@sonic:~$ show nat config pool

Pool Name         Global IP Range               Global L4 Port Range
------------    -------------------------    --------------------
Pool1             65.55.45.5                    1024-65535
Pool2              65.55.45.6-65.55.45.8         ---
Pool3              65.55.45.10-65.55.45.15       500-1000

admin@sonic:~$ show nat config bindings

Binding Name    Pool Name        Access-List      Nat Type   Twice-Nat Id
------------    ------------    ------------    --------   ------------
Bind1             Pool1             ---               snat        ---
Bind2              Pool2             1                 snat        1
Bind3              Pool3             2                  snat        --

admin@sonic:~$ show nat config globalvalues

Admin Mode        : enabled
Global Timeout : 600 secs
TCP Timeout       : 86400 secs
UDP Timeout       : 300 secs

admin@sonic:~$ show nat config zones

Port          Zone
----          ----
Ethernet2   0
Vlan100      1
```

1.11 show nat statistics

Function

Run the **show nat statistics** command to display the NAT translation statistics for each entry.

Syntax

show nat statistics

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show nat statistics

Protocol Source              Destination           Packets             Bytes
-------- ---------           --------------        -------------     -------------
all      10.0.0.1            ---                      802            1009280
all      10.0.0.2            ---                       23               5590
tcp      20.0.0.1:4500       ---                      110              12460
udp      20.0.0.1:4000       ---                     1156             789028
tcp      20.0.0.1:6000       ---                       30              34800
tcp      20.0.0.1:5000       65.55.42.1:2000          128             110204
tcp      20.0.0.1:5500       65.55.42.1:2000            8               3806
```

1.12 show nat translations

Function

Run the **show nat translations** command to display the NAT translation entries.

Syntax

show nat translations [**count**]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show nat translations

Static NAT Entries ..... 4
Static NAPT Entries ..... 2
Dynamic NAT Entries ..... 0
Dynamic NAPT Entries ..... 4
Static Twice NAT Entries ..... 0
Static Twice NAPT Entries ..... 4
Dynamic Twice NAT Entries ..... 0
Dynamic Twice NAPT Entries ..... 0
Total SNAT/SNAPT Entries ..... 9
Total DNAT/DNAPT Entries ..... 9
Total Entries ..... 14

Protocol Source              Destination         Translated Source    Translated Destination
-------- ---------           --------------      -----------------    ----------------------
```

```
all        10.0.0.1           ---                65.55.42.2         ---
all        ---                65.55.42.2         ---                10.0.0.1
all        10.0.0.2           ---                65.55.42.3         ---
all        ---                65.55.42.3         ---                10.0.0.2
tcp        20.0.0.1:4500      ---                65.55.42.1:2000    ---
tcp        ---                65.55.42.1:2000    ---                20.0.0.1:4500
udp        20.0.0.1:4000      ---                65.55.42.1:1030    ---
udp        ---                65.55.42.1:1030    ---                20.0.0.1:4000
tcp        20.0.0.1:6000      ---                65.55.42.1:1024    ---
tcp        ---                65.55.42.1:1024    ---                20.0.0.1:6000
tcp        20.0.0.1:5000      65.55.42.1:2000    65.55.42.1:1025    20.0.0.1:4500
tcp        20.0.0.1:4500      65.55.42.1:1025    65.55.42.1:2000    20.0.0.1:5000
tcp        20.0.0.1:5500      65.55.42.1:2000    65.55.42.1:1026    20.0.0.1:4500
tcp        20.0.0.1:4500      65.55.42.1:1026    65.55.42.1:2000    20.0.0.1:5500

admin@sonic:~$ show nat translations count

Static NAT Entries ..... 4
Static NAPT Entries ..... 2
Dynamic NAT Entries ..... 0
Dynamic NAPT Entries ..... 4
Static Twice NAT Entries ..... 0
Static Twice NAPT Entries ..... 4
Dynamic Twice NAT Entries ..... 0
Dynamic Twice NAPT Entries ..... 0
Total SNAT/SNAPT Entries ..... 9
Total DNAT/DNAPT Entries ..... 9
Total Entries ..... 14
```

1 ARP Commands

Command	Function
show arp	Display the ARP entries in the device with following options.
show arp-aging-time	Display the ARP aging time.

1.1 show arp

Function

Run the **show arp** command to display the ARP entries in the device with following options.

- Display the entire table.
- Display the ARP entries learnt on a specific interface.
- Display the ARP of a specific ip-address.

Syntax

show arp [**-if** *interface-name*] [*ip-address*]

Parameter Description

-if *interface-name*: Displays the ARP specific to the specified interface.

ip-address: Displays the ARP specific to the specicied ip-address.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show arp
Address                  MacAddress                  Iface             Vlan        Vrf            Status
-----------    -----------------    ----------    ------    -------    ---------
10.110.197.1     58:69:6c:dc:e8:56     eth0                -            default     reachable
41.0.0.250          00:74:9c:12:34:02     Ethernet41     -            default     reachable
Total number of entries 2
```

Optionally, you can specify the interface in order to display the ARPs learnt on that particular interface.

```
admin@sonic:~$ show arp -if Ethernet41
Address           MacAddress                  Iface             Vlan        Vrf            Status
----------    -----------------    ----------    ------    -------    ---------
41.0.0.250     00:74:9c:12:34:02     Ethernet41     -            default     reachable
Total number of entries 1
```

Optionally, you can specify an IP address in order to display only that particular entry.

```
admin@sonic:~$ show arp 41.0.0.250
Address           MacAddress                  Iface             Vlan        Vrf            Status
----------    -----------------    ----------    ------    -------    ---------
41.0.0.250     00:74:9c:12:34:02     Ethernet41     -            default     reachable
Total number of entries 1
```

1.2 show arp-aging-time

Function

Run the **show arp-aging-time** command to display the ARP aging time.

Syntax

show arp-aging-time

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show arp-aging-time
Interface            Arp Reachable-time(sec)        Arp Stale-time(sec)
-----------    -------------------------    --------------------
Ethernet1                                    45                                1800
Ethernet2                                    45                                1800
Ethernet3                                    45                                1800
Ethernet4                                    45                                1800
Ethernet5                                    45                                1800
Ethernet6                                    45                                1800
Ethernet7                                    45                                1800
Ethernet8                                    45                                1800
Ethernet9                                    45                                1800
Ethernet10                                   45                                1800
Ethernet11                                   45                                1800
Ethernet12                                   45                                1800
Ethernet13                                   45                                1800
...
```

1 DHCP Relay Commands

Command	Function
config dhcp_relay ipv4	Enable or disable DHCPv4 Relay function.
config dhcp_relay ipv4 helper	Add or delete IPv4 DHCP Relay helper addresses from a VLAN. Note that more than one IPv4 DHCP Relay helper address can be added to or removed from a VLAN interface.
config dhcp_relay ipv4 opt82	Enable or disable DHCPv4 Relay option 82 function.
config dhcp_relay ipv6	Enable or disable DHCPv6 Relay function.
config dhcp_relay ipv6 destination	Add or delete IPv6 DHCP Relay destination addresses from a VLAN. Note that more than one IPv6 DHCP Relay destination address can be added to or deleted from a VLAN interface.
config dhcp_relay ipv6 opt18	Enable or disable DHCPv6 Relay option 18 (interface-id option) on a VLAN interface.
config dhcp_relay ipv6 opt79	Enable or disable DHCPv6 Relay option 79 (Client Link-Layer Address Option) on a VLAN interface.
config feature state dhcp_relay	Load and start dhcp_relay docker.
config vlan dhcp_relay	Add or delete IPv4 DHCP Relay helper addresses to a VLAN. Note that more than one DHCP Relay helper addresses can be configured on a VLAN interface.
config vlan dhcp_relay disable --version 4	Disable DHCPv4 Relay function.
config vlan dhcp_relay enable --version 4	Enable DHCPv4 Relay function.
config vlan dhcp_relay v4_opt82	Enable or disable DHCPv4 Relay option 82 function.
show dhcp_relay ipv4 helper	Display IPv4 DHCP Relay helper.
show dhcp_relay ipv6 counters	Display IPv6 DHCP Relay counters.
show dhcp_relay ipv6 destination	Display IPv6 DHCP Relay destination.

sonic-clear dhcp_relay ipv6 counter	Clear IPv6 DHCP Relay counters.

1.1 config dhcp_relay ipv4

Function

Run the **config dhcp_relay ipv4** command to enable or disable DHCPv4 Relay function.

Syntax

config dhcp_relay ipv4 { **enable** | **disable** }

Parameter Description

enable: Enable DHCPv4 Relay function.

disable: Disable DHCPv4 Relay function.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config dhcp_relay ipv4 enable
Restarting DHCP relay service...
admin@sonic:~$ sudo config dhcp_relay ipv4 disable
Restarting DHCP relay service...
```

1.2 config dhcp_relay ipv4 helper

Function

Run the **config dhcp_relay ipv4 helper** command to add or delete IPv4 DHCP Relay helper addresses from a VLAN. Note that more than one IPv4 DHCP Relay helper address can be added to or removed from a VLAN interface.

Syntax

config dhcp_relay ipv4 helper { **add** | **del** } [*vlan-id*] [*dhcp-helper-ips*]

Parameter Description

add: Add IPv4 DHCP Relay helper addresses.

del: Delete IPv4 DHCP Relay helper addresses.

vlan-id: VLAN ID.

dhcp-helper-ips: IPv4 addresses of DHCPv4 Server. It can be one or more. If there are multiple, they should be separated by spaces.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config dhcp_relay ipv4 helper add 1000 7.7.7.7
Added DHCP relay address [7.7.7.7] to Vlan1000
Restarting DHCP relay service...
admin@sonic:~$ sudo config dhcp_relay ipv4 helper add 1000 7.7.7.7 1.1.1.1
Added DHCP relay address [7.7.7.7, 1.1.1.1] to Vlan1000
Restarting DHCP relay service...
admin@sonic:~$ sudo config dhcp_relay ipv4 helper del 1000 7.7.7.7
Removed DHCP relay address [7.7.7.7] from Vlan1000
Restarting DHCP relay service...
admin@sonic:~$ sudo config dhcp_relay ipv4 helper del 1000 7.7.7.7 1.1.1.1
Removed DHCP relay address [7.7.7.7, 1.1.1.1] from Vlan1000
Restarting DHCP relay service...
```

1.3 config dhcp_relay ipv4 opt82

Function

Run the **config dhcp_relay ipv4 opt82** command to enable or disable DHCPv4 Relay option 82 function.

Syntax

config dhcp_relay ipv4 opt82 { **enable** | **disable** }

Parameter Description

enable: Enable DHCPv4 Relay option 82 function.

disable: Disable DHCPv4 Relay option 82 function.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config dhcp_relay ipv4 opt82 enable
Restarting DHCP relay service...
admin@sonic:~$ sudo config dhcp_relay ipv4 opt82 disable
Restarting DHCP relay service...
```

1.4 config dhcp_relay ipv6

Function

Run the **config dhcp_relay ipv6** command to enable or disable DHCPv6 Relay function.

Syntax

config dhcp_relay ipv6 { **enable** | **disable** }

Parameter Description

enable: Enable DHCPv6 Relay function.

disable: Disable DHCPv6 Relay function.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config dhcp_relay ipv6 enable
Restarting DHCP relay service...
admin@sonic:~$ sudo config dhcp_relay ipv6 disable
Restarting DHCP relay service..
```

1.5 config dhcp_relay ipv6 destination

Function

Run the **config dhcp_relay ipv6 destination** command to add or delete IPv6 DHCP Relay destination addresses from a VLAN. Note that more than one IPv6 DHCP Relay destination address can be added to or deleted from a VLAN interface.

Syntax

config dhcp_relay ipv6 destination { **add** | **del** } *vlan-id dhcp-destination-ips*

Parameter Description

add: Add IPv6 DHCP Relay destination addresses.

del: Delete IPv6 DHCP Relay destination addresses.

vlan-id: VLAN ID.

dhcp-destination-ips: IPv6 addresses of DHCPv6 Relay destination address. It can be one or more. If there are multiple, they should be separated by spaces.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config dhcp_relay ipv6 destination add 1000 fc02:2000::1
Added DHCP relay address [fc02:2000::1] to Vlan1000
Restarting DHCP relay service...
admin@sonic:~$ sudo config dhcp_relay ipv6 destination add 1000 fc02:2000::1 fc02:2000::2
Added DHCP relay address [fc02:2000::1, fc02:2000::2] to Vlan1000
Restarting DHCP relay service...
admin@sonic:~$ sudo config dhcp_relay ipv6 destination del 1000 fc02:2000::1
Removed DHCP relay address [fc02:2000::1] from Vlan1000
```

```
Restarting DHCP relay service...
admin@sonic:~$ sudo config dhcp_relay ipv6 destination del 1000 fc02:2000::1 fc02:2000::2
Removed DHCP relay address [fc02:2000::1, fc02:2000::2] from Vlan1000
Restarting DHCP relay service...
```

1.6 config dhcp_relay ipv6 opt18

Function

Run the **config dhcp_relay ipv6 opt18** command to enable or disable DHCPv6 Relay option 18 (interface-id option) on a VLAN interface.

Syntax

config dhcp_relay ipv6 opt18 { **enable** | **disable** } *vlan-id*

Parameter Description

enable: Enable DHCPv6 Relay option 18 (interface-id option).

disable: Disable DHCPv6 Relay option 18 (interface-id option).

vlan-id: VLAN ID.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config dhcp_relay ipv6 opt18 enable 100
Restarting DHCP relay service...
admin@sonic:~$ sudo config dhcp_relay ipv6 opt18 disable 100
Restarting DHCP relay service...
```

1.7 config dhcp_relay ipv6 opt79

Function

Run the **config dhcp_relay ipv6 opt79** command to enable or disable DHCPv6 Relay option 79 (Client Link-Layer Address Option) on a VLAN interface.

Syntax

config dhcp_relay ipv6 opt79 { **enable** | **disable** } *vlan-id*

Parameter Description

enable: Enable DHCPv6 Relay option 79 (Client Link-Layer Address Option).

disable: Disable DHCPv6 Relay option 79 (Client Link-Layer Address Option).

vlan-id: VLAN ID.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config dhcp_relay ipv6 opt79 enable 100
Restarting DHCP relay service...
admin@sonic:~$ sudo config dhcp_relay ipv6 opt79 disable 100
Restarting DHCP relay service...
```

1.8 config feature state dhcp_relay

Function

Run the **config feature state dhcp_relay** command to load and start dhcp_relay docker.

Note
Please refer Feature config commands for the details of this command.

Syntax

config feature state dhcp_relay { **enabled** | **disabled** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config feature state dhcp_relay enabled
```

1.9 config vlan dhcp_relay

Function

Run the **config vlan dhcp_relay** command to add or delete IPv4 DHCP Relay helper addresses to a VLAN. Note that more than one DHCP Relay helper addresses can be configured on a VLAN interface.

Syntax

config vlan dhcp_relay { **add** | **del** } *vlan-id dhcp-relay-destination-ips*

Parameter Description

add: Add IPv4 DHCP Relay helper addresses.

del: Delete IPv4 DHCP Relay helper addresses.

vlan-id: VLAN ID.

dhcp-relay-destination-ips: IPv4 addresses of DHCPv4 Server. It can be one or more. If there are multiple, they should be separated by spaces.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config vlan dhcp_relay add 1000 7.7.7.7
Added DHCP relay destination address ['7.7.7.7'] to Vlan1000
Restarting DHCP relay service...

admin@sonic:~$ sudo config vlan dhcp_relay add 1000 7.7.7.7 1.1.1.1
Added DHCP relay destination address ['7.7.7.7', '1.1.1.1'] to Vlan1000
Restarting DHCP relay service...

admin@sonic:~$ sudo config vlan dhcp_relay del 1000 7.7.7.7
Removed DHCP relay destination address 7.7.7.7 from Vlan1000
Restarting DHCP relay service...

admin@sonic:~$ sudo config vlan dhcp_relay del 1000 7.7.7.7 1.1.1.1
Removed DHCP relay destination address ('7.7.7.7', '1.1.1.1') from Vlan1000
Restarting DHCP relay service...
```

1.10 config vlan dhcp_relay disable --version 4

Function

Run the **config vlan dhcp_relay disable** --version 4 command to disable DHCPv4 Relay function.

Syntax

config vlan dhcp_relay disable --version 4

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config vlan dhcp_relay disable --version 4
Disable DHCPv4 relay
Stopping DHCPv4 relay service...
```

1.11 config vlan dhcp_relay enable --version 4

Function

Run the **config vlan dhcp_relay enable --version 4** command to enable DHCPv4 Relay function.

Syntax

config vlan dhcp_relay enable --version 4

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config vlan dhcp_relay enable --version 4
Enable DHCPv4 relay
Starting DHCPv4 relay service...
```

1.12 config vlan dhcp_relay v4_opt82

Function

Run the **config vlan dhcp_relay v4_opt82** command to enable or disable DHCPv4 Relay option 82 function.

Syntax

config vlan dhcp_relay v4-opt82 { **enable** | **disable** }

Parameter Description

enable: Enable DHCPv4 Relay option 82 function.

disable: Disable DHCPv4 Relay option 82 function.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config vlan dhcp_relay v4-opt82 enable
DHCPv4 relay option82 has been enabled
Restarting DHCPv4 relay service...

admin@sonic:~$ sudo config vlan dhcp_relay v4_opt82 disable
DHCPv4 relay option82 has been disabled
```

```
Restarting DHCPv4 relay service...
```

1.13 show dhcp_relay ipv4 helper

Function

Run the **show dhcp_relay ipv4 helper** command to display IPv4 DHCP Relay helper.

Syntax

show dhcp_relay ipv4 helper

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show dhcp_relay ipv4 helper
+-------------+----------------------+
|    Interface      |    DHCP Relay Address |
+===========+==================+
|      Vlan1000     |                 172.2.2.1 |
+-------------+----------------------+
```

1.14 show dhcp_relay ipv6 counters

Function

Run the **show dhcp_relay ipv6 counters** command to display IPv6 DHCP Relay counters.

Syntax

show dhcp_relay ipv6 counters

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show dhcp_relay ipv6 counters
         Message Type   Vlan1000
-------------------   ----------
              Unknown          0
```

```
                Solicit         0
              Advertise 0
                Request 5
                Confirm 0
                  Renew 0
                 Rebind 0
                  Reply 0
                Release 0
                Decline 0
            Reconfigure         0
Information-Request         0
          Relay-Forward 0
            Relay-Reply         0
              Malformed         0
```

1.15 show dhcp_relay ipv6 destination

Function

Run the **show dhcp_relay ipv6 destination** command to display IPv6 DHCP Relay destination.

Syntax

show dhcp_relay ipv6 destination

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show dhcp_relay ipv6 destination
+-------------+----------------------+
|    Interface      |    DHCP Relay Address |
+===========+==================+
|     Vlan1000    |                  2001::1 |
+-------------+----------------------+
```

1.16 sonic-clear dhcp_relay ipv6 counter

Function

Run the **sonic-clear dhcp_relay ipv6 counter** command to clear IPv6 DHCP Relay counters.

Syntax

sonic-clear dhcp_relay ipv6 counter [**-i** *interface*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo sonic-clear dhcp_relay ipv6 counters
```

Go Back To Beginning of the document or Beginning of this section

1 DHCP Client Commands

Command	Function
config interface ip dhcp4_client	Enable or disable DHCP4 client function of an interface. This function uses the DHCPv4 protocol to obtain an IPv4 address and configuration parameters.
config interface ip dhcp6_client ia_na	Enable or disable DHCP6 client ia_na function of an interface. This function uses the DHCPv6 protocol to obtain whatever IPv6 addresses are available along with configuration parameters.
config interface ip dhcp6_client stateless_configuration	Enable or disable DHCP6 client stateless_configuration function of an interface. This function uses Information-request to get only stateless configuration parameters (i.e., without address).
show ip interface dhcp4_client	Show the lease information of the IPv4 address obtained by the interface with the DHCP4 client function enabled.
show ipv6 interface dhcp6_client	Show the lease information of the IPv6 address obtained by the interface with the DHCP6 client ia_na function enabled.

1.1 config interface ip dhcp4_client

Function

Run the **config interface ip dhcp4_client** command to enable or disable DHCP4 client function of an interface. This function uses the DHCPv4 protocol to obtain an IPv4 address and configuration parameters.

Syntax

config interface ip dhcp4_client { **enable** | **disable** } *interface-name*

Parameter Description

enable: Enables DHCP4 client function of an interface.

disable: Disables DHCP4 client function of an interface.

interface-name: Specifies the interface name. Supported interfaces include Ethernet, PortChannel, SVI, and sub-interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface ip dhcp4_client enable Ethernet1
admin@sonic:~$ sudo config interface ip dhcp4_client disable Ethernet1
```

1.2 config interface ip dhcp6_client ia_na

Function

Run the **config interface ip dhcp6_client ia_na** command to enable or disable DHCP6 client ia_na function of an interface. This function uses the DHCPv6 protocol to obtain whatever IPv6 addresses are available along with configuration parameters.

Syntax

config interface ip dhcp6_client ia_na { **enable** | **disable** } *interface-name*

Parameter Description

enable: Enables DHCP6 client ia_na function of an interface.

disable: Disables DHCP6 client ia_na function of an interface.

interface-name: Specifies the interface name. Supported interfaces include Ethernet, PortChannel, SVI, and sub-interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface ip dhcp6_client ia_na enable Ethernet1
admin@sonic:~$ sudo config interface ip dhcp6_client ia_na disable Ethernet1
```

1.3 config interface ip dhcp6_client stateless_configuration

Function

Run the **config interface ip dhcp6_client stateless_configuration** command to enable or disable DHCP6 client stateless_configuration function of an interface. This function uses Information-request to get only stateless configuration parameters (i.e., without address).

Syntax

sudo config interface ip dhcp6_client stateless_configuration { **enable** | **disable** } *interface-name*

Parameter Description

enable: Enables DHCP6 client stateless_configuration function of an interface.

disable: Disables DHCP6 client stateless_configuration function of an interface.

interface-name: Specifies the interface name. Supported interfaces include Ethernet, PortChannel, SVI, and sub-interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface ip dhcp6_client stateless_configuration enable Ethernet1
admin@sonic:~$ sudo config interface ip dhcp6_client stateless_configuration disable Ethernet1
```

1.4 show ip interface dhcp4_client

Function

Run the **show ip interface dhcp4_client** command to show the lease information of the IPv4 address obtained by the interface with the DHCP4 client function enabled.

Syntax

show ip interface dhcp4_client { **all** | *interface-name* } **leases**

Parameter Description

all: Displays IPv4 lease information obtained by all interfaces with the DHCP4 client function enabled.

interface-name: Displays the lease information of the specified interface. Supported interfaces include Ethernet, PortChannel, SVI, and sub-interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ip interfaces dhcp4_client all leases
---------------------------------------
interface : Ethernet57
fixed-address 11.0.0.2;
option subnet-mask 255.255.255.0;
option dhcp-lease-time 600;
option dhcp-message-type 5;
option dhcp-server-identifier 11.0.0.1;
option domain-name "example.org";
renew 1 2024/01/15 09:18:19;
rebind 1 2024/01/15 09:18:19;
expire 1 2024/01/15 09:18:19;
---------------------------------------
interface : Ethernet61;
fixed-address 12.0.0.2;
option subnet-mask 255.255.255.0;
option dhcp-lease-time 600;
option dhcp-message-type 5;
option dhcp-server-identifier 11.0.0.1;
option domain-name "example.org";
renew 1 2024/01/15 09:23:35;
rebind 1 2024/01/15 09:27:38;
expire 1 2024/01/15 09:28:53;
---------------------------------------

admin@sonic:~$show ip interfaces dhcp4_client Ethernet61 leases
---------------------------------------
interface : Ethernet61;
fixed-address 12.0.0.2;
option subnet-mask 255.255.255.0;
option dhcp-lease-time 600;
option dhcp-message-type 5;
option dhcp-server-identifier 11.0.0.1;
option domain-name "example.org";
renew 1 2024/01/15 09:23:35;
rebind 1 2024/01/15 09:27:38;
expire 1 2024/01/15 09:28:53;
---------------------------------------

admin@sonic:~$
```

1.5 show ipv6 interface dhcp6_client

Function

Run the **show ipv6 interface dhcp6_client** command to show the lease information of the IPv6 address obtained by the interface with the DHCP6 client ia_na function enabled.

Syntax

show ipv6 interface dhcp6_client { **all** | *interface-name* } **leases**

Parameter Description

all: Displays IPv6 lease information obtained by all interfaces with the DHCP6 client ia_na function enabled.

interface-name: Displays the lease information of the specified interface. Supported interfaces include Ethernet, PortChannel, SVI, and sub-interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ipv6 interfaces dhcp6_client all leases
-------------------------------------
interface : Ethernet61
ia-na e6:74:47:86 {
starts 1705294314;
renew 3600;
rebind 7200;
iaaddr 3000::10 {
starts 1705294314;
preferred-life 601200;
max-life 2588400;
}
}
option dhcp6.client-id 0:1:0:1:2d:37:61:c7:c0:b8:e6:74:47:86;
option dhcp6.server-id 0:1:0:1:2d:34:ef:9a:0:74:9c:12:34:2;
option dhcp6.name-servers 3ffe:501:ffff:100:200:ff:fe00:3f3e;
option dhcp6.domain-search "test.example.com.", "example.com.";
-------------------------------------
interface : Ethernet77
ia-na e6:74:47:86 {
starts 1705289033;
renew 43200;
rebind 69120;
iaaddr 2001::1 {
starts 1705289033;
```

```
preferred-life 86400;
max-life 86400;
}
}
option dhcp6.client-id 0:1:0:1:2d:37:61:c7:c0:b8:e6:74:47:86;
option dhcp6.server-id 0:3:0:1:58:69:6c:7a:98:93;
option dhcp6.name-servers 2001::1:2;
option dhcp6.domain-search "bogus.com.";
-------------------------------------

admin@sonic:~$
admin@sonic:~$ show ipv6 interfaces dhcp6_client Ethernet61 leases
-------------------------------------
interface : Ethernet61
ia-na e6:74:47:86 {
starts 1705294314;
renew 3600;
rebind 7200;
iaaddr 3000::10 {
starts 1705294314;
preferred-life 601200;
max-life 2588400;
}
}
option dhcp6.client-id 0:1:0:1:2d:37:61:c7:c0:b8:e6:74:47:86;
option dhcp6.server-id 0:1:0:1:2d:34:ef:9a:0:74:9c:12:34:2;
option dhcp6.name-servers 3ffe:501:ffff:100:200:ff:fe00:3f3e;
option dhcp6.domain-search "test.example.com.", "example.com.";
-------------------------------------

admin@sonic:~$
```

1 Route Management Commands

Command	Function
ip route	Configure a static IPv4 route.
ip route arp-to-host interface	Enable ARP-to-host routing on a specified interface.
ip route arp-to-host tag	Configure the tag of the ARP-to-host route.
ipv6 route	Configure a static IPv6 route.
ipv6 route nd-to-route interface	Enable nd-to-route on a specified interface.
ipv6 route nd-to-route tag	Configure the tag of the nd-to-route.
show ip interfaces	Display the details about all the Layer3 IP interfaces in the device for which IP address has been assigned. The type of interfaces include the following.
show ip protocol	Display the route-map that is configured for the routing protocol.
show ip route	Display either all the route entries from the routing table or a ipv4 specific route.
show ipv6 interfaces	Display the details about all the Layer3 IPv6 interfaces in the device for which IPv6 address has been assigned. The type of interfaces include the following.
show ipv6 protocol	Display the route-map that is configured for the IPv6 routing protocol.
show ipv6 route	Display either all the IPv6 route entries from the routing table or a specific IPv6 route.

1.1 ip route

Function

Run the **ip route** command to configure a static IPv4 route.

Syntax

ip route *NETWORK GATEWAY* [**DISTANCE**] [**table TABLENO**] [**nexthop-vrf VRFNAME**] [**vrf VRFNAME**] [**tag TAG**]

ip route *NETWORK IFNAME* [**DISTANCE**] [**table TABLENO**] [**nexthop-vrf VRFNAME**] [**vrf VRFNAME**] [**tag TAG**]

ip route *NETWORK GATEWAY* **IFNAME** [**DISTANCE**] [**table TABLENO**] [**nexthop-vrf VRFNAME**] [**vrf VRFNAME**] [**tag TAG**]

ip route *NETWORK* [**blackhole** | **reject**] [**DISTANCE**] [**table TABLENO**] [**nexthop-vrf VRFNAME**] [**vrf VRFNAME**] [**tag TAG**]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "ip route 1.1.1.1/24 2.2.2.2"
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "no ip route 1.1.1.1/24 2.2.2.2"
```

1.2 ip route arp-to-host interface

Function

Run the **ip route arp-to-host interface** command to enable ARP-to-host routing on a specified interface.

Syntax

ip route arp-to-host interface *interface-name*

Parameter Description

interface-name: interface name

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "ip route arp-to-host interface Ethernet1"
```

```
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "no ip route arp-to-host interface Ethernet1"
```

1.3 ip route arp-to-host tag

Function

Run the **ip route arp-to-host tag** command to configure the tag of the ARP-to-host route.

Syntax

ip route arp-to-host tag *tag-number*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "ip route arp-to-host tag 10"
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "no ip route arp-to-host tag"
```

1.4 ipv6 route

Function

Run the **ipv6 route** command to configure a static IPv6 route.

Syntax

ipv6 route *NETWORK GATEWAY* [**DISTANCE**] [**table TABLENO**] [**nexthop-vrf VRFNAME**] [**vrf VRFNAME**] [**tag TAG**]

ipv6 route *NETWORK IFNAME* [**DISTANCE**] [**table TABLENO**] [**nexthop-vrf VRFNAME**] [**vrf VRFNAME**] [**tag TAG**]

ipv6 route *NETWORK GATEWAY IFNAME* [**DISTANCE**] [**table TABLENO**] [**nexthop-vrf VRFNAME**] [**vrf VRFNAME**] [**tag TAG**]

ipv6 route *NETWORK* **[blackhole** | **reject**] [**DISTANCE**] [**table TABLENO**] [**nexthop-vrf VRFNAME**] [**vrf VRFNAME**] [**tag TAG**]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "ipv6 route 100::1/120 200::1"
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "no ipv6 route 100::1/120 200::1"
```

1.5 ipv6 route nd-to-route interface

Function

Run the **ipv6 route nd-to-route interface** command to enable nd-to-route on a specified interface.

Syntax

ipv6 route nd-to-route interface *interface-name* [**ipv6-prefix** *X:X:X:X::X/M*] [**prefix-len** *masklen*]

Parameter Description

interface-name: interface name

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "ipv6 route nd-to-route interface Ethernet1
prefix-len 120"
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "no ipv6 route nd-to-route interface Ethernet1"
```

1.6 ipv6 route nd-to-route tag

Function

Run the **ipv6 route nd-to-route tag** command to configure the tag of the nd-to-route.

Syntax

ipv6 route nd-to-route tag *tag-number*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "ipv6 route nd-to-route tag 10"
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "no ipv6 route nd-to-route tag"
```

1.7 show ip interfaces

Function

Run the **show ip interfaces** command to display the details about all the Layer3 IP interfaces in the device for which IP address has been assigned. The type of interfaces include the following.

- Front panel physical ports.
- PortChannel.
- VLAN interface.
- Loopback interfaces
- docker interface
- management interface

Syntax

show ip interfaces

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ip interfaces
Interface             Master                IPv4 address/mask          Admin/Oper
------------      ------------      ------------------      --------------
Loopback0                                      1.0.0.1/32                      up/up
Loopback11          Vrf-red                 11.1.1.1/32                   up/up
Loopback100         Vrf-blue                100.0.0.1/32                  up/up
PortChannel01                                  10.0.0.56/31                   up/down
PortChannel02                                  10.0.0.58/31                   up/down
PortChannel03                                  10.0.0.60/31                   up/down
PortChannel04                                  10.0.0.62/31                   up/down
Vlan100                 Vrf-red               1001.1.1/24                   up/up
Vlan1000                                       192.168.0.1/27                 up/up
docker0                                        240.127.1.1/24                 up/down
eth0                                           10.3.147.252/23                up/up
lo                                             127.0.0.1/8                    up/up
```

1.8 show ip protocol

Function

Run the **show ip protocol** command to display the route-map that is configured for the routing protocol.

Syntax

show ip protocol

Parameter Description

N/A

Usage Guidelines

Notes
Refer the routing stack [Quagga Command Reference] (https://www.nongnu.org/quagga/docs/quagga.pdf) or [FRR Command Reference] (https://docs.frrouting.org/en/latest/) to know more about the routing stack configuration.

Examples

```
admin@sonic:~$ show ip protocol
Protocol      : route-map
------------------------
system        : none
kernel        : none
connected     : none
static        : none
rip           : none
ripng         : none
ospf          : none
ospf6         : none
isis          : none
bgp           : RM_SET_SRC
pim           : none
hsls          : none
olsr          : none
babel         : none
  any           : none
```

1.9 show ip route

Function

Run the **show ip route** command to display either all the route entries from the routing table or a ipv4 specific route.

Syntax

show ip route [**vrf** *vrf-name*] [*ip-address*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
               O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel,
               > - selected route, * - FIB route
S>* 0.0.0.0/0 [200/0] via 10.11.162.254, eth0
C>* 1.1.0.0/16 is directly connected, Vlan100
C>* 10.1.1.0/31 is directly connected, Ethernet112
C>* 10.1.1.2/31 is directly connected, Ethernet116
C>* 10.11.162.0/24 is directly connected, eth0
C>* 127.0.0.0/8 is directly connected, lo
C>* 240.127.1.0/24 is directly connected, docker0
```

Optionally, you can specify an IP address in order to display only routes to that particular IP address

```
admin@sonic:~$ show ip route 10.1.1.0
Routing entry for 10.1.1.0/31
    Known via "connected", distance 0, metric 0, best
    * directly connected, Ethernet112
```

Vrf-name can also be specified to get IPv4 routes programmed in the vrf.

```
admin@sonic:~$ show ip route vrf Vrf-red
      Codes: K - kernel route, C - connected, S - static, R - RIP,
      O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
      T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
      F - PBR, f - OpenFabric,
      > - selected route, * - FIB route
      VRF Vrf-red:
      C>*     11.1.1.1/32 is directly connected, Loopback11, 21:50:47
      C>*     100.1.1.0/24 is directly connected, Vlan100, 03w1d06h
```

```
admin@sonic:~$ show ip route vrf Vrf-red 11.1.1.1/32
      Routing entry for 11.1.1.1/32
      Known via "connected", distance 0, metric 0, vrf Vrf-red, best
      Last update 21:57:53 ago
      * directly connected, Loopback11
```

1.10 show ipv6 interfaces

Function

Run the **show ipv6 interfaces** command to display the details about all the Layer3 IPv6 interfaces in the device for which IPv6 address has been assigned. The type of interfaces include the following.

- Front panel physical ports.
- PortChannel.
- VLAN interface.
- Loopback interfaces
- management interface

Syntax

show ipv6 interfaces

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ipv6 interfaces
Interface                  Master           IPv6 address/mask                                  Admin/Oper
-----------                --------         -----------------------------------------          ------------
Bridge                                      fe80::7c45:1dff:fe08:cdd%Bridge/64                 up/up
Loopback11                 Vrf-red          1100::1/128                                        up/up
PortChannel01                               fc00::71/126                                       up/down
PortChannel02                               fc00::75/126                                       up/down
PortChannel03                               fc00::79/126                                       up/down
```

```
PortChannel04                           fc00::7d/126
up/down
Vlan100                 Vrf-red         100::1/112
up/up
                                                    fe80::eef4:bbff:fefe:880a%Vlan100/64
eth0                                            fe80::eef4:bbff:fefe:880a%eth0/64       up/up
lo                                               fc00:1::32/128
up/up
```

1.11 show ipv6 protocol

Function

Run the **show ipv6 protocol** command to display the route-map that is configured for the IPv6 routing protocol.

Syntax

show ipv6 protocol

Parameter Description

N/A

Usage Guidelines

Notes
Refer the routing stack [Quagga Command Reference] (https://www.nongnu.org/quagga/docs/quagga.pdf) or [FRR Command Reference] (https://docs.frrouting.org/en/latest/) to know more about the routing stack configuration.

Examples

```
admin@sonic:~$ show ipv6 protocol
Protocol      : route-map
------------------------
system        : none
kernel        : none
connected     : none
static        : none
rip           : none
ripng         : none
ospf          : none
ospf6         : none
isis          : none
bgp           : RM_SET_SRC6
pim           : none
hsls          : none
```

```
olsr          : none
babel          : none
any            : none
```

1.12 show ipv6 route

Function

Run the **show ipv6 route** command to display either all the IPv6 route entries from the routing table or a specific IPv6 route.

Syntax

show ipv6 route [**vrf** *vrf-name*] [*ipv6-address*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ipv6 route
Codes: K - kernel route, C - connected, S - static, R - RIPng,
               O - OSPFv6, I - IS-IS, B - BGP, A - Babel,
               > - selected route, * - FIB route

C>* ::1/128 is directly connected, lo
C>* 2018:2001::/126 is directly connected, Ethernet112
C>* 2018:2002::/126 is directly connected, Ethernet116
C>* fc00:1::32/128 is directly connected, lo
C>* fc00:1::102/128 is directly connected, lo
C>* fc00:2::102/128 is directly connected, eth0
C * fe80::/64 is directly connected, Vlan100
C * fe80::/64 is directly connected, Ethernet112
C * fe80::/64 is directly connected, Ethernet116
C * fe80::/64 is directly connected, Bridge
C * fe80::/64 is directly connected, PortChannel0011
C>* fe80::/64 is directly connected, eth0
```

Optionally, you can specify an IPv6 address in order to display only routes to that particular IPv6 address.

```
admin@sonic:~$ show ipv6 route   fc00:1::32
Routing entry for fc00:1::32/128
  Known via "connected", distance 0, metric 0, best
  * directly connected, lo
```

Vrf-name can also be specified to get IPv6 routes programmed in the vrf.

```
admin@sonic:~$ show ipv6 route vrf Vrf-red
  Codes: K - kernel route, C - connected, S - static, R - RIP,
  O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
  T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
  F - PBR, f - OpenFabric,
  > - selected route, * - FIB route
  VRF Vrf-red:
        C>*   1100::1/128 is directly connected, Loopback11, 21:50:47
        C>*   100::/112 is directly connected, Vlan100, 03w1d06h
        C>*   fe80::/64 is directly connected, Loopback11, 21:50:47
        C>*   fe80::/64 is directly connected, Vlan100, 03w1d06h
```

```
admin@sonic:~$ show ipv6 route vrf Vrf-red 1100::1/128
  Routing entry for 1100::1/128
  Known via "connected", distance 0, metric 0, vrf Vrf-red, best
  Last update 21:57:53 ago
  * directly connected, Loopback11
```

1 OSPF Commands

Command	Function
config docker-routing-config-mode	Configure the BGP docker routing config mode. When it is 'spilt', it will stop your configuration from being overrwirrten with a builtin template each time the FFR docker container is restarted. When it is 'unified' or 'seperated', both of which overwrite any FRR routing protocol configuration.
config frr mgmt-framework	Configure the FRRouting (FRR) mgmt-framework. FRR is an open source Internet routing protocol suite. FRR mgmt-framework is the framework used to manage FRR under SONiC. The FRR suite contains many protocol components, including OSPF. To use SONiC's OSPF commands, set mgmt-framework value to true.
config frr interface ip ospf area	Enable ospf on an interface and sets associated area.
config frr interface ip ospf authentication	Specify that simple password authentication should be used for the given area. This command specifies that OSPF packets must be authenticated with MD5 HMACs within the given area. Keying material must also be configured on a per-interface basis (ip ospf message-digest-key). MD5 authentication may also be configured on a per-interface basis (ip ospf authentication message-digest). Such per-interface settings will override any per-area authentication setting.
config frr interface ip ospf authentication-key	Set OSPF authentication key to a simple password. After setting AUTH_KEY, all OSPF packets are authenticated. AUTH_KEY has length up to 8 chars. Simple text password authentication is insecure and deprecated in favour of MD5 HMAC authentication.
config frr interface ip ospf bfd	Enable BFD for OSPFv2 on the current

	interface.
config frr interface ip ospf cost	Set link cost for the specified interface. The cost value is set to router-LSA's metric field and used for SPF calculation.
config frr interface ip ospf dead-interval	Set number of seconds for RouterDeadInterval timer value used for Wait Timer and Inactivity Timer. This value must be the same for all routers attached to a common network. The default value is 40 seconds.
config frr interface ip ospf message-digest-key md5	Set OSPF authentication key to a cryptographic password. The cryptographic algorithm is MD5. KEYID identifies secret key used to create the message digest. This ID is part of the protocol and must be consistent across routers on a link. KEY is the actual message digest key, of up to 16 chars (larger strings will be truncated), and is associated with the given KEYID.
config frr interface ip ospf mtu-ignore	Disable the check of the MTU value in the OSPF DBD packets. Thus, use of this command allows the OSPF adjacency to reach the FULL state even though there is an interface MTU mismatch between two OSPF routers.
config frr interface ip ospf network	Configure OSPF network for an interface. When configuring a point-to-point network on an interface and the interface has a /32 address associated with then OSPF will treat the interface as being unnumbered. If you are doing this you must set the net.ipv4.conf..rp_filter value to 0. In order for the ospf multicast packets to be delivered by the kernel.
config frr interface ip ospf priority	Set RouterPriority integer value. The router with the highest priority will be more eligible to become Designated Router. Setting the value to 0, makes the router ineligible to become Designated Router. The default value is 1.
config frr interface ip ospf retransmit-interval	Set number of seconds for RxmtInterval timer value. This value is used when retransmitting Database Description and Link State Request packets. The default

	value is 5 seconds.
config frr interface ip ospf transmit-delay	Set the number of seconds for InfTransDelay value. LSAs' age should be incremented by this value when transmitting. The default value is 1 second.
config frr interface ipv6 ospf6 advertise prefix-list	Filter route advertisements using the specified prefix list (Dynamic Routing Prefix Lists).
config frr interface ipv6 ospf6 bfd	Enable Bidirectional Forwarding Detection for OSPF6 on this interface.
config frr interface ipv6 ospf6 dead-interval	Set the dead interval. Time, in seconds from 1-65535, without communication from a neighbor on this interface before considering it dead. This is also known as the RouterDeadInterval timer in OSPF6. Default value is 40. This timer should be set to the same value for all routers.
config frr interface ipv6 ospf6 hello-interval	Set the hello interval. The interval, in seconds from 1-65535, at which this router will send hello messages. This is also known as the HelloInterval timer in OSPF6. Default value is 10. This timer should be set to the same value for all routers. A lower value will result in faster convergence times, but will consume more resources.
config frr interface ipv6 ospf6 ifmtu	Explicitly configure an MTU value for this interface. This value will override the interface MTU determined automatically by the operating system. Useful in cases where the router is unable to determine the actual interface MTU, for example on virtual interfaces such as those used by IPsec.
config frr interface ipv6 ospf6 mtu-ignore	Make OSPF6 ignoring the MTU advertised by neighbors. OSPF6 can still achieve a full adjacency when peers do not have matching MTU values.
config frr interface ipv6 ospf6 network	Manually configure a specific type of network used on a given interface, rather than letting OSPF6 determine the type automatically. This controls how OSPF6 behaves and how it crafts messages when using an interface. broadcast: Broadcast networks, such as typical

	Ethernet networks, allow multiple routers on a segment and OSPF6 can use multicast to send messages to multiple targets at once. OSPF6 assumes that all routers on broadcast networks are directly connected and can communicate without passing through other routers. point-to-point: A point-to-point network links a single pair of routers. The interface is still capable of broadcast, and OSPF6 will dynamically discover neighbors. With this type of network, OSPF6 disables election of a DR.
config frr interface ipv6 ospf6 passive	Configure this interface as passive. This prevents the interface from actively participating in OSPF6, while still allowing OSPF6 to operate on networks connected to that interface. This is commonly used for local interfaces without other routers attached. OSPF6 will announce networks attached to passive interfaces as stub links.
config frr interface ipv6 ospf6 priority	Set priority value. A priority value, from 0-255, assigned to this router. When determining which router will become the Designated Router (DR), the router with the highest priority is more likely to be elected as the DR. The default value is 1. The value 0 is special and will prevent this router from being chosen as DR.
config frr interface ipv6 ospf6 retransmit-interval	Set number of seconds for RxmtInterval timer value. The interval, in seconds from 1-65535, at which this router will retransmit Link State Request and Database Description messages. This is also known as the RxmtInterval timer in OSPF6. Default value is 5.
config frr interface ipv6 ospf6 transmit-delay	Set the number of seconds for InfTransDelay value. The interval, in seconds from 1-3600, at which this router will transmit LSA messages. This is also known as the InfTransDelay timer in OSPF6. Default value is 1.
config frr ospf area authentication	Specify that simple password authentication should be used for the given area.

config frr ospf area default-cost	Set the cost of default-summary LSAs announced to stubby areas.
config frr ospf area export-list	Filter Type-3 summary-LSAs announced to other areas originated from intra-area paths from specified area.
config frr ospf area filter-list prefix	Filter Type-3 summary-LSAs to/from area using prefix lists.
config frr ospf area import-list	Filter Type-3 summary-LSAs. Same as export-list, but it applies to paths announced into specified area as Type-3 summary-LSAs.
config frr ospf area nssa	Configure the area to be a NSSA (Not-So-Stubby Area). This is an area that allows OSPF to import external routes into a stub area via a new LSA type (type 7). An NSSA autonomous system boundary router (ASBR) will generate this type of LSA. The area border router (ABR) translates the LSA type 7 into LSA type 5, which is propagated into the OSPF domain. NSSA areas are defined in RFC 3101.
config frr ospf area range	Summarize a group of external subnets into a single Type-7 LSA, which is then translated to a Type-5 LSA and avertised to the backbone. This command can only be used at the area boundary (NSSA ABR router). By default, the metric of the summary route is calculated as the highest metric among the summarized routes. The cost option, however, can be used to set an explicit metric. The not-advertise option, when present, prevents the summary route from being advertised, effectively filtering the summarized routes.
config frr ospf area shortcut	Configure the area as Shortcut capable. See RFC 3509.
config frr ospf area stub	Specify the area to be a Stub Area. That is, an area where no router originates routes external to OSPF and hence an area where all external routes are via the ABR(s). Hence, ABRs for such an area do not need to pass AS-External LSAs (type-5) or ASBR-Summary LSAs (type-4) into the area. They need only pass Network-

	Summary (type-3) LSAs into such an area, along with a default-route summary. This command (no-summary) specifies the area to be a Totally Stub Area. In addition to stub area limitations this area type prevents an ABR from injecting Network-Summary (type-3) LSAs into the specified stub area. Only default summary route is allowed.
config frr ospf area virtual-link	Provide a backbone area coherence by virtual link establishment. In general, OSPF protocol requires a backbone area (area 0) to be coherent and fully connected. I.e. any backbone area router must have a route to any other backbone area router. Moreover, every ABR must have a link to backbone area. However, it is not always possible to have a physical link to a backbone area. In this case between two ABR (one of them has a link to the backbone area) in the area (not stub area) a virtual link is organized.
config frr ospf area redistribute	Redistribute routes of the specified protocol or kind into OSPF, with the metric type and metric set if specified, filtering the routes using the given route-map if specified. Redistributed routes may also be filtered with distribute-lists, see ospf distribute-list configuration. Redistributed routes are distributed as into OSPF as Type-5 External LSAs into links to areas that accept external routes, Type-7 External LSAs for NSSA areas and are not redistributed at all into Stub areas, where external routes are not permitted.
config frr ospf auto-cost reference-bandwidth	Set the reference bandwidth for cost calculations, where this bandwidth is considered equivalent to an OSPF cost of 1, specified in Mbit/s. The default is 100 Mbit/s (i.e. a link of bandwidth 100 Mbit/s or higher will have a cost of 1. Cost of lower bandwidth links will be scaled with reference to this cost). NOTE: This configuration setting MUST be consistent across all routers within the OSPF domain.
config frr ospf capability opaque	Configure OSPF opaque capability. Ospfd supports Opaque LSA (RFC 5250) as

	partial support for MPLS Traffic Engineering LSAs. The opaque-lsa capability must be enabled in the configuration. An alternate command could be “mpls-te on” (Traffic Engineering). Note that FRR offers only partial support for some of the routing protocol extensions that are used with MPLS-TE; it does not support a complete RSVP-TE solution.
config frr ospf compatible rfc1583	Make software being compatible with RFC 1583. RFC 2328, the successor to RFC 1583, suggests according to section G.2 (changes) in section 16.4 a change to the path preference algorithm that prevents possible routing loops that were possible in the old version of OSPFv2. More specifically it demands that inter-area paths and intra-area backbone path are now of equal preference but still both preferred to external paths.
config frr ospf default-information originate	Originate an AS-External (type-5) LSA describing a default route into all external-routing capable areas, of the specified metric and metric type. If the ‘always’ keyword is given then the default is always advertised, even when there is no default present in the routing table.
config frr ospf default-metric	Set the default metric value for the OSPF.
config frr ospf distribute-list out	Apply the access-list filter to redistributed routes of the given type before allowing the routes to be redistributed into OSPF (ospf redistribution).
config frr ospf log-adjacency-changes	Configure ospfd to log changes in adjacency. With the optional detail argument, all changes in adjacency status are shown. Without detail, only changes to full or regressions are shown.
config frr ospf max-metric router-lsa	Enable RFC 3137 support, where the OSPF process describes its transit links in its router-LSA as having infinite distance so that other routers will avoid calculating transit paths through the router while still being able to reach networks through the router. This support may be enabled administratively (and indefinitely) or

	conditionally. Conditional enabling of max-metric router-lsas can be for a period of seconds after startup and/or for a period of seconds prior to shutdown. Enabling this for a period after startup allows OSPF to converge fully first without affecting any existing routes used by other routers, while still allowing any connected stub links and/or redistributed routes to be reachable. Enabling this for a period of time in advance of shutdown allows the router to gracefully excuse itself from the OSPF domain. Enabling this feature administratively allows for administrative intervention for whatever reason, for an indefinite period of time. Note that if the configuration is written to file, this administrative form of the stub-router command will also be written to file. If ospfd is restarted later, the command will then take effect until manually deconfigured.
config frr ospf network area	Specify the OSPF enabled interface(s). If the interface has an address from range A.B.C.D/M then the command below enables ospf on this interface so router can provide network information to the other ospf routers via this interface.
config frr ospf ospf abr-type	Configure the ABR type. The “Cisco” and “IBM” types are equivalent. The OSPF standard for ABR behaviour does not allow an ABR to consider routes through non-backbone areas when its links to the backbone are down, even when there are other ABRs in attached non-backbone areas which still can reach the backbone - this restriction exists primarily to ensure routing-loops are avoided. With the “Cisco” or “IBM” ABR type, the default in this release of FRR, this restriction is lifted, allowing an ABR to consider summaries learned from other ABRs through non-backbone areas, and hence route via non-backbone areas as a last resort when, and only when, backbone links are down.
config frr ospf ospf opaque-lsa	Configure OSPF opaque LSA. Ospfd supports Opaque LSA (RFC 2370) as

	partial support for MPLS Traffic Engineering LSAs. The opaque-lsa capability must be enabled in the configuration. An alternate command could be “mpls-te on” (Traffic Engineering). Note that FRR offers only partial support for some of the routing protocol extensions that are used with MPLS-TE; it does not support a complete RSVP-TE solution.
config frr ospf ospf rfc1583compatibility	Make software being compatible with RFC 1583. RFC 2328, the successor to RFC 1583, suggests according to section G.2 (changes) in section 16.4 a change to the path preference algorithm that prevents possible routing loops that were possible in the old version of OSPFv2. More specifically it demands that inter-area paths and intra-area backbone path are now of equal preference but still both preferred to external paths.
config frr ospf ospf router-id	Set the router-ID of the OSPF process. The router-ID may be an IP address of the router, but need not be - it can be any arbitrary 32bit number. However it MUST be unique within the entire OSPF domain to the OSPF speaker - bad things will happen if multiple OSPF speakers are configured with the same router-ID! If one is not specified then ospfd will obtain a router-ID automatically from zebra.
config frr ospf ospf write-multiplier	Tune the amount of work done in the packet read and write threads before relinquishing control. The parameter is the number of packets to process before returning. The defult value of this parameter is 20.
config frr ospf passive-interface	Make all interfaces that belong to this router passive by default. For the description of passive interface look at ip ospf passive [A.B.C.D]. Per-interface configuration takes precedence over the default value.
config frr ospf proactive-arp	Enables or disables sending ARP requests to update neighbor table entries. It speeds up convergence for /32 networks on a P2P connection. This feature is enabled by

	default.
config frr ospf router-info	Enable Router Information (RFC 4970) LSA advertisement with AS scope (default) or Area scope flooding when area is specified. Old syntax router-info area <A.B.C.D> is always supported but mark as deprecated as the area ID is no more necessary. Indeed, router information support multi-area and detect automatically the areas.
config frr ospf timers lsa min-arrival	Set the minimum time interval that should be elapsed before accepting a version of the same LSA.
config frr ospf timers throttle lsa all	Control the generation (sending) of LSAs. The first LSA is always generated immediately upon an OSPF topology change, and the next LSA generated is controlled by the minimum start interval. The subsequent LSAs generated for the same LSA are rate-limited until the maximum interval is reached. The “same LSA” is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. The timers lsa arrival command controls the minimum interval for accepting the same LSA. If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped. It is recommended that the arrival interval be less than or equal to the hold-time interval of the timers throttle lsa all command.
config frr ospf timers throttle spf	Set the initial delay, the initial-holdtime and the maximum-holdtime between when SPF is calculated and the event which triggered the calculation. The times are specified in milliseconds and must be in the range of 0 to 600000 milliseconds. The delay specifies the minimum amount of time to delay SPF calculation (hence it affects how long SPF calculation is delayed after an event which occurs outside of the holdtime of any previous SPF calculation, and also serves as a minimum holdtime). Consecutive SPF calculations will always be separated by at least ‘hold-time’ milliseconds. The

	hold-time is adaptive and initially is set to the initial-holdtime configured with the above command. Events which occur within the holdtime of the previous SPF calculation will cause the holdtime to be increased by initial-holdtime, bounded by the maximum-holdtime configured with this command. If the adaptive hold-time elapses without any SPF-triggering event occurring then the current holdtime is reset to the initial-holdtime. The current holdtime can be viewed with show ip ospf, where it is expressed as a multiplier of the initial-holdtime.
config frr ospf write-multiplier	Tune the amount of work done in the packet read and write threads before relinquishing control. The parameter is the number of packets to process before returning. The defult value of this parameter is 20.
config frr ospf6 area export-list	Filter Type-3 summary-LSAs announced to other areas originated from intra-area paths from specified area.
config frr ospf6 area filter-list prefix	Filter Type-3 summary-LSAs to/from area using prefix lists.
config frr ospf6 area import-list	Filter Type-3 summary-LSAs. Same as export-list, but it applies to paths announced into specified area as Type-3 summary-LSAs.
config frr ospf6 area range	Summarize a group of internal subnets into a single Inter-Area-Prefix LSA. This command can only be used at the area boundary (ABR router). By default, the metric of the summary route is calculated as the highest metric among the summarized routes. The cost option, however, can be used to set an explicit metric. The not-advertise option, when present, prevents the summary route from being advertised, effectively filtering the summarized routes.
config frr ospf6 area stub	Specify the area to be a Stub Area. That is, an area where no router originates routes external to OSPF and hence an area where all external routes are via the ABR(s). Hence, ABRs for such an area do not need

	to pass AS-External LSAs (type-5) or ASBR-Summary LSAs (type-4) into the area. They need only pass Network-Summary (type-3) LSAs into such an area, along with a default-route summary. This command (no-summary) specifies the area to be a Totally Stub Area. In addition to stub area limitations this area type prevents an ABR from injecting Network-Summary (type-3) LSAs into the specified stub area. Only default summary route is allowed.
config frr ospf6 area redistribute	Redistribute routes of the specified protocol or kind into OSPFv3, with the metric type and metric set if specified, filtering the routes using the given route-map if specified.
config frr ospf6 auto-cost reference-bandwidth	Set the reference bandwidth for cost calculations, where this bandwidth is considered equivalent to an OSPF cost of 1, specified in Mbits/s. The default is 100Mbit/s (i.e. a link of bandwidth 100Mbit/s or higher will have a cost of 1. Cost of lower bandwidth links will be scaled with reference to this cost).
config frr ospf6 router-id	Set router's Router-ID.
config frr ospf6 stub-router administrative	Administratively declare this router as a stub router, having no external connections.
config frr ospf6 timers lsa min-arrival	Set LSA min-arrival timers. The minimum time allowed between advertisements by neighbors, from 0-600000, in milliseconds. Default is 1000.
config frr ospf6 timers throttle spf	Set the initial delay, the initial-holdtime and the maximum-holdtime between when SPF is calculated and the event which triggered the calculation. The times are specified in milliseconds and must be in the range of 0 to 600000 milliseconds. The delay specifies the minimum amount of time to delay SPF calculation (hence it affects how long SPF calculation is delayed after an event which occurs outside of the holdtime of any previous SPF calculation, and also serves as a minimum holdtime). Consecutive SPF

	calculations will always be separated by at least 'hold-time' milliseconds. The hold-time is adaptive and initially is set to the initial-holdtime configured with the above command. Events which occur within the holdtime of the previous SPF calculation will cause the holdtime to be increased by initial-holdtime, bounded by the maximum-holdtime configured with this command. If the adaptive hold-time elapses without any SPF-triggering event occurring then the current holdtime is reset to the initial-holdtime.
show ip ospf	Display the OSPF status.
show ipv6 ospf6	Display the OSPF6 status.

1.1 config docker-routing-config-mode

Function

Run the **config docker-routing-config-mode** command to configure the BGP docker routing config mode. When it is 'spilt', it will stop your configuration from being overrwirrten with a builtin template each time the FFR docker container is restarted. When it is 'unified' or 'seperated', both of which overwrite any FRR routing protocol configuration.

Syntax

config docker-routing-config-mode [**separated** | **split** | **unified**]

Parameter Description

separated: FRR config generated from ConfigDB, each FRR daemon has its own config file.

split: FRR config not generated from ConfigDB, each FRR daemon has its own config file.

unified: FRR config generated from ConfigDB, single FRR config file.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config docker-routing-config-mode split
```

1.2 config frr mgmt-framework

Function

Run the **config frr mgmt-framework** command to configure the FRRouting (FRR) mgmt-framework. FRR is an open source Internet routing protocol suite. FRR mgmt-framework is the framework used to manage FRR under SONiC. The FRR suite contains many protocol components, including OSPF. To use SONiC's OSPF commands, set mgmt-framework value to true.

Syntax

config frr mgmt-framework { **false** | **true** }

Parameter Description

false: Disable frr mgmt-framework.

true: Enable frr mgmt-framework.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr mgmt-framework true
```

1.3 config frr interface ip ospf area

Function

Run the **config frr interface ip ospf area** command to enable ospf on an interface and sets associated area.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ip ospf area** *A.B.C.D* [**--addr** *A.B.C.D*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

--addr A.B.C.D: Address of interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ip ospf area 1.1.1.1
```

1.4 config frr interface ip ospf authentication

Function

Run the **config frr interface ip ospf authentication** command to specify that simple password authentication should be used for the given area. This command specifies that OSPF packets must be authenticated with MD5 HMACs within the given area. Keying material must also be configured on a per-interface basis (ip ospf message-digest-key). MD5 authentication may also be configured on a per-interface basis (ip ospf authentication message-digest). Such per-interface settings will override any per-area authentication setting.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ip ospf authentication** { **default** | **message-digest** | **null** } [**--addr** *A.B.C.D*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

default: authentication on this interface.

message-digest: Use message-digest authentication.

null: Use null authentication.

--addr A.B.C.D: Address of interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ip ospf authentication default
```

1.5 config frr interface ip ospf authentication-key

Function

Run the **config frr interface ip ospf authentication-key** command to set OSPF authentication key to a simple password. After setting AUTH_KEY, all OSPF packets are authenticated. AUTH_KEY has length up to 8 chars. Simple text password authentication is insecure and deprecated in favour of MD5 HMAC authentication.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ip ospf authentication-key** *key* [**--addr** *A.B.C.D*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

key: The OSPF password (key).

--addr A.B.C.D: Address of interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ip ospf authentication default
```

1.6 config frr interface ip ospf bfd

Function

Run the **config frr interface ip ospf bfd** command to enable BFD for OSPFv2 on the current interface.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ip ospf bfd**

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ip ospf bfd
```

1.7 config frr interface ip ospf cost

Function

Run the **config frr interface ip ospf cost** command to set link cost for the specified interface. The cost value is set to router-LSA's metric field and used for SPF calculation.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ip ospf cost** *cost-value* [**--addr** *A.B.C.D*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

cost-value: The value range is from 1 to 65535.

--addr A.B.C.D: Address of interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ip ospf cost 10
```

1.8 config frr interface ip ospf dead-interval

Function

Run the **config frr interface ip ospf dead-interval** command to set number of seconds for RouterDeadInterval timer value used for Wait Timer and Inactivity Timer. This value must be the same for all routers attached to a common network. The default value is 40 seconds.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ip ospf cost** *interval* [**--addr** *A.B.C.D*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

interval: The value range is from 1 to 65535.

--addr A.B.C.D: Address of interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ip ospf dead-interval 100
```

1.9 config frr interface ip ospf message-digest-key md5

Function

Run the **config frr interface ip ospf message-digest-key md5** command to set OSPF authentication key to a cryptographic password. The cryptographic algorithm is MD5. KEYID identifies secret key used to create the message digest. This ID is part of the protocol and must be consistent across routers on a link. KEY is the actual message digest key, of up to 16 chars (larger strings will be truncated), and is associated with the given KEYID.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ip ospf message-digest-key** *key-id* **md5** *key* [**--addr** *A.B.C.D*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

key-id: KEYID identifies secret key used to create the message digest. This ID is part of the protocol and must be consistent across routers on a link. The value range is from 1 to 255.

key: The actual message digest key, of up to 16 chars (larger strings will be truncated).

--addr A.B.C.D: Address of interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ip ospf message-digest-key 5 md5 foo
```

1.10 config frr interface ip ospf mtu-ignore

Function

Run the **config frr interface ip ospf mtu-ignore** command to disable the check of the MTU value in the OSPF DBD packets. Thus, use of this command allows the OSPF adjacency to reach the FULL state even though there is an interface MTU mismatch between two OSPF routers.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ip ospf mtu-ignore** [**--addr** *A.B.C.D*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

--addr A.B.C.D: Address of interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ip ospf message-digest-key 5 md5 foo
```

1.11 config frr interface ip ospf network

Function

Run the **config frr interface ip ospf network** command to configure OSPF network for an interface. When configuring a point-to-point network on an interface and the interface has a /32 address associated with then OSPF will treat the interface as being unnumbered. If you are doing this you must set the net.ipv4.conf..rp_filter value to 0. In order for the ospf multicast packets to be delivered by the kernel.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ip ospf network** { **broadcast** | **non-broadcast** | **point-to-multipoint** | **point-to-point** } [**--addr** *A.B.C.D*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

broadcast: Specify OSPF broadcast multi-access network.

non-broadcast: Specify OSPF NBMA network.

point-to-multipoint: Specify OSPF point-to-multipoint network.

point-to-point: Specify OSPF point-to-point network.

--addr A.B.C.D: Address of interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ip ospf network broadcast
```

1.12 config frr interface ip ospf priority

Function

Run the **config frr interface ip ospf priority** command to set RouterPriority integer value. The router with the highest priority will be more eligible to become Designated Router. Setting the value to 0, makes the router ineligible to become Designated Router. The default value is 1.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ip ospf priority** *priority-value* [**--addr** *A.B.C.D*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

priority-value: RouterPriority integer value, the value range is from 0 to 255.

--addr A.B.C.D: Address of interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ip ospf priority 5
```

1.13 config frr interface ip ospf retransmit-interval

Function

Run the **config frr interface ip ospf retransmit-interval** command to set number of seconds for RxmtInterval timer value. This value is used when retransmitting Database Description and Link State Request packets. The default value is 5 seconds.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ip ospf retransmit-interval** *interval* [**--addr** *A.B.C.D*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

interval: Number of seconds for RxmtInterval timer value, the value range is from 1 to 65535.

--addr A.B.C.D: Address of interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ip ospf retransmit-interval 100
```

1.14 config frr interface ip ospf transmit-delay

Function

Run the **config frr interface ip ospf transmit-delay** command to set the number of seconds for InfTransDelay value. LSAs' age should be incremented by this value when transmitting. The default value is 1 second.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ip ospf transmit-delay** *delay-time* [**--addr** *A.B.C.D*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

delay-time: The number of seconds for InfTransDelay value, the value range is from 1 to 3600.

--addr A.B.C.D: Address of interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ip ospf transmit-delay 5
```

1.15 config frr interface ipv6 ospf6 advertise prefix-list

Function

Run the **config frr interface ipv6 ospf6 advertise prefix-list** command to filter route advertisements using the specified prefix list (Dynamic Routing Prefix Lists).

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ipv6 ospf6 advertise prefix-list** *name*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

name: Name of an IPv6 prefix-list.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ipv6 ospf6 advertise prefix-list foo
```

1.16 config frr interface ipv6 ospf6 bfd

Function

Run the **config frr interface ipv6 ospf6 bfd** command to enable Bidirectional Forwarding Detection for OSPF6 on this interface.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ipv6 ospf6 bfd**

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ipv6 ospf6 bfd
```

1.17 config frr interface ipv6 ospf6 dead-interval

Function

Run the **config frr interface ipv6 ospf6 dead-interval** command to set the dead interval. Time, in seconds from 1-65535, without communication from a neighbor on this interface before considering it dead. This is also known as the RouterDeadInterval timer in OSPF6. Default value is 40. This timer should be set to the same value for all routers.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ipv6 ospf6 dead-interval** *time*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

time: In seconds from 1-65535, without communication from a neighbor on this interface before considering it dead.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ipv6 ospf6 dead-interval 100
```

1.18 config frr interface ipv6 ospf6 hello-interval

Function

Run the **config frr interface ipv6 ospf6 hello-interval** command to set the hello interval. The interval, in seconds from 1-65535, at which this router will send hello messages. This is also known as the HelloInterval timer in OSPF6. Default value is 10. This timer should be set to the same value for all routers. A lower value will result in faster convergence times, but will consume more resources.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ipv6 ospf6 hello-interval** *time*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

time: The interval, in seconds from 1-65535, at which this router will send hello messages.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ipv6 ospf6 hello-interval 100
```

1.19 config frr interface ipv6 ospf6 ifmtu

Function

Run the **config frr interface ipv6 ospf6 ifmtu** command to explicitly configure an MTU value for this interface. This value will override the interface MTU determined automatically by the operating system. Useful in cases where the router is unable to determine the actual interface MTU, for example on virtual interfaces such as those used by IPsec.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ipv6 ospf6 ifmtu** *mtu*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

mtu: MTU value for this interface, the value range is from 1 to 65535.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ipv6 ospf6 ifmtu 24000
```

1.20 config frr interface ipv6 ospf6 mtu-ignore

Function

Run the **config frr interface ipv6 ospf6 mtu-ignore** command to make OSPF6 ignoring the MTU advertised by neighbors. OSPF6 can still achieve a full adjacency when peers do not have matching MTU values.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ipv6 ospf6 mtu-ignore**

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ipv6 ospf6 mtu-ignore
```

1.21 config frr interface ipv6 ospf6 network

Function

Run the **config frr interface ipv6 ospf6 network** command to manually configure a specific type of network used on a given interface, rather than letting OSPF6 determine the type automatically. This controls how OSPF6 behaves and how it crafts messages when using an interface. broadcast: Broadcast networks, such as typical Ethernet networks, allow multiple routers on a segment and OSPF6 can use multicast to send messages to multiple targets at once. OSPF6 assumes that all routers on broadcast networks are directly connected and

can communicate without passing through other routers. point-to-point: A point-to-point network links a single pair of routers. The interface is still capable of broadcast, and OSPF6 will dynamically discover neighbors. With this type of network, OSPF6 disables election of a DR.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ipv6 ospf6 network** { **broadcast** | **point-to-point** }

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

broadcast: Specify OSPF6 broadcast network.

point-to-point: Specify OSPF6 point-to-point network.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ipv6 ospf6 network broadcast
```

1.22 config frr interface ipv6 ospf6 passive

Function

Run the **config frr interface ipv6 ospf6 passive** command to configure this interface as passive. This prevents the interface from actively participating in OSPF6, while still allowing OSPF6 to operate on networks connected to that interface. This is commonly used for local interfaces without other routers attached. OSPF6 will announce networks attached to passive interfaces as stub links.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ipv6 ospf6 passive**

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ipv6 ospf6 passive
```

1.23 config frr interface ipv6 ospf6 priority

Function

Run the **config frr interface ipv6 ospf6 priority** command to set priority value. A priority value, from 0-255, assigned to this router. When determining which router will become the Designated Router (DR), the router with the highest priority is more likely to be elected as the DR. The default value is 1. The value 0 is special and will prevent this router from being chosen as DR.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ipv6 ospf6 priority** *priority-value*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

priority-value: The value range is from 0 to 255.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ipv6 ospf6 priority 5
```

1.24 config frr interface ipv6 ospf6 retransmit-interval

Function

Run the **config frr interface ipv6 ospf6 retransmit-interval** command to set number of seconds for RxmtInterval timer value. The interval, in seconds from 1-65535, at which this router will retransmit Link State Request and Database Description messages. This is also known as the RxmtInterval timer in OSPF6. Default value is 5.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ipv6 ospf6 retransmit-interval** *interval*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

interval: Number of seconds for RxmtInterval timer value, the value range is from 1 to 65535.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ipv6 ospf6 retransmit-interval 10
```

1.25 config frr interface ipv6 ospf6 transmit-delay

Function

Run the **config frr interface ipv6 ospf6 transmit-delay** command to set the number of seconds for InfTransDelay value. The interval, in seconds from 1-3600, at which this router will transmit LSA messages. This is also known as the InfTransDelay timer in OSPF6. Default value is 1.

Syntax

config frr interface *interface-name* [**--vrfname** *VRF*] [**no**] **ipv6 ospf6 transmit-delay** *delay-time*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Interface's name.

delay-time: The number of seconds for InfTransDelay value, the value range is from 1 to 3600.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr interface Ethernet1 ipv6 ospf6 transmit-delay 5
```

1.26 config frr ospf area authentication

Function

Run the **config frr ospf area authentication** command to specify that simple password authentication should be used for the given area.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **authentication** { **default** | **message-digest** }

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

default: Enable authentication.

message-digest: Use message-digest authentication.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf area 1.1.1.3 authentication message-digest
```

1.27 config frr ospf area default-cost

Function

Run the **config frr ospf area default-cost** command to set the cost of default-summary LSAs announced to stubby areas.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **default-cost** *cost*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

cost: The cost of default-summary LSAs announced to stubby areas, the value range is from 0 to 16777215.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf area 1.1.1.3 default-cost 100
```

1.28 config frr ospf area export-list

Function

Run the **config frr ospf area export-list** command to filter Type-3 summary-LSAs announced to other areas originated from intra-area paths from specified area.

NOTE
This command is only relevant if the router is an ABR for the specified area.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **export-list** *name*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

name: Name of the access-list.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf area 1.1.1.3 export-list foo
```

1.29 config frr ospf area filter-list prefix

Function

Run the **config frr ospf area filter-list prefix** command to filter Type-3 summary-LSAs to/from area using prefix lists.

NOTE
This command makes sense in ABR only.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **filter-list prefix** *name* { **in** | **out** }

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

name: Name of the access-list.

in: Filter networks sent to this area.

out: Filter networks sent from this area.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf area 1.1.1.3 filter-list prefix foo in
```

1.30 config frr ospf area import-list

Function

Run the **config frr ospf area import-list** command to filter Type-3 summary-LSAs. Same as export-list, but it applies to paths announced into specified area as Type-3 summary-LSAs.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **import-list** *name*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

name: Name of the access-list.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf area 1.1.1.3 import-list foo
```

1.31 config frr ospf area nssa

Function

Run the **config frr ospf area nssa** command to configure the area to be a NSSA (Not-So-Stubby Area). This is an area that allows OSPF to import external routes into a stub area via a new LSA type (type 7). An NSSA autonomous system boundary router (ASBR) will generate this type of LSA. The area border router (ABR) translates the LSA type 7 into LSA type 5, which is propagated into the OSPF domain. NSSA areas are defined in RFC 3101.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **nssa** { **default** | **no-summary** | **translate-never** | **translate-candidate** | **translate-always** }

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

default: Configure OSPF area as nssa.

no-summary: Do not inject inter-area routes into nssa.

translate-always: Configure NSSA-ABR to always translate.

translate-candidate: Configure NSSA-ABR for translate election (default).

translate-never: Configure NSSA-ABR to never translate.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf area 1.1.1.3 nssa default
```

1.32 config frr ospf area range

Function

Run the **config frr ospf area range** command to summarize a group of external subnets into a single Type-7 LSA, which is then translated to a Type-5 LSA and avertised to the backbone. This command can only be used at the area boundary (NSSA ABR router). By default, the metric of the summary route is calculated as the highest metric among the summarized routes. The cost option, however, can be used to set an explicit metric. The not-advertise option, when present, prevents the summary route from being advertised, effectively filtering the summarized routes.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **range** *A.B.C.D/M* [**--advertise** { **false** | **true** }] [**--cost** *cost-value*] [**--substitute** *A.B.C.D/M*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

--advertise false: Do not advertise this range.

--advertise true: Advertise this range.

--cost *cost-value*: User specified metric for this range, the value range is from 0 to 16777215.

--substitute *A.B.C.D/M*: Announce area range as another prefix.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf area 1.1.1.3 range 10.0.0.0/24
```

1.33 config frr ospf area shortcut

Function

Run the **config frr ospf area shortcut** command to configure the area as Shortcut capable. See RFC 3509.

NOTE:
This requires that the 'abr-type' be set to 'shortcut'.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **shortcut** { **default** | **disable** | **enable** }

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

default: Set default shortcutting behavior.

disable: Disable shortcutting through the area.

enable: Enable shortcutting through the area.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf area 1.1.1.3 shortcut default
```

1.34 config frr ospf area stub

Function

Run the **config frr ospf area stub** command to specify the area to be a Stub Area. That is, an area where no router originates routes external to OSPF and hence an area where all external routes are via the ABR(s). Hence, ABRs for such an area do not need to pass AS-External LSAs (type-5) or ASBR-Summary LSAs (type-4) into the area. They need only pass Network-Summary (type-3) LSAs into such an area, along with a default-route summary. This command (no-summary) specifies the area to be a Totally Stub Area. In addition to stub area limitations this area type prevents an ABR from injecting Network-Summary (type-3) LSAs into the specified stub area. Only default summary route is allowed.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **stub** { **default** | **no-summary** }

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

default: Configure OSPF area as stub.

no-summary: Do not inject inter-area routes into stub.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf area 1.1.1.3 stub default
```

1.35 config frr ospf area virtual-link

Function

Run the **config frr ospf area virtual-link** command to provide a backbone area coherence by virtual link establishment. In general, OSPF protocol requires a backbone area (area 0) to be coherent and fully connected. I.e. any backbone area router must have a route to any other backbone area router. Moreover, every ABR must have a link to backbone area. However, it is not always possible to have a physical link to a backbone area. In this case between two ABR (one of them has a link to the backbone area) in the area (not stub area) a virtual link is organized.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **virtual-link** A.B.C.D [**--dead-interval** *dead-interval-value*] [**--hello-interval** *hello-interval-value*] [**--retransmit-interval** *retransmit-interval-value*] [**--transmit-delay** *transmit-interval-value*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

--dead-interval *dead-interval-value*: Interval time after which a neighbor is declared down, the value range is from 1 to 65535.

--hello-interval *hello-interval-value*: Time between HELLO packets, the value range is from 1 to 65535.

--retransmit-interval *retransmit-interval-value*: Time between retransmitting lost link state advertisements, the value range is from 1 to 65535.

--transmit-delay *transmit-interval-value*: Link state transmit delay, the value range is from 1 to 65535.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf area 1.1.1.1 virtual-link 1.1.1.6
```

1.36 config frr ospf area redistribute

Function

Run the **config frr ospf area redistribute** command to redistribute routes of the specified protocol or kind into OSPF, with the metric type and metric set if specified, filtering the routes using the given route-map if specified. Redistributed routes may also be filtered with distribute-lists, see ospf distribute-list configuration. Redistributed routes are distributed as into OSPF as Type-5 External LSAs into links to areas that accept external routes, Type-7 External LSAs for NSSA areas and are not redistributed at all into Stub areas, where external routes are not permitted.

NOTE:
Note that for connected routes, one may instead use the ip ospf passive [A.B.C.D] configuration.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **redistribute** { **arp-host** | **babel** | **bgp** | **connected** | **eigrp** | **isis** | **kernel** | **nhrp** | **openfabric** | **sharp** | **rip** | **static** | **table** | **vnc** } [**--metric-type** *type*] [**--metric** *metric-value*] [**--route-map** *name*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

arp-host: Arp to host route.

babel: Babel routing protocol (Babel).

bgp: Border Gateway Protocol (BGP).

connected: Connected routes (directly attached subnet or host).

eigrp: Enhanced Interior Gateway Routing Protocol (EIGRP).

isis: Intermediate System to Intermediate System (IS-IS).

kernel: Kernel routes (not installed via the zebra RIB).

nhrp: Next Hop Resolution Protocol (NHRP).

openfabric: OpenFabric Routing Protocol.

rip: Routing Information Protocol (RIP).

static: Statically configured routes.

table: Non-main Kernel Routing Table.

vnc: Virtual Network Control (VNC).

--metric-type *type*: OSPF exterior metric type for redistributed routes, the value range is from 1 to 2.

--metric *metric-value*: Metric for redistributed routes, the value range is from 0 to 16777214.

--route-map WORD: Route map reference.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf area 1.1.1.1 virtual-link 1.1.1.6
```

1.37 config frr ospf auto-cost reference-bandwidth

Function

Run the **config frr ospf auto-cost reference-bandwidth** command to set the reference bandwidth for cost calculations, where this bandwidth is considered equivalent to an OSPF cost of 1, specified in Mbit/s. The default is 100 Mbit/s (i.e. a link of bandwidth 100 Mbit/s or higher will have a cost of 1. Cost of lower bandwidth links will be scaled with reference to this cost). NOTE: This configuration setting MUST be consistent across all routers within the OSPF domain.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **auto-cost reference-bandwidth** *bandwidth*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

bandwidth: Set the reference bandwidth for cost calculations, the value range is from 1 to 4294967.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf auto-cost reference-bandwidth 100
```

1.38 config frr ospf capability opaque

Function

Run the **config frr ospf capability opaque** command to configure OSPF opaque capability. Ospfd supports Opaque LSA (RFC 5250) as partial support for MPLS Traffic Engineering LSAs. The opaque-lsa capability must be enabled in the configuration. An alternate command could be "mpls-te on" (Traffic Engineering). Note that FRR offers only partial support for some of the routing protocol extensions that are used with MPLS-TE; it does not support a complete RSVP-TE solution.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **capability opaque**

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf capability opaque
```

1.39 config frr ospf compatible rfc1583

Function

Run the **config frr ospf compatible rfc1583** command to make software being compatible with RFC 1583. RFC 2328, the successor to RFC 1583, suggests according to section G.2 (changes) in section 16.4 a change to the path preference algorithm that prevents possible routing loops that were possible in the old version of OSPFv2. More specifically it demands that inter-area paths and intra-area backbone path are now of equal preference but still both preferred to external paths.

NOTE
This command should NOT be set normally.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **compatible rfc1583**

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf compatible rfc1583
```

1.40 config frr ospf default-information originate

Function

Run the **config frr ospf default-information originate** command to originate an AS-External (type-5) LSA describing a default route into all external-routing capable areas, of the specified metric and metric type. If the 'always' keyword is given then the default is always advertised, even when there is no default present in the routing table.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **default-information originate** [**--always** { **true** | **false** }] [**--metric** *metric-value*] [**--metric-type** *metric-type*] [**--route-map** *route-map-name*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

--always { **true** | **false** }: Always advertise default route.

--metric *metric-value*: OSPF default metric, the value range is from 0 to 16777214.

--metric-type *metric-type*: OSPF metric type for default routes, the value range is from 1 to 2.

--route-map *route-map-name*: Route map reference.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf default-information originate
```

1.41 config frr ospf default-metric

Function

Run the **config frr ospf default-metric** command to set the default metric value for the OSPF.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **default-metric** *default-metric-value*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

default-metric-value: set the default metric value, the value range is from 0 to 16777214.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf default-metric 10
```

1.42 config frr ospf distribute-list out

Function

Run the **config frr ospf distribute-list out** command to apply the access-list filter to redistributed routes of the given type before allowing the routes to be redistributed into OSPF (ospf redistribution).

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **distribute-list** *access-list-name* **out** { **arp-host** | **babel** | **bgp** | **connected** | **eigrp** | **isis** | **kernel** | **nhrp** | **openfabric** | **rip** | **sharp** | **static** | **table** | **vnc** }

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

access-list-name: Access-list name.

arp-host: Arp to host route.

babel: Babel routing protocol (Babel).

bgp: Border Gateway Protocol (BGP).

connected: Connected routes (directly attached subnet or host).

eigrp: Enhanced Interior Gateway Routing Protocol (EIGRP).

isis: Intermediate System to Intermediate System (IS-IS).

kernel: Kernel routes (not installed via the zebra RIB).

nhrp: Next Hop Resolution Protocol (NHRP).

openfabric: OpenFabric Routing Protocol.

rip: Routing Information Protocol (RIP).

static: Statically configured routes.

table: Non-main Kernel Routing Table.

vnc: Virtual Network Control (VNC).

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf distribute-list foo out kernel
```

1.43 config frr ospf log-adjacency-changes

Function

Run the **config frr ospf log-adjacency-changes** command to configure ospfd to log changes in adjacency. With the optional detail argument, all changes in adjacency status are shown. Without detail, only changes to full or regressions are shown.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **log-adjacency-changes** { **BRIEF** | **DETAIL** }

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

BRIEF: Log brief state changes.

DETAIL: Log all state changes.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf log-adjacency-changes DETAIL
```

1.44 config frr ospf max-metric router-lsa

Function

Run the **config frr ospf max-metric router-lsa** command to enable RFC 3137 support, where the OSPF process describes its transit links in its router-LSA as having infinite distance so that other routers will avoid calculating transit paths through the router while still being able to reach networks through the router. This support may be enabled administratively (and indefinitely) or conditionally. Conditional enabling of max-metric router-lsas can be for a period of seconds after startup and/or for a period of seconds prior

to shutdown. Enabling this for a period after startup allows OSPF to converge fully first without affecting any existing routes used by other routers, while still allowing any connected stub links and/or redistributed routes to be reachable. Enabling this for a period of time in advance of shutdown allows the router to gracefully excuse itself from the OSPF domain. Enabling this feature administratively allows for administrative intervention for whatever reason, for an indefinite period of time. Note that if the configuration is written to file, this administrative form of the stub-router command will also be written to file. If ospfd is restarted later, the command will then take effect until manually deconfigured.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **max-metric router-lsa** { **administrative** | **on-shutdown** *time* | **on-startup** *time* }

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

administrative: Administratively applied, for an indefinite period.

on-shutdown: Advertise stub-router prior to full shutdown of OSPF.

time: The value range is from 5 to 86400.

on-startup: Automatically advertise stub Router-LSA on startup of OSPF.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf max-metric router-lsa on-startup 10.
```

1.45 config frr ospf network area

Function

Run the **config frr ospf network area** command to specify the OSPF enabled interface(s). If the interface has an address from range A.B.C.D/M then the command below enables ospf on this interface so router can provide network information to the other ospf routers via this interface.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **network** *A.B.C.D/M* **area** *A.B.C.D*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf network 192.168.1.0/24 area 1.1.1.1
```

1.46 config frr ospf ospf abr-type

Function

Run the **config frr ospf ospf abr-type** command to configure the ABR type. The “Cisco” and “IBM” types are equivalent. The OSPF standard for ABR behaviour does not allow an ABR to consider routes through non-backbone areas when its links to the backbone are down, even when there are other ABRs in attached non-backbone areas which still can reach the backbone - this restriction exists primarily to ensure routing-loops are avoided. With the “Cisco” or “IBM” ABR type, the default in this release of FRR, this restriction is lifted, allowing an ABR to consider summaries learned from other ABRs through non-backbone areas, and hence route via non-backbone areas as a last resort when, and only when, backbone links are down.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **ospf abr-type** { **cisco** | **ibm** | **shortcut** | **standard** }

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

cisco: Alternative ABR, cisco implementation.

ibm: Alternative ABR, IBM implementation.

shortcut: Shortcut ABR.

standard: Standard behavior (RFC2328).

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf ospf abr-type shortcut
```

1.47 config frr ospf ospf opaque-lsa

Function

Run the **config frr ospf ospf opaque-lsa** command to configure OSPF opaque LSA. Ospfd supports Opaque LSA (RFC 2370) as partial support for MPLS Traffic Engineering LSAs. The opaque-lsa capability must be enabled in the configuration. An alternate command could

be “mpls-te on” (Traffic Engineering). Note that FRR offers only partial support for some of the routing protocol extensions that are used with MPLS-TE; it does not support a complete RSVP-TE solution.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **ospf opaque-lsa**

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf ospf opaque-lsa
```

1.48 config frr ospf ospf rfc1583compatibility

Function

Run the **config frr ospf ospf rfc1583compatibility** command to make software being compatible with RFC 1583. RFC 2328, the successor to RFC 1583, suggests according to section G.2 (changes) in section 16.4 a change to the path preference algorithm that prevents possible routing loops that were possible in the old version of OSPFv2. More specifically it demands that inter-area paths and intra-area backbone path are now of equal preference but still both preferred to external paths.

NOTE
This command should NOT be set normally.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **ospf rfc1583compatibility**

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf ospf rfc1583compatibility
```

1.49 config frr ospf ospf router-id

Function

Run the **config frr ospf ospf router-id** command to set the router-ID of the OSPF process. The router-ID may be an IP address of the router, but need not be - it can be any arbitrary 32bit number. However it MUST be unique within the entire OSPF domain to the OSPF speaker - bad things will happen if multiple OSPF speakers are configured with the same router-ID! If one is not specified then ospfd will obtain a router-ID automatically from zebra.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **ospf router-id** *A.B.C.D*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

A.B.C.D: The router-ID of the OSPF process.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf ospf router-id 1.1.1.1
```

1.50 config frr ospf ospf write-multiplier

Function

Run the **config frr ospf ospf write-multiplier** command to tune the amount of work done in the packet read and write threads before relinquishing control. The parameter is the number of packets to process before returning. The defult value of this parameter is 20.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **ospf write-multiplier** *number*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

number: The number of packets to process before returning, the value range is from 1 to 100.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf ospf write-multiplier 10
```

1.51 config frr ospf passive-interface

Function

Run the **config frr ospf passive-interface** command to make all interfaces that belong to this router passive by default. For the description of passive interface look at ip ospf passive [A.B.C.D]. Per-interface configuration takes precedence over the default value.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **passive-interface** *interface-name*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

interface-name: Default or interface name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf passive-interface Ethernet1
```

1.52 config frr ospf proactive-arp

Function

Run the **config frr ospf proactive-arp** command to enables or disables sending ARP requests to update neighbor table entries. It speeds up convergence for /32 networks on a P2P connection. This feature is enabled by default.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **proactive-arp**

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf proactive-arp
```

1.53 config frr ospf router-info

Function

Run the **config frr ospf router-info** command to enable Router Information (RFC 4970) LSA advertisement with AS scope (default) or Area scope flooding when area is specified. Old syntax router-info area <A.B.C.D> is always supported but mark as deprecated as the area ID is no more necessary. Indeed, router information support multi-area and detect automatically the areas.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **router-info** { **area** { *A.B.C.D* | **default** } | **as** }

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

area: Enable the Router Information functionality with Area flooding scope.

as: Enable the Router Information functionality with AS flooding scope.

default: Enable the Router Information functionality with Area flooding scope.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf router-info as
```

1.54 config frr ospf timers lsa min-arrival

Function

Run the **config frr ospf timers lsa min-arrival** command to set the minimum time interval that should be elapsed before accepting a version of the same LSA.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **timers lsa min-arrival** *time*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

time: the minimum time interval that should be elapsed before accepting a version of the same LSA, the value range is from 0 to 600000.

Usage Guidelines

N/A

Examples

admin@sonic:~$ sudo config frr ospf timers lsa min-arrival 10

1.55 config frr ospf timers throttle lsa all

Function

Run the **config frr ospf timers throttle lsa all** command to control the generation (sending) of LSAs. The first LSA is always generated immediately upon an OSPF topology change, and the next LSA generated is controlled by the minimum start interval. The subsequent LSAs generated for the same LSA are rate-limited until the maximum interval is reached. The "same LSA" is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. The timers lsa arrival command controls the minimum interval for accepting the same LSA. If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped. It is recommended that the arrival interval be less than or equal to the hold-time interval of the timers throttle lsa all command.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **timers throttle lsa all** *time*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

time: The value range is from 0 to 5000.

Usage Guidelines

N/A

Examples

admin@sonic:~$ sudo config frr ospf timers throttle lsa all 10

1.56 config frr ospf timers throttle spf

Function

Run the **config frr ospf timers throttle spf** command to set the initial delay, the initial-holdtime and the maximum-holdtime between when SPF is calculated and the event which triggered the calculation. The times are specified in milliseconds and must be in the range of 0 to 600000 milliseconds. The delay specifies the minimum amount of time to delay SPF calculation (hence it affects how long SPF calculation is delayed after an event which occurs outside of the holdtime of any previous SPF calculation, and also serves as a

minimum holdtime). Consecutive SPF calculations will always be separated by at least 'hold-time' milliseconds. The hold-time is adaptive and initially is set to the initial-holdtime configured with the above command. Events which occur within the holdtime of the previous SPF calculation will cause the holdtime to be increased by initial-holdtime, bounded by the maximum-holdtime configured with this command. If the adaptive hold-time elapses without any SPF-triggering event occurring then the current holdtime is reset to the initial-holdtime. The current holdtime can be viewed with show ip ospf, where it is expressed as a multiplier of the initial-holdtime.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **timers throttle spf** *initial-delay initial-holdtime maximum-holdtime*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

initial-delay: The value range is from 0 to 600000.

initial-holdtime: The value range is from 0 to 600000.

maximum-holdtime: The value range is from 0 to 600000.

Usage Guidelines

N/A

Examples

admin@sonic:~$ sudo config frr ospf timers throttle spf 100 100 100

1.57 config frr ospf write-multiplier

Function

Run the **config frr ospf write-multiplier** command to tune the amount of work done in the packet read and write threads before relinquishing control. The parameter is the number of packets to process before returning. The defult value of this parameter is 20.

Syntax

config frr ospf [**--vrfname** *VRF*] [**no**] **write-multiplier** *number*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

number: The number of packets to process before returning, the value range is from 0 to 100.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf write-multiplie 10
```

1.58 config frr ospf6 area export-list

Function

Run the **config frr ospf6 area export-list** command to filter Type-3 summary-LSAs announced to other areas originated from intra-area paths from specified area.

Syntax

config frr ospf6 [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **export-list** *name*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

name: Name of the access-list.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf6 area 1.1.1.3 export-list foo
```

1.59 config frr ospf6 area filter-list prefix

Function

Run the **config frr ospf6 area filter-list prefix** command to filter Type-3 summary-LSAs to/from area using prefix lists.

NOTE
This command makes sense in ABR only.

Syntax

config frr ospf6 [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **filter-list prefix** *name* { **in** | **out** }

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

name: Name of the access-list.

in: Filter networks sent to this area.

out: Filter networks sent from this area.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf6 area 1.1.1.3 filter-list prefix foo in
```

1.60 config frr ospf6 area import-list

Function

Run the **config frr ospf6 area import-list** command to filter Type-3 summary-LSAs. Same as export-list, but it applies to paths announced into specified area as Type-3 summary-LSAs.

Syntax

config frr ospf6 [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **import-list** *name*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

name: Name of the access-list.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf6 area 1.1.1.3 import-list foo
```

1.61 config frr ospf6 area range

Function

Run the **config frr ospf6 area range** command to summarize a group of internal subnets into a single Inter-Area-Prefix LSA. This command can only be used at the area boundary (ABR router). By default, the metric of the summary route is calculated as the highest metric among the summarized routes. The cost option, however, can be used to set an explicit metric. The not-advertise option, when present, prevents the summary route from being advertised, effectively filtering the summarized routes.

Syntax

config frr ospf6 [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **range** *X:X::X:X/M* [**--advertise** { **false** | **true** }] [**--cost** *cost-value*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

--advertise false: Do not advertise this range.

--advertise true: Advertise this range.

--cost *cost-value*: User specified metric for this range, the value range is from 0 to 16777215.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf6 area 1.1.1.1 range 1::32/64
```

1.62 config frr ospf6 area stub

Function

Run the **config frr ospf6 area stub** command to specify the area to be a Stub Area. That is, an area where no router originates routes external to OSPF and hence an area where all external routes are via the ABR(s). Hence, ABRs for such an area do not need to pass AS-External LSAs (type-5) or ASBR-Summary LSAs (type-4) into the area. They need only pass Network-Summary (type-3) LSAs into such an area, along with a default-route summary. This command (no-summary) specifies the area to be a Totally Stub Area. In addition to stub area limitations this area type prevents an ABR from injecting Network-Summary (type-3) LSAs into the specified stub area. Only default summary route is allowed.

Syntax

config frr ospf6 [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **stub** { **default** | **no-summary** }

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

default: Configure OSPF area as stub.

no-summary: Do not inject inter-area routes into stub.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf6 area 1.1.1.3 stub default
```

1.63 config frr ospf6 area redistribute

Function

Run the **config frr ospf6 area redistribute** command to redistribute routes of the specified protocol or kind into OSPFv3, with the metric type and metric set if specified, filtering the routes using the given route-map if specified.

Syntax

config frr ospf6 [**--vrfname** *VRF*] [**no**] **area** *A.B.C.D* **redistribute** { **babel** | **bgp** | **connected** | **isis** | **kernel** | **nd-route** | **nhrp** | **openfabric** | **ripng** | **sharp** | **static** | **table** | **vnc** } [**--route-map** *name*]

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

babel: Babel routing protocol (Babel).

bgp: Border Gateway Protocol (BGP).

connected: Connected routes (directly attached subnet or host).

isis: Intermediate System to Intermediate System (IS-IS).

kernel: Kernel routes (not installed via the zebra RIB).

nd-route: ND to route.

nhrp: Next Hop Resolution Protocol (NHRP).

openfabric: OpenFabric Routing Protocol.

ripng: Routing Information Protocol next-generation (IPv6) (RIPng).

static: Statically configured routes.

table: Non-main Kernel Routing Table.

vnc: Virtual Network Control (VNC).

--metric-type *type*: OSPF exterior metric type for redistributed routes, the value range is from 1 to 2.

--route-map WORD: Route map reference.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf6 redistribute kernel
```

1.64 config frr ospf6 auto-cost reference-bandwidth

Function

Run the **config frr ospf6 auto-cost reference-bandwidth** command to set the reference bandwidth for cost calculations, where this bandwidth is considered equivalent to an OSPF cost of 1, specified in Mbits/s. The default is 100Mbit/s (i.e. a link of bandwidth 100Mbit/s or higher will have a cost of 1. Cost of lower bandwidth links will be scaled with reference to this cost).

NOTE:
This configuration setting MUST be consistent across all routers within the OSPF domain.

Syntax

config frr ospf6 [**--vrfname** *VRF*] [**no**] **auto-cost reference-bandwidth** *bandwidth*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

bandwidth: The reference bandwidth for cost calculations, the value range is from 1 to 4294967.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf6 auto-cost reference-bandwidth 100
```

1.65 config frr ospf6 router-id

Function

Run the **config frr ospf6 router-id** command to set router's Router-ID.

Syntax

config frr ospf6 [**--vrfname** *VRF*] [**no**] **ospf6 router-id** *A.B.C.D*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf6 ospf6 router-id 1.1.1.1
```

1.66 config frr ospf6 stub-router administrative

Function

Run the **config frr ospf6 stub-router administrative** command to administratively declare this router as a stub router, having no external connections.

Syntax

config frr ospf6 [**--vrfname** *VRF*] [**no**] **stub-router administrative**

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf6 stub-router administrative
```

1.67 config frr ospf6 timers lsa min-arrival

Function

Run the **config frr ospf6 timers lsa min-arrival** command to set LSA min-arrival timers. The minimum time allowed between advertisements by neighbors, from 0-600000, in milliseconds. Default is 1000.

Syntax

config frr ospf6 [**--vrfname** *VRF*] [**no**] **timers lsa min-arrival** *time*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

time: The minimum time allowed between advertisements by neighbors, from 0-600000, in milliseconds.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf6 timers lsa min-arrival 2000
```

1.68 config frr ospf6 timers throttle spf

Function

Run the **config frr ospf6 timers throttle spf** command to set the initial delay, the initial-holdtime and the maximum-holdtime between when SPF is calculated and the event which triggered the calculation. The times are specified in milliseconds and must be in the range of 0 to 600000 milliseconds. The delay specifies the minimum amount of time to delay SPF calculation (hence it affects how long SPF calculation is delayed after an event which occurs outside of the holdtime of any previous SPF calculation, and also serves as a minimum holdtime). Consecutive SPF calculations will always be separated by at least 'hold-time' milliseconds. The hold-time is adaptive and initially is set to the initial-holdtime configured with the above command. Events which occur within the holdtime of the previous SPF calculation will cause the holdtime to be increased by initial-holdtime, bounded by the maximum-holdtime configured with this command. If the adaptive hold-time elapses without any SPF-triggering event occurring then the current holdtime is reset to the initial-holdtime.

Syntax

config frr ospf6 [**--vrfname** *VRF*] [**no**] **timers throttle spf** *initial-delay initial-holdtime maximum-holdtime*

Parameter Description

--vrfname *VRF*: Specify a VRF for ospf.

no: Negate a command or set its defaults.

initial-delay: The value range is from 0 to 600000.

initial-holdtime: The value range is from 0 to 600000.

maximum-holdtime: The value range is from 0 to 600000.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config frr ospf6 timers throttle spf 100 100 100
```

1.69 show ip ospf

Function

Run the **show ip ospf** command to display the OSPF status.

Syntax

show ip ospf [**all** | **border-routers** | **database** | **interface** | **neighbor** | **route** | **router-info**]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ip ospf all
  OSPF Routing Process, Router ID: 10.0.0.5
  Supports only single TOS (TOS0) routes
  This implementation conforms to RFC2328
  RFC1583Compatibility flag is disabled
  OpaqueCapability flag is disabled
  Initial SPF scheduling delay 0 millisec(s)
  Minimum hold time between consecutive SPFs 50 millisec(s)
  Maximum hold time between consecutive SPFs 5000 millisec(s)
  Hold time multiplier is currently 1
  SPF algorithm last executed 44m57s ago
  Last SPF duration 23 usecs
  SPF timer is inactive
  LSA minimum interval 5000 msecs
  LSA minimum arrival 1000 msecs
  Write Multiplier set to 20
  Refresh timer 10 secs
  Number of external LSA 0. Checksum Sum 0x00000000
  Number of opaque AS LSA 0. Checksum Sum 0x00000000
  Number of areas attached to this router: 4
  Area ID: 0.0.0.0 (Backbone)
    Number of interfaces in this area: Total: 1, Active: 0
    Number of fully adjacent neighbors in this area: 0
    Area has no authentication
    SPF algorithm executed 0 times
    Number of LSA 0
    Number of router LSA 0. Checksum Sum 0x00000000
    Number of network LSA 0. Checksum Sum 0x00000000
    Number of summary LSA 0. Checksum Sum 0x00000000
```

```
    Number of ASBR summary LSA 0. Checksum Sum 0x00000000
    Number of NSSA LSA 0. Checksum Sum 0x00000000
    Number of opaque link LSA 0. Checksum Sum 0x00000000
    Number of opaque area LSA 0. Checksum Sum 0x00000000

  Area ID: 0.0.0.1
    Shortcutting mode: Default, S-bit consensus: ok
    Number of interfaces in this area: Total: 0, Active: 0
    Number of fully adjacent neighbors in this area: 0
    Area has no authentication
    Number of full virtual adjacencies going through this area: 0
    SPF algorithm executed 3 times
    Number of LSA 1
    Number of router LSA 1. Checksum Sum 0x00004ef4
    Number of network LSA 0. Checksum Sum 0x00000000
    Number of summary LSA 0. Checksum Sum 0x00000000
    Number of ASBR summary LSA 0. Checksum Sum 0x00000000
    Number of NSSA LSA 0. Checksum Sum 0x00000000
    Number of opaque link LSA 0. Checksum Sum 0x00000000
    Number of opaque area LSA 0. Checksum Sum 0x00000000
```

1.70 show ipv6 ospf6

Function

Run the **show ipv6 ospf6** command to display the OSPF6 status.

Syntax

show ipv6 ospf6 [**all** | **border-routers** | **interface** | **neighbor** | **route** | **area** | **database** | **linkstate** | **redistribute** | **spf**]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ipv6 ospf6 all
   OSPFv3 Routing Process (0) with Router-ID 51.0.0.1
   Running 00:28:28
   LSA minimum arrival 1000 msecs
   Initial SPF scheduling delay 0 millisec(s)
   Minimum hold time between consecutive SPFs 50 millsecond(s)
   Maximum hold time between consecutive SPFs 5000 millsecond(s)
   Hold time multiplier is currently 1
```

```
  SPF algorithm has not been run
  SPF timer is inactive
  Number of AS scoped LSAs is 0
  Number of areas in this router is 1

  Area 0.0.0.5
        Number of Area scoped LSAs is 0
        Interface attached to this area: Ethernet14
SPF has not been run
```

1 BGP Commands

Command	Function
bgp advertise lowest-priority on-startup	Configure BGP to minimize the priorities of the BGP routes to be advertised upon system restart.
bgp evpn-vni-list	Configure the VNI list configuration of EVPN.
bgp initial-advertise-delay	Intend for the configuration of delayed route advertisement upon system restart.
clear bgp advertise lowest-priority on-startup	Restore the priorities of the BGP routes advertised to neighbors.
config bgp remove neighbor	Remove particular IPv4 or IPv6 BGP neighbor configuration using either the IP address or hostname.
config bgp shutdown all	Shutdown all the BGP IPv4 & IPv6 sessions.
config bgp shutdown neighbor	Shut down a BGP session with a neighbor by that neighbor's IP address or hostname.
config bgp startup all	Start up all the IPv4 & IPv6 BGP neighbors.
config bgp startup neighbor	Start up the particular IPv4 or IPv6 BGP neighbor using either the IP address or hostname.
redistribute	Redistribute the route information of other routing protocols to BGP.
show bgp evpn-vni-list	Display the VNI list configuration of EVPN.
show ip bgp neighbors	Display all the details of IPv4 & IPv6 BGP neighbors when no optional argument is specified.
show ipv6 bgp neighbors	Display all the details of one particular IPv6 Border Gateway Protocol (BGP) neighbor. Option is also available to display only the advertised routes, or the received routes, or all routes.
show ip bgp network	Display all the details of IPv4 Border

	Gateway Protocol (BGP) prefixes.
show ipv6 bgp network	Display all the details of IPv6 Border Gateway Protocol (BGP) prefixes.
show ip bgp summary	Display the summary of all IPv4 & IPv6 bgp neighbors that are configured and the corresponding states.
show ipv6 bgp summary	Display the summary of all IPv6 bgp neighbors that are configured and the corresponding states.
show route-map	Display the routing policy that takes precedence over the other route processes that are configured.

1.1 bgp advertise lowest-priority on-startup

Function

Run the **bgp advertise lowest-priority on-startup** command to configure BGP to minimize the priorities of the BGP routes to be advertised upon system restart.

Syntax

[**no**] **bgp advertise lowest-priority on-startup** [*recover-time*]

Parameter Description

recover-time: The time for restoring the priority of the advertised routes, in seconds. The value ranges from 1 to 65535, and the default value is 600.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "router bgp 100" -c "bgp advertise lowest-priority on-startup"
```

1.2 bgp evpn-vni-list

Function

Run the **bgp evpn-vni-list** command to configure the VNI list configuration of EVPN.

Syntax

[**no**] **bgp evpn-vni-list** { *list-name* } *vni1*, *vni2*,...

Parameter Description

List-name: The name of a VNI list.

vni: The VNI ID. The value ranges from 1 to 16777215. The information of multiple VNIs can be configured at the same time, and all the VNIs are separated using commas.

Usage Guidelines

When the local host goes online, BGP will send the host ARP routing information to its neighbors. However, if the peer end does not want to generate traffic redirection through ARP, you can control the local ARP routes so that local ARP routes are not sent to the peer end.

This command combines route map and is used on neighbors.

Examples

```
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "bgp evpn-vni-list v1 100,200"
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "route-map map1 deny 10" -c "match evpn deny-arp v1 local"
```

```
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "route-map map1 permit 20"
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "router bgp 65530" -c "address-family l2vpn
evpn" -c "neighbor 13.1.1.1 activate" -c "neighbor 13.1.1.1 route-map map1 out"
```

1.3 bgp initial-advertise-delay

Function

Run the **bgp initial-advertise-delay** command to intend for the configuration of delayed route advertisement upon system restart.

Syntax

[**no**] **bgp initial-advertise-delay** { *delay-time* [*startup-time*] | **prefix-list** *name* }

Parameter Description

delay-time: The delay time for advertising routes after the BGP neighborship is established upon system restart, in seconds. The value ranges from 1 to 600. The default value is 1.

startup-time: The time for system restart (the mechanism of delayed route advertisement is adopted for the neighbor in this period), in seconds. The value range is from 5 to 58400. The default value is 600.

name: The name of the prefix list.

Usage Guidelines

Delay-time indicates the maximum time to wait for BGP neighbors to send routes to their neighbors after establishing a connection. After a neighborship is established, normally the first route is advertised immediately, and the subsequent route advertisement is delayed as default (see the neighbor advertisement-interval command). Startup-time indicates the user configurable startup time, which is timed from the time when the command takes effect. During startup-time, BGP neighbor routes are advertised at the interval of delay-time. This command can change the route advertisement behavior of BGP peers after system restart.

The prefix-list policy is configured to ensure that partial routes can be normally delivered. The prefix-list policy applies to distributed routes. Matched routes will be normally delivered without being affected by delayed advertisement. For details about the address family scope to which the prefix-list policy applies, see the neighbor prefix-list command.

This command is used by the administrator to adjust the BGP route advertisement behavior during device restart based on the hardware conditions, number of neighbors, number of routes, and actual deployment requirements.

Examples

```
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "router bgp 100" -c "bgp initial-advertise-delay
60 500" -c "bgp initial-advertise-delay prefix-list aa"
```

1.4 clear bgp advertise lowest-priority on-startup

Function

Run the **clear bgp advertise lowest-priority on-startup** command to restore the priorities of the BGP routes advertised to neighbors.

Syntax

clear bgp advertise lowest-priority on-startup

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo vtysh -c "clear bgp advertise lowest-priority on-startup"
```

1.5 config bgp remove neighbor

Function

Run the **config bgp remove neighbor** command to remove particular IPv4 or IPv6 BGP neighbor configuration using either the IP address or hostname.

Syntax

sudo config bgp remove neighbor { *ip-address* | *hostname* }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config bgp remove neighbor 192.168.1.124

admin@sonic:~$ sudo config bgp remove neighbor 2603:10b0:b0f:346::4a

admin@sonic:~$ sudo config bgp remove neighbor SONIC02SPINE
```

1.6 config bgp shutdown all

Function

Run the **config bgp shutdown all** command to shutdown all the BGP IPv4 & IPv6 sessions.

When the session is shutdown using this command, BGP state in "show ip bgp summary" is displayed as "Idle (Admin)".

Syntax

config bgp shutdown all

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config bgp shutdown all
```

1.7 config bgp shutdown neighbor

Function

Run the **config bgp shutdown neighbor** command to shut down a BGP session with a neighbor by that neighbor's IP address or hostname.

Syntax

sudo config bgp shutdown neighbor { *ip-address* | *hostname* }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config bgp shutdown neighbor 192.168.1.124

admin@sonic:~$ sudo config bgp shutdown neighbor SONIC02SPINE
```

1.8 config bgp startup all

Function

Run the **config bgp startup all** command to start up all the IPv4 & IPv6 BGP neighbors.

Syntax

config bgp startup all

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config bgp startup all
```

1.9 config bgp startup neighbor

Function

Run the **config bgp startup neighbor** command to start up the particular IPv4 or IPv6 BGP neighbor using either the IP address or hostname.

Syntax

config bgp startup neighbor { *ip-address* | *hostname* }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config bgp startup neighbor 192.168.1.124

admin@sonic:~$ sudo config bgp startup neighbor SONIC02SPINE
```

1.10 redistribute

Function

Run the **redistribute** command to redistribute the route information of other routing protocols to BGP.

Redistribution arp-host added to IPv4 unicast address family.

Redistribution nd route added to IPv6 unicast address family.

Syntax

[**no**] **redistribute** [**arp-host** | **nd-route**]

Parameter Description

arp-host: Host routes converted from ARP entries.

nd-route: Host routes converted from ND entries.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "router bgp 100" -c "address-family ipv4
unicast" -c "redistribute arp-host" -c "address-family ipv6 unicast" -c "redistribute nd-route"
```

1.11 show bgp evpn-vni-list

Function

Run the **show bgp evpn-vni-list** command to display the VNI list configuration of EVPN.

Syntax

show bgp evpn-vni-list { *list-name* }

Parameter Description

list-name: The name of a VNI list.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo vtysh -c "show bgp evpn-vni-list "
bgp evpn-vni-list v1:
    10 20
```

1.12 show ip bgp neighbors

Function

Run the **show ip bgp neighbors** command to display all the details of IPv4 & IPv6 BGP neighbors when no optional argument is specified.

When the optional argument IPv4_address is specified, it displays the detailed neighbor information about that specific IPv4 neighbor.

Command has got additional optional arguments to display only the advertised routes, or the received routes, or all routes.

In order to get details for an IPv6 neigbor, use "show bgp ipv6 neighbor" command.

Syntax

- Versions >= 201904 using default FRR routing stack:

show bgp neighbors [*ipv4-address* [**advertised-routes** | **received-routes** | **routes**]]

- Versions <= 201811 using Quagga routing stack:

show ip bgp neighbors [*ipv4-address* [**advertised-routes** | **received-routes** | **routes**]]

Parameter Description

ipv4-address: Display the detailed neighbor information about the specific IPv4 neighbor.

advertised-routes: Display only the advertised routes.

received-routes: Display only the received routes.

routes: Display all routes.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ip bgp neighbors
BGP neighbor is 10.0.0.57, remote AS 64600, local AS 65100, external link
Description: Router01T1
BGP version 4, remote router ID 100.1.0.29, local router ID 10.1.0.32
BGP state = Established, up for 00:42:15
Last read 00:00:00, Last write 00:00:03
Hold time is 10, keepalive interval is 3 seconds
Configured hold time is 10, keepalive interval is 3 seconds
Neighbor capabilities:
  4 Byte AS: advertised and received
  AddPath:
    IPv4 Unicast: RX advertised IPv4 Unicast and received
  Route refresh: advertised and received(new)
  Address Family IPv4 Unicast: advertised and received
  Hostname Capability: advertised (name: sonic-z9264f-9251,domain name: n/a) not received
  Graceful Restart Capability: advertised and received
    Remote Restart timer is 300 seconds
    Address families by peer:
      none
Graceful restart information:
  End-of-RIB send: IPv4 Unicast
  End-of-RIB received: IPv4 Unicast
Message statistics:
  Inq depth is 0
  Outq depth is 0
                       Sent       Rcvd
  Opens:                  2          1
  Notifications:          2          0
  Updates:             3206       3202
  Keepalives:           845        847
  Route Refresh:          0          0
  Capability:             0          0
```

```
  Total:                    4055          4050
Minimum time between advertisement runs is 0 seconds
 For address family: IPv4 Unicast
 Update group 1, subgroup 1
 Packet Queue length 0
 Inbound soft reconfiguration allowed
 Community attribute sent to this neighbor(all)
 6400 accepted prefixes

 Connections established 1; dropped 0
 Last reset 00:42:37, due to NOTIFICATION sent (Cease/Connection collision resolution)
 Local host: 10.0.0.56, Local port: 179
 Foreign host: 10.0.0.57, Foreign port: 46419
 Nexthop: 10.0.0.56
 Nexthop global: fc00::71
 Nexthop local: fe80::2204:fff:fe36:9449
 BGP connection: shared network
 BGP Connect Retry Timer in Seconds: 120
 Read thread: on    Write thread: on
```

Optionally, you can specify an IP address in order to display only that particular neighbor. In this mode, you can optionally specify whether you want to display all routes advertised to the specified neighbor, all routes received from the specified neighbor or all routes (received and accepted) from the specified neighbor.

```
admin@sonic:~$ show bgp neighbors 10.0.0.57

admin@sonic:~$ show bgp neighbors 10.0.0.57 advertised-routes

admin@sonic:~$ show bgp neighbors 10.0.0.57 received-routes

admin@sonic:~$ show bgp neighbors 10.0.0.57 routes
```

1.13 show ipv6 bgp neighbors

Function

Run the **show ipv6 bgp neighbors** command to display all the details of one particular IPv6 Border Gateway Protocol (BGP) neighbor. Option is also available to display only the advertised routes, or the received routes, or all routes.

Syntax

- Versions >= 201904 using default FRR routing stack:

show bgp ipv6 neighbors [*ipv6-address* [**advertised-routes** | **received-routes** | **routes**]]

- Versions <= 201811 using Quagga routing stack:

show ipv6 bgp neighbors [*ipv6-address* [**advertised-routes** | **received-routes** | **routes**]]

Parameter Description

ipv6-address: Display the detailed neighbor information about the specific IPv6 neighbor.

advertised-routes: Display only the advertised routes.

received-routes: Display only the received routes.

routes: Display all routes.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ipv6 bgp neighbors
BGP neighbor is 3000::1, remote AS 65100, local AS 1, external link
  Local Role: undefined
  Remote Role: undefined
Hostname: sonic
  BGP version 4, remote router ID 1.2.3.4, local router ID 1.2.3.4
  BGP state = Idle
  Last read 00:00:35, Last write 00:00:04
  Hold time is 180 seconds, keepalive interval is 60 seconds
  Configured hold time is 180 seconds, keepalive interval is 60 seconds
  Configured tcp-mss is 0, synced tcp-mss is 0
  Configured conditional advertisements interval is 60 seconds
  Graceful restart information:
    Local GR Mode: Restart*

    Remote GR Mode: NotApplicable

    R bit: False
    N bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 120
      Configured LLGR Stale Path Time(sec): 0
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  9          7
    Notifications:          2         18
    Updates:                0          0
    Keepalives:             5          0
    Route Refresh:          0          0
    Capability:             0          0
    Total:                 16         25
```

```
  Minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast
  Not part of any update group
  Community attribute sent to this neighbor(all)
  0 accepted prefixes

  Connections established 0; dropped 0
  Last reset 00:00:35,    Notification received (OPEN Message Error/Bad BGP Identifier)
  External BGP neighbor may be up to 1 hops away.
Local host: 3000::251, Local port: 42380
Foreign host: 3000::1, Foreign port: 179
Nexthop: 10.0.0.28
Nexthop global: 3000::251
Nexthop local: fe80::c2b8:e6ff:fe74:4786
```

Optionally, you can specify an IP address in order to display only that particular neighbor. In this mode, you can optionally specify whether you want to display all routes advertised to the specified neighbor, all routes received from the specified neighbor or all routes (received and accepted) from the specified neighbor.

```
admin@sonic:~$ show ipv6 bgp neighbors fc00::72 advertised-routes

admin@sonic:~$ show ipv6 bgp neighbors fc00::72 received-routes

admin@sonic:~$ show ipv6 bgp neighbors fc00::72 routes
```

1.14 show ip bgp network

Function

Run the **show ip bgp network** command to display all the details of IPv4 Border Gateway Protocol (BGP) prefixes.

Syntax

show ip bgp network [*ipv4-address* | *ipv4-prefix*] [**bestpath** | **multipath** | **longer-prefixes** | **json**]

Parameter Description

N/A

Usage Guidelines

The "longer-prefixes" option is only available when a network prefix with a "/" notation is used.

Examples

```
admin@sonic:~$ show ip bgp network
```

```
admin@sonic:~$ show ip bgp network 10.1.0.32 bestpath

admin@sonic:~$ show ip bgp network 10.1.0.32 multipath

admin@sonic:~$ show ip bgp network 10.1.0.32 json

admin@sonic:~$ show ip bgp network 10.1.0.32/32 bestpath

admin@sonic:~$ show ip bgp network 10.1.0.32/32 multipath

admin@sonic:~$ show ip bgp network 10.1.0.32/32 json

admin@sonic:~$ show ip bgp network 10.1.0.32/32 longer-prefixes
```

1.15 show ipv6 bgp network

Function

Run the **show ipv6 bgp network** command to display all the details of IPv6 Border Gateway Protocol (BGP) prefixes.

Syntax

show ip bgp network [*ipv4-address* | *ipv4-prefix*] [**bestpath** | **multipath** | **longer-prefixes** | **json**]

Parameter Description

N/A

Usage Guidelines

The "longer-prefixes" option is only available when a network prefix with a "/" notation is used.

Examples

```
admin@sonic:~$ show ipv6 bgp network

admin@sonic:~$ show ipv6 bgp network fc00::72 bestpath

admin@sonic:~$ show ipv6 bgp network fc00::72 multipath

admin@sonic:~$ show ipv6 bgp network fc00::72 json

admin@sonic:~$ show ipv6 bgp network fc00::72/64 bestpath

admin@sonic:~$ show ipv6 bgp network fc00::72/64 multipath
```

```
admin@sonic:~$ show ipv6 bgp network fc00::72/64 json

admin@sonic:~$ show ipv6 bgp network fc00::72/64 longer-prefixes
```

1.16 show ip bgp summary

Function

Run the **show ip bgp summary** command to display the summary of all IPv4 & IPv6 bgp neighbors that are configured and the corresponding states.

Syntax

- Versions >= 201904 using default FRR routing stack:

show bgp summary

- Versions <= 201811 using Quagga routing stack:

show ip bgp summary

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ip bgp summary

IPv4 Unicast Summary:
BGP router identifier 10.1.0.32, local AS number 65100 vrf-id 0
BGP table version 6465
RIB entries 12807, using 2001 KiB of memory
Peers 4, using 83 KiB of memory
Peer groups 2, using 128 bytes of memory

Neighbor        V     AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd
NeighborName
10.0.0.57       4  64600    3995    4001        0    0    0 00:39:32         6400 Lab-T1-01
10.0.0.59       4  64600    3995    3998        0    0    0 00:39:32         6400 Lab-T1-02
10.0.0.61       4  64600    3995    4001        0    0    0 00:39:32         6400 Lab-T1-03
10.0.0.63       4  64600    3995    3998        0    0    0 00:39:32         6400
NotAvailable

Total number of neighbors 4
```

```
admin@sonic:~$ show bgp summary
```

```
IPv4 Unicast Summary:
BGP router identifier 10.1.0.32, local AS number 65100 vrf-id 0
BGP table version 6465
RIB entries 12807, using 2001 KiB of memory
Peers 4, using 83 KiB of memory
Peer groups 2, using 128 bytes of memory

Neighbor        V      AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd
10.0.0.57       4   64600    3995    4001        0    0    0 00:39:32         6400
10.0.0.59       4   64600    3995    3998        0    0    0 00:39:32         6400
10.0.0.61       4   64600    3995    4001        0    0    0 00:39:32         6400
10.0.0.63       4   64600    3995    3998        0    0    0 00:39:32         6400

Total number of neighbors 4

IPv6 Unicast Summary:
BGP router identifier 10.1.0.32, local AS number 65100 vrf-id 0
BGP table version 12803
RIB entries 12805, using 2001 KiB of memory
Peers 4, using 83 KiB of memory
Peer groups 2, using 128 bytes of memory

Neighbor        V      AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd
fc00::72        4   64600    3995    5208        0    0    0 00:39:30         6400
fc00::76        4   64600    3994    5208        0    0    0 00:39:30         6400
fc00::7a        4   64600    3993    5208        0    0    0 00:39:30         6400
fc00::7e        4   64600    3993    5208        0    0    0 00:39:30         6400

Total number of neighbors 4
```

1.17 show ipv6 bgp summary

Function

Run the **show ipv6 bgp summary** command to display the summary of all IPv6 bgp neighbors that are configured and the corresponding states.

Syntax

- Versions >= 201904 using default FRR routing stack:

show bgp ipv6 summary

- Versions <= 201811 using Quagga routing stack:

show ipv6 bgp summary

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show bgp ipv6 summary
BGP router identifier 10.1.0.32, local AS number 65100 vrf-id 0
BGP table version 12803
RIB entries 12805, using 2001 KiB of memory
Peers 4, using 83 KiB of memory
Peer groups 2, using 128 bytes of memory

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd
NeighborName
fc00::72        4      64600    3995    5208        0    0    0 00:39:30         6400 Lab-T1-01
fc00::76        4      64600    3994    5208        0    0    0 00:39:30         6400 Lab-T1-02
fc00::7a        4      64600    3993    5208        0    0    0 00:39:30         6400 Lab-T1-03
fc00::7e        4      64600    3993    5208        0    0    0 00:39:30         6400 Lab-T1-04

Total number of neighbors 4
```

1.18 show route-map

Function

Run the **show route-map** command to display the routing policy that takes precedence over the other route processes that are configured.

Syntax

show route-map

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show route-map
ZEBRA:
route-map RM_SET_SRC, permit, sequence 10
  Match clauses:
  Set clauses:
```

```
    src 10.12.0.102
  Call clause:
  Action:
    Exit routemap
ZEBRA:
route-map RM_SET_SRC6, permit, sequence 10
  Match clauses:
  Set clauses:
    src fc00:1::102
  Call clause:
  Action:
    Exit routemap
BGP:
route-map FROM_BGP_SPEAKER_V4, permit, sequence 10
  Match clauses:
  Set clauses:
  Call clause:
  Action:
    Exit routemap
BGP:
route-map TO_BGP_SPEAKER_V4, deny, sequence 10
  Match clauses:
  Set clauses:
  Call clause:
  Action:
    Exit routemap
BGP:
route-map ISOLATE, permit, sequence 10
  Match clauses:
  Set clauses:
    as-path prepend 65000
  Call clause:
  Action:
    Exit routemap
```

1 VRF Commands

Command	Function
config interface vrf bind	Bind an interface to a vrf. By default, all L3 interfaces will be in default vrf. Above vrf bind command will let users bind interface to a vrf. Using the bind or unbind vrf command will cause L3 interfaces to lose all IP addresses, ARP, and routes.
config interface vrf unbind	Unbind an interface from a vrf. This will move the interface to default vrf.
config vrf add	Create vrf in SONiC system with provided vrf-name.
config vrf add mgmt	Enable the management VRF in the system. This command restarts the "interfaces-config" service which in turn regenerates the /etc/network/interfaces file and restarts the "networking" service. This creates a new interface and l3mdev CGROUP with the name as "mgmt" and enslaves the management interface "eth0" into this master interface "mgmt". Note that the VRFName "mgmt" (or "management") is reserved for management VRF. i.e. Data VRFs should not use these reserved VRF names.
config vrf del	Delete vrf with name vrf-name.
config vrf del mgmt	Disable the management VRF in the system. This command restarts the "interfaces-config" service which in turn regenerates the /etc/network/interfaces file and restarts the "networking" service. This deletes the interface "mgmt" and deletes the l3mdev CGROUP named "mgmt" and puts back the management interface "eth0" into the default VRF. Note that the VRFName "mgmt" (or "management") is reserved for management VRF. i.e. Data VRFs should not use these reserved VRF names.
show management_interface address	Display the IP address(es) configured for

	the management interface "eth0" and the management network default gateway.
show mgmt-vrf	Display whether the management VRF is enabled or disabled. It also displays the details about the the links (eth0, mgmt, lo-m) that are related to management VRF.
show mgmt-vrf routes	Display the routes that are present in the routing table 5000 that is meant for management VRF.
show vrf	Display all vrfs configured on the system along with interface binding to the vrf. If vrf-name is also provided as part of the command, if the vrf is created it will display all interfaces binding to the vrf, if vrf is not created nothing will be displayed.

1.1 config interface vrf bind

Function

Run the **config interface vrf bind** command to bind an interface to a vrf. By default, all L3 interfaces will be in default vrf. Above vrf bind command will let users bind interface to a vrf. Using the bind or unbind vrf command will cause L3 interfaces to lose all IP addresses, ARP, and routes.

Syntax

config interface vrf bind [*interface-name*] [*vrf-name*]

Parameter Description

interface-name: Routed interface name.

vrf-name: VRF name.

Usage Guidelines

When a L2 interface is bound to a VRF, it is automatically converted to a L3 interface.

If a L3 interface has been bound to a non-default VRF, it cannot be bound to another. To change the VRF of the L3 interface, unbind the old VRF and then bind a new one.

A L3 interface configured with a static route cannot be bound to a VRF.

Examples

```
admin@sonic:~$ sudo config interface vrf bind Ethernet1 Vrf1
```

1.2 config interface vrf unbind

Function

Run the **config interface vrf unbind** command to unbind an interface from a vrf. This will move the interface to default vrf.

Syntax

config interface vrf unbind [*interface-name*] [*vrf-name*]

Parameter Description

interface-name: Routed interface name.

vrf-name: VRF name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface vrf unbind Ethernet1 Vrf1
```

1.3 config vrf add

Function

Run the **config vrf add** command to create vrf in SONiC system with provided vrf-name.

Syntax

config vrf add [*vrf-name*]

Parameter Description

N/A

Usage Guidelines

vrf-name should always start with keyword "Vrf".

Examples

N/A

1.4 config vrf add mgmt

Function

Run the **config vrf add mgmt** command to enable the management VRF in the system. This command restarts the "interfaces-config" service which in turn regenerates the /etc/network/interfaces file and restarts the "networking" service. This creates a new interface and l3mdev CGROUP with the name as "mgmt" and enslaves the management interface "eth0" into this master interface "mgmt". Note that the VRFName "mgmt" (or "management") is reserved for management VRF. i.e. Data VRFs should not use these reserved VRF names.

Syntax

config vrf add mgmt

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config vrf add mgmt
```

1.5 config vrf del

Function

Run the **config vrf del** command to delete vrf with name vrf-name.

Syntax

config vrf del [*vrf-name*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

N/A

1.6 config vrf del mgmt

Function

Run the **config vrf del mgmt** command to disable the management VRF in the system. This command restarts the "interfaces-config" service which in turn regenerates the /etc/network/interfaces file and restarts the "networking" service. This deletes the interface "mgmt" and deletes the l3mdev CGROUP named "mgmt" and puts back the management interface "eth0" into the default VRF. Note that the VRFName "mgmt" (or "management") is reserved for management VRF. i.e. Data VRFs should not use these reserved VRF names.

Syntax

config vrf del mgmt

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config vrf del mgmt
```

1.7 show management_interface address

Function

Run the **show management_interface address** command to display the IP address(es) configured for the management interface "eth0" and the management network default gateway.

Syntax

show management_interface address

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show management_interface address
Management IP address = 10.16.210.75/24
Management NetWork Default Gateway = 10.16.210.254
Management IP address = FC00:2::32/64
Management Network Default Gateway = fc00:2::1
```

1.8 show mgmt-vrf

Function

Run the **show mgmt-vrf** command to display whether the management VRF is enabled or disabled. It also displays the details about the the links (eth0, mgmt, lo-m) that are related to management VRF.

Syntax

show mgmt-vrf

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show mgmt-vrf

ManagementVRF : Enabled
```

```
Management VRF interfaces in Linux:
348: mgmt: <NOARP,MASTER,UP,LOWER_UP> mtu 65536 qdisc noqueue state UP mode DEFAULT group
default qlen 1000
    link/ether f2:2a:d9:bc:e8:f0 brd ff:ff:ff:ff:ff:ff
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master mgmt state UP mode
DEFAULT group default qlen 1000
    link/ether 4c:76:25:f4:f9:f3 brd ff:ff:ff:ff:ff:ff
350: lo-m: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue master mgmt state UNKNOWN
mode DEFAULT group default qlen 1000
    link/ether b2:4c:c6:f3:e9:92 brd ff:ff:ff:ff:ff:ff

NOTE: The management interface "eth0" shows the "master" as "mgmt" since it is part of management
VRF.
```

1.9 show mgmt-vrf routes

Function

Run the **show mgmt-vrf routes** command to display the routes that are present in the routing table 5000 that is meant for management VRF.

Syntax

show mgmt-vrf routes

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show mgmt-vrf routes

Routes in Management VRF Routing Table:
default via 10.16.210.254 dev eth0 metric 201
broadcast 10.16.210.0 dev eth0 proto kernel scope link src 10.16.210.75
10.16.210.0/24 dev eth0 proto kernel scope link src 10.16.210.75
local 10.16.210.75 dev eth0 proto kernel scope host src 10.16.210.75
broadcast 10.16.210.255 dev eth0 proto kernel scope link src 10.16.210.75
broadcast 127.0.0.0 dev lo-m proto kernel scope link src 127.0.0.1
127.0.0.0/8 dev lo-m proto kernel scope link src 127.0.0.1
local 127.0.0.1 dev lo-m proto kernel scope host src 127.0.0.1
broadcast 127.255.255.255 dev lo-m proto kernel scope link src 127.0.0.1
```

1.10 show vrf

Function

Run the **show vrf** command to display all vrfs configured on the system along with interface binding to the vrf. If vrf-name is also provided as part of the command, if the vrf is created it will display all interfaces binding to the vrf, if vrf is not created nothing will be displayed.

Syntax

show vrf [*vrf-name*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vrf
VRF            Interfaces
-------        ------------
default        Vlan20
rf-red         Vlan100
                 pback11
                 Eth0.100
rf-blue      Loopback100
                 Loopback102
                 Ethernet0.10
                 PortChannel101
```

1 ACL Commands

Command	Function
config acl add table	Create new ACL tables.
config acl clear counters	Clear ACL counters.
config acl log-update	Control the log output interval by setting the interval for packets to match logs. View ACL logging in the syslog file.
config acl remove rule	Delete a rule from an ACL table.
config acl remove table	Delete an ACL table.
config acl update full	Update the rules in all the tables or in one specific table in full.
config acl update incremental	Configure the rules.
show acl counters	Display the ACL statistics counters.
show acl log-update interval	Display the output interval of ACL matching logs.
show acl resources	Display the ACL resources.
show acl rule	Display all the ACL rules present in all the ACL tables or only the rules present in specified table "TABLE_NAME" or only the rule matching the RULE_ID option.
show acl table	Display either all the ACL tables that are configured or only the specified "TABLE_NAME".

1.1 config acl add table

Function

Run the **config acl add table** command to create new ACL tables.

You can use the high-capacity configuration mode and community configuration mode to create an ACL table. The distinction between the high-capacity configuration mode and the community configuration mode applies only to the ACLs of the data plane.

Syntax

- high-capacity configuration mode:

config acl add table [*OPTIONS*] *table-name table-type* [**-d** *description*] [**-p** *ports*] [**-s** { **ingress** | **egress** }] [**-sp** *cir-cbs*] [**-sd** *dscp-value*] [**-ss** { **SSH** | **NTP** | **SNMP** }]

- community configuration mode:

config acl add table [*OPTIONS*] *table-name table-type* [**-d** *description*] [**-p** *ports*] [**-s** { **ingress** | **egress** }] [**-sp** *cir-cbs*] [**-sd** *dscp-value*] [**-ss** { **SSH** | **NTP** | **SNMP** }] **-m community**

Parameter Description

table-name: The name of the ACL table to create.

table-type: The type of ACL table to create (e.g. "L3", "L3V6", "MIRROR")

description: A description of the table for the user. (default is the table_name)

ports: A comma-separated list of ports/interfaces to add to the table. The behavior is as follows:

- Physical ports will be bound as physical ports
- Portchannels will be bound as portchannels - passing a portchannel member is invalid
- VLANs will be expanded into their members (e.g. "Vlan1000" will become "Ethernet0,Ethernet2,Ethernet4...")

stage: The stage this ACL table will be applied to, either ingress or egress. (default is ingress)

cir-cbs: Configuration example: 1000000_2000. The cir indicates the bandwidth limit per second (KBits). The cbs indicates the burst traffic limit (KBytes). This parameter is used for qos acl.

dscp-value: Specifies the new dscp value of the packet. The value ranges from 0 to 63. This parameter is used for qos acl.

SSH | NTP | SNMP: Indicates the service type of CTRLPLANE ACL. This parameter is used for CTRLPLANE acl.

Usage Guidelines

- ACL restrictions in high-capacity configuration mode
  - In high-capacity configuration mode, only one object (physical interface or portchannel interface) can be applied to the ACL application in the egress direction.
  - In high-capacity configuration mode, when an ACL is applied to portchannel, only one portchannel interface can be applied to an ACL.
  - In high-capacity configuration mode, when an ACL is applied to vni, only one vni can be applied to an ACL.
  - In high-capacity configuration mode, ACL cannot be applied to both physical interfaces and portchannel interfaces.
  - After the ACL is configured in high-capacity mode, it cannot be changed to the community mode. After the ACL is configured as the community mode, it cannot be changed to the high-capacity mode.

Examples

```
admin@sonic:~$ sudo config acl add table EXAMPLE L3 -p Ethernet1,Ethernet4 -s ingress

admin@sonic:~$ sudo config acl add table EXAMPLE_2 L3V6 -p Ethernet2 -s egress

admin@sonic:~$ sudo config acl add table EXAMPLE_3 L3_QOS -p Ethernet5 -s ingress -sp 1024_2048 -sd 30

admin@sonic:~$ sudo config acl add table EXAMPLE_4 L2_QOS -p Ethernet3 -s ingress -sd 28

admin@sonic:~$ sudo config acl add table EXAMPLE_5 L3V6_QOS -p Ethernet6 -s ingress -sp 1000_2000

admin@sonic:~$ sudo config acl add table EXAMPLE_6 CTRLPLANE -ss SSH
```

1.2 config acl clear counters

Function

Run the **config acl clear counters** command to clear ACL counters.

Syntax

sudo sonic-clear acl counters [*table-name*]

Parameter Description

table-name: The name of the ACL table.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show acl counters
RULE NAME            TABLE NAME             PRIO        PACKETS COUNT        BYTES COUNT      UPDATE TIME
-------------     ------------     ------     ---------------     -------------     ---------------
RULE_1                    TEST                          9999                 76042306        9733442816     2023-
03-21 07:35:45
DEFAULT_RULE      TEST                                  1                                0                          0
1970-01-01 00:00:00
admin@sonic:~$ sudo sonic-clear acl counters
admin@sonic:~$ show acl counters
RULE NAME            TABLE NAME             PRIO          PACKETS COUNT          BYTES COUNT      UPDATE
TIME
-------------     ------------     ------     ---------------     -------------     ---------------
RULE_1                    TEST                          9999                                  0
0      1970-01-01 00:00:00
DEFAULT_RULE      TEST                                  1                                0                          0
1970-01-01 00:00:00
```

```
admin@sonic:~$ show acl counters
RULE NAME        TABLE NAME        PRIO      PACKETS COUNT      BYTES COUNT    UPDATE TIME
------------   ------------   ------    ---------------    -----------   ---------------
RULE_1           CUSTOM            9999      84264487      10785890048    2023-03-21 09:44:57
DEFAULT_RULE    CUSTOM                1              0                    0    1970-01-01 00:00:00
RULE_1           TEST                 9999      84258128      10785075968    2023-03-21 09:44:57
DEFAULT_RULE    TEST                  1              0                    0    1970-01-01 00:00:00
admin@sonic:~$ sudo sonic-clear acl counters TEST
admin@sonic:~$ show acl counters
RULE NAME        TABLE NAME      PRIO    PACKETS COUNT      BYTES COUNT    UPDATE TIME
------------   ------------   ------   ---------------      -------------   ------------
RULE_1           CUSTOM          9999         85557677     10951382656    2023-03-21 09:45:07
DEFAULT_RULE    CUSTOM               1                0                    0    1970-01-01 00:00:00
RULE_1           TEST                9999                0                    0    1970-01-01 00:00:00
DEFAULT_RULE    TEST                  1                0                    0    1970-01-01 00:00:00
```

1.3 config acl log-update

Function

Run the **config acl log-update** command to control the log output interval by setting the interval for packets to match logs. View ACL logging in the syslog file.

Syntax

config acl log-update { **interval** *time* | **default** }

Parameter Description

interval *time*: Log output interval, in minutes. The default value 0 indicates that no log is output.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config acl add table TEST L3 -p Ethernet49 -s ingress
admin@sonic:~$ cat L3_ACL.json
{
    "acl": {
        "acl-sets": {
            "acl-set": {
                "TEST": {
                    "acl-entries": {
                        "acl-entry": {
                            "1": {
                                "actions": {
                                    "config": {
                                        "forwarding-action": "REJECT",
                                        "log-action": "LOG_SYSLOG"
                                    }
                                },
                                "config": {
                                    "sequence-id": 1
                                },
                                "ip": {
                                    "config": {
                                        "source-ip-address": "0.0.0.0/0",
                                        "destination-ip-address": "0.0.0.0/0"
                                    }
                                }
                            }
                        }
                    },
                    "config": {
                        "name": "TEST"
                    }
                }
            }
        }
    }
}
admin@sonic:~$ sudo config acl update incremental L3_ACL.json
```

```
admin@sonic:~$ sudo config acl log-update interval 1
admin@sonic:~$ show acl log-update interval
acl log-update interval 1

admin@sonic:~$ sudo config acl log-update interval 5
admin@sonic:~$ show acl log-update interval
acl log-update interval 5

admin@sonic:~$ sudo config acl log-update default
admin@sonic:~$ show acl log-update interval
acl log-update interval 0 (default)
```

1.4 config acl remove rule

Function

Run the **config acl remove rule** command to delete a rule from a table.

Syntax

sudo acl-loader delete *table_name rule_name*

Parameter Description

table-name: The name of the table to which the rule to be deleted belongs.

rule-name: The name of the rule to delete.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show acl rule
Table      Rule            Priority      Action      Match
-------   ------------   ----------   --------   ----------------------
TEST       RULE_1          9999          DROP     DST_IP: 0.0.0.0/0
                                                  LOG_ACTION: LOG_SYSLOG
                                                  SRC_IP: 0.0.0.0/0
TEST       RULE_2          9998          DROP    DST_IP: 0.0.0.0/0
                                                  LOG_ACTION: LOG_SYSLOG
                                                  SRC_IP: 0.0.0.1/32
TEST       DEFAULT_RULE   1             DROP     ETHER_TYPE: 2048
admin@sonic:~$ sudo acl-loader delete TEST RULE_1
admin@sonic:~$ show acl rule
Table      Rule            Priority      Action      Match
-------   ------------   ----------   --------   ----------------------
TEST       RULE_2          9998          DROP    DST_IP: 0.0.0.0/0
                                                  LOG_ACTION: LOG_SYSLOG
                                                  SRC_IP: 0.0.0.1/32
```

```
TEST        DEFAULT_RULE   1               DROP     ETHER_TYPE: 2048
```

1.5 config acl remove table

Function

Run the **config acl remove table** command to delete an ACL table.

Syntax

config acl remove table [*OPTIONS*] *table-name* [**-p** *ports*] [**-up**] [**-ud**]

Parameter Description

table-name: The name of the ACL table to delete.

- Physical ports will be bound as physical ports

ud: unset_dscp. Example Delete the configured QOS dscp parameters.

up: unset_policer. Delete the configured QOS policer parameters.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show acl table
Name      Type      Binding       Description      Stage      Dscp     CIR      CBS
------   ------   ----------   -------------   -------   ------   -----   -----
CUSTOM    L2        Ethernet1     CUSTOM             egress
TEST         L3        Ethernet49    TEST               ingress
admin@sonic:~$ sudo config acl remove table TEST
admin@sonic:~$ show acl table
Name      Type      Binding      Description      Stage      Dscp     CIR      CBS
------   ------   ---------   -------------   -------   ------   -----   -----
CUSTOM    L2        Ethernet1    CUSTOM             egress
```

```
admin@sonic:~$ show acl table
Name      Type      Binding      Description      Stage      Dscp     CIR      CBS
------   ------   ---------   -------------   -------   ------   -----   -----
TEST      L3_QOS    Ethernet1     TEST               ingress    30        1024     2048
admin@sonic:~$ sudo config acl remove table TEST -p Ethernet1
admin@sonic:~$ show acl table
Name      Type      Binding      Description      Stage      Dscp     CIR      CBS
------   ------   ---------   -------------   -------   ------   -----   -----
TEST      L3_QOS                 TEST                          30        1024     2048
```

```
admin@sonic:~$ show acl table
Name      Type      Binding      Description      Stage      Dscp     CIR      CBS
```

```
------  ------  ---------  -------------  -------  ------  -----  -----
TEST    L3_QOS  Ethernet1  TEST           ingress  30      1024   2048
admin@sonic:~$ sudo config acl remove table TEST -up -ud
admin@sonic:~$ show acl table
Name    Type    Binding    Description    Stage    Dscp    CIR    CBS
------  ------  ---------  -------------  -------  ------  -----  -----
TEST    L3_QOS  Ethernet1  TEST           ingress
```

1.6 config acl update full

Function

Run the **config acl update full** command to update the rules in all the tables or in one specific table in full.

If a table_name is provided, the operation will be restricted in the specified table. All existing rules in the specified table or all tables will be removed. New rules loaded from file will be installed. If the table_name is specified, only rules within that table will be removed and new rules in that table will be installed. If the table_name is not specified, all rules from all tables will be removed and only the rules present in the input file will be added.

The command does not modify anything in the list of acl tables. It modifies only the rules present in those pre-existing tables.

In order to create acl tables, either follow the config_db.json method or minigraph method to populate the list of ACL tables.

After creating tables, either the config_db.json method or the minigraph method or the CLI method (explained here) can be used to populate the rules in those ACL tables.

This command updates only the ACL rules and it does not disturb the ACL tables; i.e. the output of "show acl table" is not altered by using this command; only the output of "show acl rule" will be changed after this command.

When "--session_name" optional argument is specified, command sets the session_name for the ACL table with this mirror session name. It fails if the specified mirror session name does not exist.

When "--mirror_stage" optional argument is specified, command sets the mirror action to ingress/egress based on this parameter. By default command sets ingress mirror action in case argument is not specified.

When the optional argument "max_priority" is specified, each rule's priority is calculated by subtracting its "sequence_id" value from the "max_priority". If this value is not passed, the default "max_priority" 10000 is used.

Syntax

config acl update full [**--table_name** *table-name*] [**--session_name** *session_name*] [**--mirror_stage** { **ingress** | **egress** }] [**--max_priority** *priority-value*] *acl-json-file-name*

Parameter Description

table_name: Specifiy the name of the ACL table to load. Example: config acl update full "--table_name DT_ACL_T1 /etc/sonic/acl_table_1.json"

session_name: Specifiy the name of the ACL session to load. Example: config acl update full "--session_name mirror_ses1 /etc/sonic/acl_table_1.json"

priority_value: Specify the maximum priority to use when loading ACL rules. Example: config acl update full "--max-priority 100 /etc/sonic/acl_table_1.json"

Usage Guidelines

- All these optional parameters should be inside double quotes. If none of the options are provided, double quotes are not required for specifying filename alone.
- Any number of optional parameters can be configured in the same command.

Examples

```
admin@sonic:~$ sudo config acl update full /etc/sonic/acl_full_snmp_1_2_ssh_4.json
admin@sonic:~$ sudo config acl update full "--table_name SNMP-ACL
/etc/sonic/acl_full_snmp_1_2_ssh_4.json"
admin@sonic:~$ sudo config acl update full "--session_name everflow0
/etc/sonic/acl_full_snmp_1_2_ssh_4.json"00
```

1.7 config acl update incremental

Function

Run the **config acl update incremental** command to perform incremental update of ACL rule table. This command gets existing rules from Config DB and compares with rules specified in input file and performs corresponding modifications.

Syntax

config acl update incremental [**--session_name** *session_name*] [--**mirror_stage** { **ingress** | **egress** }] *acl_json_file_name*

Parameter Description

N/A

Usage Guidelines

When "--session_name" optional argument is specified, command sets the session_name for the ACL table with this mirror session name. It fails if the specified mirror session name does not exist.

When "--mirror_stage" optional argument is specified, command sets the mirror action to ingress/egress based on this parameter. By default command sets ingress mirror action in case argument is not specified.

Examples

```
admin@sonic:~$ sudo config acl update incremental acl_rule.json
```

L3 ACL json example:

```
{
    "acl": {
        "acl-sets": {
            "acl-set": {
                "TEST2": {
                    "acl-entries": {
                        "acl-entry": {
                            "1": {
                                "actions": {
                                    "config": {
                                        "forwarding-action": "ACCEPT",
                                        "log-action": "LOG_SYSLOG"
                                        }
                                },
                                "config": {
                                    "sequence-id": 1
                                },
                                "icmp": {
                                    "config": {
                                        "type": "1",
                                        "code": "1"
                                    }
                                },
                                "ip": {
                                    "config": {
                                        "protocol":"IP_ICMP",
                                        "source-ip-address": "172.20.3.1/32",
                                        "destination-ip-address":"172.20.2.0/24"
                                    }
                                }
                            },
                             "2": {
                                "actions": {
                                    "config": {
                                        "forwarding-action": "ACCEPT"
                                    }
                                },
                                "config": {
                                    "sequence-id": 2
                                },
```

```
                                    "ip": {
                                        "config": {
                                            "protocol": "IP_TCP",
                                            "source-ip-address": "1.1.1.1/32",
                                            "destination-ip-address": "2.2.2.2/32"
                                        }
                                    },
                                    "transport": {
                                        "config": {
                                            "source-port": "555",
                                            "destination-port": "2222",
                                            "tcp-flags": [
                                              "TCP_ACK",
                                              "TCP_SYN"
                                            ]
                                        }
                                    }
                                }
                            }
                        },
                        "config": {
                            "name": "TEST2"
                        }
                    }
                }
            }
        }
}
```

L3 ACL json example Parameters:

- acl_rule.json: Specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.
- forwarding-action(ACCEPT): If this option is set, it indicates that the rule belongs to the allowed class.
- forwarding-action(REJECT): If this option is configured, the keyword indicates that the rule is reject.
- forwarding-action(TRAP): If this option is configured, this rule matches packets and sends a copy to the CPU. At the same time, the forwarded packets are discarded.
- forwarding-action(COPY): If this option is configured, it indicates that the rule matches packets and sends a copy to the CPU. In addition, the packets forwarded are not affected.
- redirect-action(REDIRECT:target): If this option is configured, it indicates that the rule belongs to the redirection class.To use the ACL redirection function, change the

"forwarding-action" to "redirect-action".The redirection action must be configured in the "redirect-action:REDIRECT:target" format. The "target" indicates the redirected target in the following formats:

- ipaddress(ipv4)
- port/portchannel
- ipaddress@port/portchannel
- ipaddress@vrfname
- ipaddress1,ipaddress2...
- ipaddress1,ipaddress2@port/portchannel/vrfname,... (Next hop group)
- ipaddress1@port/portchannel/vrfname,ipaddress2@port/portchannel/vrfname,... (Next hop group)

- protocol: indicates the IP protocol number. The value ranges from 0 to 255. For convenience, the system provides short names of common IP protocol numbers to replace specific IP protocol numbers, including IP_TCP, IP_UDP, and IP_ICMP.
- source-ip-address: If this parameter is specified, the IP packets sent from a host or from hosts within a certain IP network segment are to be matched.
- source-port: indicates the source port number of the matched packets. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- destination-ip-address: If this option is configured, the packets destined for a specific host or hosts on a specific IP network segment are to be matched.
- destination-port: indicates the destination port of the matched packet. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- tcp-flags: indicates the TCP FLAG bit. It includes TCP_FIN, TCP_SYN, TCP_RST, TCP_PSH, TCP_ACK, and TCP_URG.
- log-action: If this option is configured, the matching log is periodically generated if packets are matched.

L3 ACL NOTE:

- L3 ACLs can be configured on access, aggregation, or core devices based on user distribution. L3 ACLs take effect only on the configured devices and will not affect other devices on the network.
- When a large number of ACEs (1000+) are configured on the M2-W6510-48GT4V, M2-W6510-32C, M2-W6510-48V8C, M2-W6910-64C, M2-W6920-4S, M2-W6920-32QC2X, M2-W6520-24DC8QC, and M2-W6930-64QC, the time for installing ACEs on interfaces will increase significantly.
- For the M2-W6920-4S, M2-W6920-32QC2X, and M2-W6930-64QC, up to 127 entries can be configured for the ACL of the same type in the egress direction. If the ACL is applied to multiple interfaces, the total number of entries must be less than 127. That is, the sum of the number of interfaces to which the same type of ACL is applied multiplied by the number of entries must be less than 127. For example, for two egress Layer 3 ACLs, table A and table B, the sum of the number of interfaces to which table A is applied multiplied by the number of entries in table A and the number of interfaces to which table B is applied multiplied by the number of entries in table B must be less than 127.
- For the M2-W6520-24QC8DC, the egress ACL does not support the “ether type” field.

- For the M2-W6930-64QC, if an ACL is applied to an interface and then applied to another, resources may be insufficient, and the system logs will be printed prompting FP resource insufficiency.
- When the COPY or TRAP action is configured for ACL, the traffic is sent to the CPU. If the traffic rate is too high, the CPU may be overloaded, resulting in CPU resource exhaustion. Therefore, when configuring an ACL, especially in high-traffic scenarios, exercise caution with the COPY and TRAP action and limit the traffic rate to prevent CPU overload.
- When the same type of ACL is applied to the same direction of the same interface or the same type of ACL is applied at both the global and interface levels, if traffic matches multiple ACL entries in the same direction with the same priority, the traffic behavior is uncertain. You are advised to set different priorities for different ACL entries based on the scenario.
- The ACL statistics counter in the egress direction does not count packets sent by the CPU. Instead, it only counts the packets on the forwarding plane.
- The ACL capacity displayed by the command does not match the actual capacity supported by the chip. Therefore, check the log to determine whether the chip ACL capacity is exceeded.
- ACL traffic statistics counter, interface-based IPv4/IPv6 traffic statistics counter, and VXLAN traffic statistics counter include the packets that are discarded.
- The egress ACL does not support the TRAP, COPY, or REDIRECT action.
- The egress ACL does not support range matching.
- For the M2-W6930-64QC, when an ACL is configured in community mode on one among the four breakout interfaces split from an interface, it also takes effect on the adjacent interface at the same time. For example, if interface Ethernet 1 is split into Ethernet 1, Ethernet 3, Ethernet 5, and Ethernet 7, and an ACL is applied to Ethernet 1, the ACL also takes effect on Ethernet 3.
- If you want to redirect traffic to a next-hop group through ACL redirection, the members of the next-hop group must be on the same VRF, otherwise the ACL will not be created successfully.
- When traffic is redirected to a next-hop group through ACL redirection, the members of the next-hop group in the form of an IP address belong to VRF 0 by default.
- The ACL resource counters in the "show acl resources group" command output are not accurate.

L3V6 ACL json example:

```
{
    "acl": {
        "acl-sets": {
            "acl-set": {
                "TEST2": {
                    "acl-entries": {
                        "acl-entry": {
                            "1": {
                                "actions": {
                                    "config": {
                                        "forwarding-action": "ACCEPT",
```

```
                    "log-action": "LOG_SYSLOG"
                }
            },
            "config": {
                "sequence-id": 1
            },
            "icmp": {
                "config": {
                    "type": "1",
                    "code": "1"
                }
            },
            "ip": {
                "config": {
                    "protocol":"IP_ICMP",
                    "source-ip-address": "201::2/128",
                    "destination-ip-address":"0::0/0"
                }
            }
        },
        "2": {
            "actions": {
                "config": {
                    "forwarding-action": "ACCEPT"
                }
            },
            "config": {
                "sequence-id": 2
            },
            "ip": {
                "config": {
                    "protocol": "IP_TCP",
                    "source-ip-address": "200::1/128",
                    "destination-ip-address": "0::/0"
                }
            },
            "transport": {
                "config": {
                    "source-port": "555",
                    "destination-port": "2222",
                    "tcp-flags": [
                      "TCP_ACK",
                      "TCP_SYN"
                    ]
                }
            }
```

```
                                }
                            }
                        },
                        "config": {
                            "name": "TEST2"
                        }
                    }
                }
            }
        }
    }
}
```

L3V6 ACL json example Parameters:

- acl_rule.json: Specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.
- forwarding-action(ACCEPT): If this option is set, it indicates that the rule belongs to the allowed class.
- forwarding-action(REJECT): If this option is configured, the keyword indicates that the rule is reject.
- forwarding-action(TRAP): If this option is configured, this rule matches packets and sends a copy to the CPU. At the same time, the forwarded packets are discarded.
- forwarding-action(COPY): If this option is configured, it indicates that the rule matches packets and sends a copy to the CPU. In addition, the packets forwarded are not affected.
- redirect-action(REDIRECT:target): If this option is configured, it indicates that the rule belongs to the redirection class.To use the ACL redirection function, change the "forwarding-action" to "redirect-action".The redirection action must be configured in the "redirect-action:REDIRECT:target" format. The "target" indicates the redirected target in the following formats:
  - ipaddress(ipv6)
  - port/portchannel
  - ipaddress@port/portchannel
  - ipaddress@vrfname
  - ipaddress1,ipaddress2...
  - ipaddress1,ipaddress2@port/portchannel/vrfname,... (Next hop group)
- ipaddress1@port/portchannel/vrfname,ipaddress2@port/portchannel/vrfname,... (Next hop group)protocol: indicates the IP protocol number. The value ranges from 0 to 255. For convenience, the system provides short names of common IP protocol numbers to replace specific IP protocol numbers, including IP_TCP, IP_UDP.
- source-ip-address: If this parameter is specified, the IPv6 packets sent from a host or from hosts within a certain IPv6 network segment are to be matched.

- source-port: indicates the source port number of the matched packets. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- destination-ip-address: If this option is configured, the IPv6 packets destined for a specific host or hosts on a specific IPv6 network segment are to be matched.
- destination-port: indicates the destination port of the matched packet. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- tcp-flags: indicates the TCP FLAG bit. It includes TCP_FIN, TCP_SYN, TCP_RST, TCP_PSH, TCP_ACK, and TCP_URG.
- log-action: If this option is configured, the matching log is periodically generated if packets are matched.

L3V6 ACL NOTE:

- L3v6 ACLs can be configured on access, aggregation, or core devices based on user distribution. L3v6 ACLs take effect only on the configured devices and will not affect other devices on the network.
- When a large number of ACEs (1000+) are configured on the M2-W6510-48GT4V, M2-W6510-32C, M2-W6510-48V8C, M2-W6910-64C, M2-W6920-4S, M2-W6920-32QC2X, M2-W6520-24DC8QC, and M2-W6930-64QC, the time for installing ACEs on interfaces will increase significantly.
- For the M2-W6920-4S, M2-W6920-32QC2X, and M2-W6930-64QC, up to 127 entries can be configured for the ACL of the same type in the egress direction. If the ACL is applied to multiple interfaces, the total number of entries must be less than 127. That is, the sum of the number of interfaces to which the same type of ACL is applied multiplied by the number of entries must be less than 127. For example, for two egress Layer 3 ACLs, table A and table B, the sum of the number of interfaces to which table A is applied multiplied by the number of entries in table A and the number of interfaces to which table B is applied multiplied by the number of entries in table B must be less than 127.
- For the M2-W6520-24QC8DC, the egress ACL does not support the “ether type” field.
- For the M2-W6930-64QC, if an ACL is applied to an interface and then applied to another, resources may be insufficient, and the system logs will be printed prompting FP resource insufficiency.
- When the COPY or TRAP action is configured for ACL, the traffic is sent to the CPU. If the traffic rate is too high, the CPU may be overloaded, resulting in CPU resource exhaustion. Therefore, when configuring an ACL, especially in high-traffic scenarios, exercise caution with the COPY and TRAP action and limit the traffic rate to prevent CPU overload.
- When the same type of ACL is applied to the same direction of the same interface or the same type of ACL is applied at both the global and interface levels, if traffic matches multiple ACL entries in the same direction with the same priority, the traffic behavior is uncertain. You are advised to set different priorities for different ACL entries based on the scenario.
- The ACL statistics counter in the egress direction does not count packets sent by the CPU. Instead, it only counts the packets on the forwarding plane.
- The ACL capacity displayed by the command does not match the actual capacity supported by the chip. Therefore, check the log to determine whether the chip ACL capacity is exceeded.
- ACL traffic statistics counter, interface-based IPv4/IPv6 traffic statistics counter, and

VXLAN traffic statistics counter include the packets that are discarded.

- The egress ACL does not support the TRAP, COPY, or REDIRECT action.
- The egress ACL does not support range matching.
- For the M2-W6930-64QC, when an ACL is configured in community mode on one among the four breakout interfaces split from an interface, it also takes effect on the adjacent interface at the same time. For example, if interface Ethernet 1 is split into Ethernet 1, Ethernet 3, Ethernet 5, and Ethernet 7, and an ACL is applied to Ethernet 1, the ACL also takes effect on Ethernet 3.
- If you want to redirect traffic to a next-hop group through ACL redirection, the members of the next-hop group must be on the same VRF, otherwise the ACL will not be created successfully.
- When traffic is redirected to a next-hop group through ACL redirection, the members of the next-hop group in the form of an IP address belong to VRF 0 by default.
- The ACL resource counters in the "show acl resources group" command output are not accurate.

CTRLPLANE ACL json example:

```
{
    "acl": {
        "acl-sets": {
            "acl-set": {
                "TEST4": {
                    "acl-entries": {
                        "acl-entry": {
                            "1": {
                                "actions": {
                                    "config": {
                                        "forwarding-action": "REJECT",
                                        "log-action": "LOG_SYSLOG"
                                    }
                                },
                                "config": {
                                    "sequence-id": 10
                                },
                                "ip": {
                                    "config": {
                                        "source-ip-address": "192.168.2.2/32"
                                    }
                                },
                                "transport": {
                                    "config": {
                                        "destination-port": "2222"
                                    }
                                }
                            }
                        }
```

```
                    },
                    "config": {
                        "name": "CUSTOM"
                    }
                }
            }
        }
    }
}
```

CTRLPLANE ACL json example Parameters:

- acl_rule.json: Specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.
- forwarding-action(ACCEPT): If this option is set, it indicates that the rule belongs to the allowed class.
- forwarding-action(REJECT): If this option is configured, the keyword indicates that the rule is reject.
- source-ip-address: If this parameter is specified, the IP packets sent by a host with the source IP address or the packets sent by hosts within a certain IP network segment match the IP packets sent by any host. The value can be an IPv4 or IPv6 address.
- destination-port: indicates the matched packet port number. This field does not need to be specified by default.
- tcp-flags: indicates the TCP FLAG bit. It includes TCP_FIN, TCP_SYN, TCP_RST, TCP_PSH, TCP_ACK, and TCP_URG.

CTRLPLANE ACL NOTE:

- CTRLPLANE ACLs can be configured on access, aggregation, or core devices based on user distribution. CTRLPLANE ACLs take effect only on the configured devices and will not affect other devices on the network.
- When no ACE is configured for a CTRLPLANE ACL, no iptables entry is generated by default. You need to configure ACEs first.
- After ACEs are configured for a CTRLPLANE ACL, an iptables entry denying all packets is generated in the ACL.
- Write the ACEs of a CTRLPLANE ACL to be added into a .json file, and then run the “sudo config acl update incremental acl_rule.json” command to configure the ACEs. To delete the ACEs from an ACL, run the “sudo acl-loader delete table-name rule-name” command.
- The CTRLPLANE ACL does not support statistics counter.

#L2 ACL json example:

```
{
    "acl": {
        "acl-sets": {
```

```
            "acl-set": {
                "CUSTOM": {
                    "acl-entries": {
                        "acl-entry": {
                            "1": {
                                "actions": {
                                    "config": {
                                        "forwarding-action": "ACCEPT",
                                        "log-action": "LOG_SYSLOG"
                                    }
                                },
                                "config": {
                                    "sequence-id": 10
                                },
                                "l2": {
                                    "config": {
                                        "ethertype": "2048",
                                        "destination-mac": "00:e0:f8:00:00:0c",
                                        "destination-mac-mask": "ff:ff:ff:ff:ff:ff"
                                    }
                                }
                            }
                        }
                    },
                    "config": {
                        "name": "CUSTOM"
                    }
                }
            }
        }
    }
}
```

L2 ACL json example Parameters:

- acl_rule.json: Specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.
- forwarding-action(ACCEPT): If this option is set, it indicates that the rule belongs to the allowed class.
- forwarding-action(REJECT): If this option is configured, the keyword indicates that the rule is reject.
- forwarding-action(TRAP): If this option is configured, this rule matches packets and sends a copy to the CPU. At the same time, the forwarded packets are discarded.
- forwarding-action(COPY): If this option is configured, it indicates that the rule matches

packets and sends a copy to the CPU. In addition, the packets forwarded are not affected.

- redirect-action(REDIRECT:target): If this option is configured, it indicates that the rule belongs to the redirection class.To use the ACL redirection function, change the "forwarding-action" to "redirect-action".The redirection action must be configured in the "redirect-action:REDIRECT:target" format. The "target" indicates the redirected target in the following formats:
  - ipaddress(ipv4)
  - port/portchannel
  - ipaddress@port/portchannel
  - ipaddress@vrfname
  - ipaddress1,ipaddress2...
  - ipaddress1,ipaddress2@port/portchannel/vrfname,... (Next hop group)
- ether type: If configured, Layer 2 packets of the specified Ethernet type must be matched.
- source-mac: If this option is configured, it matches Layer 2 packets sent by a host with the source MAC address or packets sent by hosts within a certain MAC address segment.
- destination-mac: indicates that Layer 2 packets whose destination mac address is a host or packets whose destination MAC address is a host on a specific MAC address segment are to be matched.
- log-action: If this option is configured, the matching log is periodically generated if packets are matched.

L2 ACL NOTE:

L2 ACLs can be configured on access, aggregation, or core devices based on user distribution. L2 ACLs take effect only on the configured devices and will not affect other devices on the network.

When a large number of ACEs (1000+) are configured for the M2-W6510-48GT4V, M2-W6510-32C, M2-W6510-48V8C, M2-W6910-64C, M2-W6920-4S, M2-W6920-32QC2X, M2-W6520-24DC8QC, and M2-W6930-64QC, the time for installing ACEs on interfaces will increase significantly.

For the M2-W6920-4S, M2-W6920-32QC2X, and M2-W6930-64QC, up to 127 entries can be configured for the ACL of the same type in the egress direction. If the ACL is applied to multiple interfaces, the total number of entries must be less than 127. That is, the sum of the number of interfaces to which the same type of ACL is applied multiplied by the number of entries must be less than 127. For example, for two egress Layer 3 ACLs, table A and table B, the sum of the number of interfaces to which table A is applied multiplied by the number of entries in table A and the number of interfaces to which table B is applied multiplied by the number of entries in table B must be less than 127.

For the M2-W6520-24QC8DC, the egress ACL does not support the “ether type” field.

For the M2-W6930-64QC, if an ACL is applied to an interface and then applied to another, resources may be insufficient, and the system logs will be printed prompting FP resource insufficiency.

When the COPY or TRAP action is configured for ACL, the traffic is sent to the CPU. If the traffic rate is too high, the CPU may be overloaded, resulting in CPU resource exhaustion.

Therefore, when configuring an ACL, especially in high-traffic scenarios, exercise caution with the COPY and TRAP action and limit the traffic rate to prevent CPU overload.

When the same type of ACL is applied to the same direction of the same interface or the same type of ACL is applied at both the global and interface levels, if traffic matches multiple ACL entries in the same direction with the same priority, the traffic behavior is uncertain. You are advised to set different priorities for different ACL entries based on the scenario.

The ACL statistics counter in the egress direction does not count packets sent by the CPU. Instead, it only counts the packets on the forwarding plane.

The ACL capacity displayed by the command does not match the actual capacity supported by the chip. Therefore, check the log to determine whether the chip ACL capacity is exceeded.

ACL traffic statistics counter, interface-based IPv4/IPv6 traffic statistics counter, and VXLAN traffic statistics counter include the packets that are discarded.

The egress ACL does not support the TRAP, COPY, or REDIRECT action.

The egress ACL does not support range matching.

For the M2-W6930-64QC, when an ACL is configured in community mode on one among the four breakout interfaces split from an interface, it also takes effect on the adjacent interface at the same time. For example, if interface Ethernet 1 is split into Ethernet 1, Ethernet 3, Ethernet 5, and Ethernet 7, and an ACL is applied to Ethernet 1, the ACL also takes effect on Ethernet 3.

If you want to redirect traffic to a next-hop group through ACL redirection, the members of the next-hop group must be on the same VRF, otherwise the ACL will not be created successfully.

When traffic is redirected to a next-hop group through ACL redirection, the members of the next-hop group in the form of an IP address belong to VRF 0 by default.

The ACL resource counters in the “show acl resources group” command output are not accurate.

L3_QOS ACL json example:

```
{
        "acl": {
                "acl-sets": {
                        "acl-set": {
                                "TEST2": {
                                        "acl-entries": {
                                                "acl-entry": {
                                                        "1": {
                                                                "actions": {
                                                                        "config": {
                                                                                "policer-action":
"policer_test",
                                                                                "dscp-action": "10",
```

```
                                                "log-action":
"LOG_SYSLOG"
                                        }
                                },
                                "config": {
                                        "sequence-id": 1
                                },
                                "icmp": {
                                        "config": {
                                                "type": "1",
                                                "code": "1"
                                        }
                                },
                                "ip": {
                                        "config": {
                                                "protocol":"IP_ICMP",
                                                "source-ip-address":
"172.20.3.1/32",
                                                "destination-ip-
address":"172.20.2.0/24"
                                        }
                                }
                        },
                        "2": {
                                "actions": {
                                        "config": {
                                                "forwarding-action":
"ACCEPT"
                                        }
                                },
                                "config": {
                                        "sequence-id": 2
                                },
                                "ip": {
                                        "config": {
                                                "protocol": "IP_TCP",
                                                "source-ip-address":
"1.1.1.1/32",
                                                "destination-ip-
address": "2.2.2.2/32"
                                        }
                                },
                                "transport": {
                                        "config": {
                                                "source-port": "555",
```

```
                                                                "destination-port":
"2222",
                                                                "tcp-flags": [
                                                                    "TCP_ACK",
                                                                    "TCP_SYN"
                                                                ]
                                                            }
                                                        }
                                                    }
                                                }
                                            },
                                            "config": {
                                                "name": "TEST2"
                                            }
                                        }
                                    }
                                }
                            }
                        }
}
```

L3_QOS ACL json example Parameters:

- acl_rule.json: Specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.
- policer-action: If this option is configured, the policer action will be performed on the packet after the rule matches the packet. After setting the policer-acltion action, enter the name of the policer template that you want to configure.
- dscp-action: If this option is configured, the dscp priority of the packet is re-marked after the rule matches the packet. After DSCp-action is set, the value of dscp re-marking ranges from 0 to 63.
- forwarding-action(ACCEPT): If this option is set, it indicates that the rule belongs to the allowed class.
- forwarding-action(REJECT): If this option is configured, the keyword indicates that the rule is reject.
- protocol: indicates the IP protocol number. The value ranges from 0 to 255. For convenience, the system provides short names of common IP protocol numbers to replace specific IP protocol numbers, including IP_TCP, IP_UDP, and IP_ICMP.
- sourece-ip-address: If this parameter is specified, the IP packets sent from a host or from hosts within a certain IP network segment are to be matched.
- source-port: indicates the source port number of the matched packets. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- destination-ip-address: If this option is configured, the packets destined for a specific host or hosts on a specific IP network segment are to be matched.

- destination-port: indicates the destination port of the matched packet. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- tcp-flags: indicates the TCP FLAG bit. It includes TCP_FIN, TCP_SYN, TCP_RST, TCP_PSH, TCP_ACK, and TCP_URG.
- log-action: If this option is configured, the matching log is periodically generated if packets are matched.

L3_QOS ACL NOTE:

- L3_QoS ACLs can be configured on access, aggregation, or core devices based on user distribution. L3_QoS ACLs take effect only on the configured devices and will not affect other devices on the network.
- When a large number of ACEs (1000+) are configured for the M2-W6510-48GT4V, M2-W6510-32C, M2-W6510-48V8C, M2-W6910-64C, M2-W6920-4S, M2-W6920-32QC2X, M2-W6520-24DC8QC, and M2-W6930-64QC, the time for installing ACEs on interfaces will increase significantly.
- For the M2-W6920-4S, M2-W6920-32QC2X, and M2-W6930-64QC, up to 127 entries can be configured for the ACL of the same type in the egress direction. If the ACL is applied to multiple interfaces, the total number of entries must be less than 127. That is, the sum of the number of interfaces to which the same type of ACL is applied multiplied by the number of entries must be less than 127. For example, for two egress Layer 3 ACLs, table A and table B, the sum of the number of interfaces to which table A is applied multiplied by the number of entries in table A and the number of interfaces to which table B is applied multiplied by the number of entries in table B must be less than 127.
- The M2-W6920-4S, M2-W6920-32QC2X, and M2-W6930-64QC do not support egress QoS ACL.
- For the M2-W6520-24QC8DC, the egress ACL does not support the “ether type” field.
- For the M2-W6930-64QC, if an ACL is applied to an interface and then applied to another, resources may be insufficient, and the system logs will be printed prompting FP resource insufficiency.
- When the same type of ACL is applied to the same direction of the same interface or the same type of ACL is applied at both the global and interface levels, if traffic matches multiple ACL entries in the same direction with the same priority, the traffic behavior is uncertain. You are advised to set different priorities for different ACL entries based on the scenario.
- The ACL statistics counter in the egress direction does not count packets sent by the CPU. Instead, it only counts the packets on the forwarding plane.
- The ACL capacity displayed by the command does not match the actual capacity supported by the chip. Therefore, check the log to determine whether the chip ACL capacity is exceeded.
- ACL traffic statistics counter, interface-based IPv4/IPv6 traffic statistics counter, and VXLAN traffic statistics counter include the packets that are discarded.
- The egress ACL does not support range matching.
- For the M2-W6930-64QC, when an ACL is configured in community mode on one among the four breakout interfaces split from an interface, it also takes effect on the adjacent interface at the same time. For example, if interface Ethernet 1 is split into Ethernet 1, Ethernet 3, Ethernet 5, and Ethernet 7, and an ACL is applied to Ethernet 1, the ACL also takes effect on Ethernet 3.

- The ACL resource counters in the “show acl resources group” command output are not accurate.

L3V6_QOS ACL json example:

```
{
        "acl": {
                "acl-sets": {
                        "acl-set": {
                                "TEST2": {
                                        "acl-entries": {
                                                "acl-entry": {
                                                        "1": {
                                                                "actions": {
                                                                        "config": {
                                                                                "policer-action":
"policer_test",
                                                                                "dscp-action": "7",
                                                                                "log-action":
"LOG_SYSLOG"
                                                                        }
                                                                },
                                                                "config": {
                                                                        "sequence-id": 1
                                                                },
                                                                "icmp": {
                                                                        "config": {
                                                                                "type": "1",
                                                                                "code": "1"
                                                                        }
                                                                },
                                                                "ip": {
                                                                        "config": {
                                                                                "protocol":"IP_ICMP",
                                                                                "source-ip-address":
"201::2/128",
                                                                                "destination-ip-
address":"0::/0"
                                                                        }
                                                                }
                                                        },
                                                        "2": {
                                                                "actions": {
                                                                        "config": {
                                                                                "forwarding-action":
"ACCEPT"
```

```
                                                        }
                                                },
                                                "config": {
                                                        "sequence-id": 2
                                                },
                                                "ip": {
                                                        "config": {
                                                                "protocol": "IP_TCP",
                                                                "source-ip-address":
"200::1/128",
                                                                "destination-ip-
address": "0::/0"
                                                        }
                                                },
                                                "transport": {
                                                        "config": {
                                                                "source-port": "555",
                                                                "destination-port":
"2222",
                                                                "tcp-flags": [
                                                                    "TCP_ACK",
                                                                    "TCP_SYN"
                                                                ]
                                                        }
                                                }
                                        }
                                }
                        },
                        "config": {
                                "name": "TEST2"
                        }
                }
        }
}
```

L3V6_QOS ACL json example Parameters:

- acl_rule.json: Specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.
- policer-action: If this option is configured, the policer action will be performed on the packet after the rule matches the packet. After setting the policer-acltion action, enter the name of the policer template that you want to configure.

- dscp-action: If this option is configured, the dscp priority of the packet is re-marked after the rule matches the packet. After DSCp-action is set, the value of dscp re-marking ranges from 0 to 63.
- forwarding-action(ACCEPT): If this option is set, it indicates that the rule belongs to the allowed class.
- forwarding-action(REJECT): If this option is configured, the keyword indicates that the rule is reject.
- protocol: indicates the IP protocol number. The value ranges from 0 to 255. For convenience, the system provides short names of common IP protocol numbers to replace specific IP protocol numbers, including IP_TCP, IP_UDP.
- source-ip-address: If this parameter is specified, the IPv6 packets sent from a host or from hosts within a certain IPv6 network segment are to be matched.
- source-port: indicates the source port number of the matched packets. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- destination-ip-address: If this option is configured, the IPv6 packets destined for a specific host or hosts on a specific IPv6 network segment are to be matched.
- destination-port: indicates the destination port of the matched packet. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- tcp-flags: indicates the TCP FLAG bit. It includes TCP_FIN, TCP_SYN, TCP_RST, TCP_PSH, TCP_ACK, and TCP_URG.
- log-action: If this option is configured, the matching log is periodically generated if packets are matched.

L3V6_QOS ACL NOTE:

- L3v6_QoS ACLs can be configured on access, aggregation, or core devices based on user distribution. L3v6_QoS ACLs take effect only on the configured devices and will not affect other devices on the network.
- When a large number of ACEs (1000+) are configured for the M2-W6510-48GT4V, M2-W6510-32C, M2-W6510-48V8C, M2-W6910-64C, M2-W6920-4S, M2-W6920-32QC2X, M2-W6520-24DC8QC, and M2-W6930-64QC, the time for installing ACEs on interfaces will increase significantly.
- For the M2-W6920-4S, M2-W6920-32QC2X, and M2-W6930-64QC, up to 127 entries can be configured for the ACL of the same type in the egress direction. If the ACL is applied to multiple interfaces, the total number of entries must be less than 127. That is, the sum of the number of interfaces to which the same type of ACL is applied multiplied by the number of entries must be less than 127. For example, for two egress Layer 3 ACLs, table A and table B, the sum of the number of interfaces to which table A is applied multiplied by the number of entries in table A and the number of interfaces to which table B is applied multiplied by the number of entries in table B must be less than 127.
- The M2-W6920-4S, M2-W6920-32QC2X, and M2-W6930-64QC do not support egress QoS ACL.
- For the M2-W6520-24QC8DC, the egress ACL does not support the “ether type” field.
- For the M2-W6930-64QC, if an ACL is applied to an interface and then applied to another, resources may be insufficient, and the system logs will be printed prompting FP resource insufficiency.

- When the same type of ACL is applied to the same direction of the same interface or the same type of ACL is applied at both the global and interface levels, if traffic matches multiple ACL entries in the same direction with the same priority, the traffic behavior is uncertain. You are advised to set different priorities for different ACL entries based on the scenario.
- The ACL statistics counter in the egress direction does not count packets sent by the CPU. Instead, it only counts the packets on the forwarding plane.
- The ACL capacity displayed by the command does not match the actual capacity supported by the chip. Therefore, check the log to determine whether the chip ACL capacity is exceeded.
- ACL traffic statistics counter, interface-based IPv4/IPv6 traffic statistics counter, and VXLAN traffic statistics counter include the packets that are discarded.
- The egress ACL does not support range matching.
- For the M2-W6930-64QC, when an ACL is configured in community mode on one among the four breakout interfaces split from an interface, it also takes effect on the adjacent interface at the same time. For example, if interface Ethernet 1 is split into Ethernet 1, Ethernet 3, Ethernet 5, and Ethernet 7, and an ACL is applied to Ethernet 1, the ACL also takes effect on Ethernet 3.
- The ACL resource counters in the “show acl resources group” command output are not accurate.

L2_QOS ACL json example:

```
{
        "acl": {
                "acl-sets": {
                        "acl-set": {
                                "CUSTOM": {
                                        "acl-entries": {
                                                "acl-entry": {
                                                        "1": {
                                                                "actions": {
                                                                        "config": {
                                                                                "policer-action":
"policer_test",
                                                                                "dscp-action": "10",
                                                                                "log-action":
"LOG_SYSLOG"
                                                                        }
                                                                },
                                                                "config": {
                                                                        "sequence-id": 10
                                                                },
                                                                "l2": {
                                                                        "config": {
                                                                                "ethertype": "2048",
```

```
                                                                    "destination-mac":
"00:e0:f8:00:00:0c",
                                                                    "destination-mac-
mask": "ff:ff:ff:ff:ff:ff"
                                                                }
                                                            }
                                                        }
                                                    }
                                                },
                                                "config": {
                                                    "name": "CUSTOM"
                                                }
                                            }
                                        }
                                    }
                                }
                            }
}
```

L2_QOS ACL json example Parameters:

- acl_rule.json: Specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.
- policer-action: If this option is configured, the policer action will be performed on the packet after the rule matches the packet. After setting the policer-acltion action, enter the name of the policer template that you want to configure.
- dscp-action: If this option is configured, the dscp priority of the packet is re-marked after the rule matches the packet. After DSCp-action is set, the value of dscp re-marking ranges from 0 to 63.
- forwarding-action(ACCEPT): If this option is set, it indicates that the rule belongs to the allowed class.
- forwarding-action(REJECT): If this option is configured, the keyword indicates that the rule is reject.
- ether type: If configured, Layer 2 packets of the specified Ethernet type must be matched.
- source-mac: If this option is configured, it matches Layer 2 packets sent by a host with the source MAC address or packets sent by hosts within a certain MAC address segment.
- destination-mac: indicates that Layer 2 packets whose destination mac address is a host or packets whose destination MAC address is a host on a specific MAC address segment are to be matched.
- log-action: If this option is configured, the matching log is periodically generated if packets are matched.

L2_QOS ACL NOTE:

- L2_QoS ACLs can be configured on access, aggregation, or core devices based on user distribution. L2_QoS ACLs take effect only on the configured devices and will not affect

other devices on the network.

- When a large number of ACEs (1000+) are configured for the M2-W6510-48GT4V, M2-W6510-32C, M2-W6510-48V8C, M2-W6910-64C, M2-W6920-4S, M2-W6920-32QC2X, M2-W6520-24DC8QC, and M2-W6930-64QC, the time for installing ACEs on interfaces will increase significantly.
- For the M2-W6920-4S, M2-W6920-32QC2X, and M2-W6930-64QC, up to 127 entries can be configured for the ACL of the same type in the egress direction. If the ACL is applied to multiple interfaces, the total number of entries must be less than 127. That is, the sum of the number of interfaces to which the same type of ACL is applied multiplied by the number of entries must be less than 127. For example, for two egress Layer 3 ACLs, table A and table B, the sum of the number of interfaces to which table A is applied multiplied by the number of entries in table A and the number of interfaces to which table B is applied multiplied by the number of entries in table B must be less than 127.
- The M2-W6920-4S, M2-W6920-32QC2X, and M2-W6930-64QC do not support egress QoS ACL.
- For the M2-W6520-24QC8DC, the egress ACL does not support the “ether type” field.
- For the M2-W6930-64QC, if an ACL is applied to an interface and then applied to another, resources may be insufficient, and the system logs will be printed prompting FP resource insufficiency.
- When the same type of ACL is applied to the same direction of the same interface or the same type of ACL is applied at both the global and interface levels, if traffic matches multiple ACL entries in the same direction with the same priority, the traffic behavior is uncertain. You are advised to set different priorities for different ACL entries based on the scenario.
- The ACL statistics counter in the egress direction does not count packets sent by the CPU. Instead, it only counts the packets on the forwarding plane.
- The ACL capacity displayed by the command does not match the actual capacity supported by the chip. Therefore, check the log to determine whether the chip ACL capacity is exceeded.
- ACL traffic statistics counter, interface-based IPv4/IPv6 traffic statistics counter, and VXLAN traffic statistics counter include the packets that are discarded.
- The egress ACL does not support range matching.
- For the M2-W6930-64QC, when an ACL is configured in community mode on one among the four breakout interfaces split from an interface, it also takes effect on the adjacent interface at the same time. For example, if interface Ethernet 1 is split into Ethernet 1, Ethernet 3, Ethernet 5, and Ethernet 7, and an ACL is applied to Ethernet 1, the ACL also takes effect on Ethernet 3.
- The ACL resource counters in the “show acl resources group” command output are not accurate.

MIRROR ACL json example:

```
{
    "acl": {
        "acl-sets": {
```

```
"acl-set": {
    "TEST2": {
        "acl-entries": {
            "acl-entry": {
                "1": {
                    "actions": {
                        "config": {
                            "forwarding-action": "ACCEPT",
                            "log-action": "LOG_SYSLOG"
                        }
                    },
                    "config": {
                        "sequence-id": 1
                    },
                    "icmp": {
                        "config": {
                            "type": "1",
                            "code": "1"
                        }
                    },
                    "ip": {
                        "config": {
                            "protocol":"IP_ICMP",
                            "source-ip-address": "172.20.3.1/32",
                            "destination-ip-address":"172.20.2.0/24"
                        }
                    }
                },
                "2": {
                    "actions": {
                        "config": {
                            "forwarding-action": "ACCEPT"
                        }
                    },
                    "config": {
                        "sequence-id": 2
                    },
                    "icmp": {
                        "config": {
                            "type": "1",
                            "code": "1"
                        }
                    },
                    "ip": {
                        "config": {
                            "protocol": "IP_TCP",
```

```
                                    "source-ip-address": "1.1.1.1/32",
                                    "destination-ip-address": "2.2.2.2/32"
                                }
                            },
                            "transport": {
                                "config": {
                                    "source-port": "555",
                                    "destination-port": "2222",
                                    "tcp-flags": [
                                      "TCP_ACK",
                                      "TCP_SYN"
                                    ]
                                }
                            }
                        }
                    }
                },
                "config": {
                    "name": "TEST2"
                }
            }
        }
    }
}
```

MIRROR ACL json example Parameters:

- acl_rule.json: specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.
- forwarding-action(ACCEPT) : If this option is configured, it indicates that the rule belongs to the allowed class. After this field is set to ACCEPT, the ACL RULE action of the MIRROR type in the ingress direction is converted to MIRROR_INGRESS_ACTION, indicating the traffic of the mirror ingress direction.
- protocol: indicates the IP protocol number. The value ranges from 0 to 255. For convenience, the system provides short names of common IP protocol numbers to replace specific IP protocol numbers, including IP_TCP, IP_UDP, and IP_ICMP.
- source-ip-address: If this parameter is specified, the IP packets sent from a host or from hosts within a certain IP network segment are to be matched.
- source-port: indicates the source port number of the matched packets. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- destination-ip-address: If this option is configured, the packets destined for a specific host or hosts on a specific IP network segment are to be matched.

- destination-port: indicates the destination port of the matched packet. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- tcp-flags: indicates the TCP FLAG bit. It includes TCP_FIN, TCP_SYN, TCP_RST, TCP_PSH, TCP_ACK, and TCP_URG.
- log-action: If this option is configured, the matching log is periodically generated if packets are matched.

MIRROR ACL NOTE:

- MIRROR ACL configuration depends on MIRROR configuration. MIRROR ACLs can be configured on access, aggregation, or core devices based on user distribution. MIRROR ACLs take effect only on the configured devices and will not affect other devices on the network.
- When a large number of ACEs (1000+) are configured for the M2-W6510-48GT4V, M2-W6510-32C, M2-W6510-48V8C, M2-W6910-64C, M2-W6920-4S, M2-W6920-32QC2X, M2-W6520-24DC8QC, and M2-W6930-64QC, the time for installing ACEs on interfaces will increase significantly.
- For the M2-W6920-4S, M2-W6920-32QC2X, and M2-W6930-64QC, up to 127 entries can be configured for the ACL of the same type in the egress direction. If the ACL is applied to multiple interfaces, the total number of entries must be less than 127. That is, the sum of the number of interfaces to which the same type of ACL is applied multiplied by the number of entries must be less than 127. For example, for two egress Layer 3 ACLs, table A and table B, the sum of the number of interfaces to which table A is applied multiplied by the number of entries in table A and the number of interfaces to which table B is applied multiplied by the number of entries in table B must be less than 127.
- For the M2-W6520-24QC8DC, the egress ACL does not support the “ether type” field.
- For the M2-W6930-64QC, if an ACL is applied to an interface and then applied to another, resources may be insufficient, and the system logs will be printed prompting FP resource insufficiency.
- When the same type of ACL is applied to the same direction of the same interface or the same type of ACL is applied at both the global and interface levels, if traffic matches multiple ACL entries in the same direction with the same priority, the traffic behavior is uncertain. You are advised to set different priorities for different ACL entries based on the scenario.
- The ACL statistics counter in the egress direction does not count packets sent by the CPU. Instead, it only counts the packets on the forwarding plane.
- The ACL capacity displayed by the command does not match the actual capacity supported by the chip. Therefore, check the log to determine whether the chip ACL capacity is exceeded.
- ACL traffic statistics counter, interface-based IPv4/IPv6 traffic statistics counter, and VXLAN traffic statistics counter include the packets that are discarded.
- The egress ACL does not support range matching.
- For the M2-W6930-64QC, when an ACL is configured in community mode on one among the four breakout interfaces split from an interface, it also takes effect on the adjacent interface at the same time. For example, if interface Ethernet 1 is split into Ethernet 1, Ethernet 3, Ethernet 5, and Ethernet 7, and an ACL is applied to Ethernet 1, the ACL also takes effect on Ethernet 3.
- The ACL resource counters in the “show acl resources group” command output are not

accurate.

MIRRORV6 ACL json example:

```
{
        "acl": {
                "acl-sets": {
                        "acl-set": {
                                "TEST2": {
                                        "acl-entries": {
                                                "acl-entry": {
                                                        "1": {
                                                                "actions": {
                                                                        "config": {
                                                                                "forwarding-action":
"ACCEPT",
                                                                                "log-action":
"LOG_SYSLOG"
                                                                        }
                                                                },
                                                                "config": {
                                                                        "sequence-id": 1
                                                                },
                                                                "icmp": {
                                                                        "config": {
                                                                                "type": "1",
                                                                                "code": "1"
                                                                        }
                                                                },
                                                                "ip": {
                                                                        "config": {
                                                                                "protocol":"IP_ICMP",
                                                                                "source-ip-address":
"201::2/128",
                                                                                "destination-ip-
address":"0::0/0"
                                                                        }
                                                                }
                                                        },
                                                        "2": {
                                                                "actions": {
                                                                        "config": {
                                                                                "forwarding-action":
"ACCEPT"
                                                                        }
                                                                },
                                                                "config": {
```

```
                                                        "sequence-id": 2
                                                },
                                                "icmp": {
                                                        "config": {
                                                                "type": "1",
                                                                "code": "1"
                                                        }
                                                },
                                                "ip": {
                                                        "config": {
                                                                "protocol": "IP_TCP",
                                                                "source-ip-address":
"200::1/128",
                                                                "destination-ip-
address": "0::/0"
                                                        }
                                                },
                                                "transport": {
                                                        "config": {
                                                                "source-port": "555",
                                                                "destination-port":
"2222",
                                                                "tcp-flags": [
                                                                    "TCP_ACK",
                                                                    "TCP_SYN"
                                                                ]
                                                        }
                                                }
                                        }
                                }
                        },
                        "config": {
                                "name": "TEST2"
                        }
                }
        }
}
```

MIRRORV6 ACL json example Parameters:

- acl_rule.json: specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.

- forwarding-action(ACCEPT) : If this option is configured, it indicates that the rule belongs to the allowed class. After this field is set to ACCEPT, the ACL RULE action of the MIRROR type in the ingress direction is converted to MIRROR_INGRESS_ACTION, indicating the traffic of the mirror ingress direction.
- protocol: indicates the IP protocol number. The value ranges from 0 to 255. For convenience, the system provides short names of common IP protocol numbers to replace specific IP protocol numbers, including IP_TCP, IP_UDP, and IP_ICMP.
- source-ip-address: If this parameter is specified, the IP packets sent from a host or from hosts within a certain IP network segment are to be matched.
- source-port: indicates the source port number of the matched packets. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- destination-ip-address: If this option is configured, the packets destined for a specific host or hosts on a specific IP network segment are to be matched.
- destination-port: indicates the destination port of the matched packet. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- tcp-flags: indicates the TCP FLAG bit. It includes TCP_FIN, TCP_SYN, TCP_RST, TCP_PSH, TCP_ACK, and TCP_URG.
- log-action: If this option is configured, the matching log is periodically generated if packets are matched.

MIRRORV6 ACL NOTE

- MIRRORv6 ACL configuration depends on MIRRORv6 configuration. MIRRORv6 ACLs can be configured on access, aggregation, or core devices based on user distribution. MIRRORv6 ACLs take effect only on the configured devices and will not affect other devices on the network.
- When a large number of ACEs (1000+) are configured for the M2-W6510-48GT4V, M2-W6510-32C, M2-W6510-48V8C, M2-W6910-64C, M2-W6920-4S, M2-W6920-32QC2X, M2-W6520-24DC8QC, and M2-W6930-64QC, the time for installing ACEs on interfaces will increase significantly.
- For the M2-W6920-4S, M2-W6920-32QC2X, and M2-W6930-64QC, up to 127 entries can be configured for the ACL of the same type in the egress direction. If the ACL is applied to multiple interfaces, the total number of entries must be less than 127. That is, the sum of the number of interfaces to which the same type of ACL is applied multiplied by the number of entries must be less than 127. For example, for two egress Layer 3 ACLs, table A and table B, the sum of the number of interfaces to which table A is applied multiplied by the number of entries in table A and the number of interfaces to which table B is applied multiplied by the number of entries in table B must be less than 127.
- For the M2-W6520-24QC8DC, the egress ACL does not support the “ether type” field.
- For the M2-W6930-64QC, if an ACL is applied to an interface and then applied to another, resources may be insufficient, and the system logs will be printed prompting FP resource insufficiency.
- When the same type of ACL is applied to the same direction of the same interface or the same type of ACL is applied at both the global and interface levels, if traffic matches multiple ACL entries in the same direction with the same priority, the traffic behavior is uncertain. You are advised to set different priorities for different ACL entries based on the scenario.

- The ACL statistics counter in the egress direction does not count packets sent by the CPU. Instead, it only counts the packets on the forwarding plane.
- The ACL capacity displayed by the command does not match the actual capacity supported by the chip. Therefore, check the log to determine whether the chip ACL capacity is exceeded.
- ACL traffic statistics counter, interface-based IPv4/IPv6 traffic statistics counter, and VXLAN traffic statistics counter include the packets that are discarded.
- The egress ACL does not support range matching.
- For the M2-W6930-64QC, when an ACL is configured in community mode on one among the four breakout interfaces split from an interface, it also takes effect on the adjacent interface at the same time. For example, if interface Ethernet 1 is split into Ethernet 1, Ethernet 3, Ethernet 5, and Ethernet 7, and an ACL is applied to Ethernet 1, the ACL also takes effect on Ethernet 3.
- The ACL resource counters in the “show acl resources group” command output are not accurate.

1.8 config policer

Function

Run the **config policer** command to configure a policer template for an ACL.

Syntax

config policer add policer_name [**-mode** [**sr_tcm** | **tr_tcm** | **storm**]] [-**meter_type** [**packets** | **bytes**]] [**-color** [**blind** | **aware**]] [**-cir** *cir_value*] [**-cbs** *cbs_value*] [**-pir** *pir_value*] [**-pbs** *pbs_value*] [**-green_action** [**forward** | **drop**]] [**-yellow_action** [**forward** | **drop**]] [**-red_action** [**forward** | **drop**]]

Parameter Description

policer_name: Indicates the name of the policer template.

mode: Policer's modes, including sr_tcm (single-rate three-color markers, green, yellow, and red), tr_tcm (dual-rate three-color markers, green, yellow, and red), and storm (single-rate two-color markers, green, and red).

meter_type: Includes packets (based on data packets) and bytes (based on bytes).

color: Includes blind (color-blind mode, the policy coloring scheme before the message is ignored) and aware (non-color-blind mode, the policy coloring scheme before the message is not ignored).

cir: Committed information rate.

cbs: Committed burst size.

pir: Peak information rate.

pbs: Peak burst size.

green_action: Indicates the green packet action, including forward (permit) and drop (drop).

yellow_action: Indicates the yellow packet action, including forward (allowed) and drop (dropped).

red_action: Indicates the red packet action, including forward (permit) and drop (drop).

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config policer add policer_test -mode tr_tcm -meter_type bytes -color blind -cir 100000000 -cbs 1000 -pir 200000000 -pbs 2000 -green_action forward -yellow_action forward -red_action forward
```

```
admin@sonic:~$ show acl counters CUSTOM
RULE NAME     TABLE NAME       PRIO      PACKETS COUNT     BYTES COUNT    UPDATE TIME
----------  ------------  -------  -------------  ------------  --------------
RULE_1             CUSTOM       9999       50121379    6415571584  2023-03-21 06:48:57
DEFAULT_RULE  CUSTOM            1              0             0     1970-01-01 00:00:00
```

```
admin@sonic:~$ sudo config policer add policer_test1 -mode sr_tcm -meter_type bytes -color blind -cir 100000000 -cbs 1000 -pbs 2000 -green_action forward -yellow_action forward -red_action forward
```

1.9 show acl counters

Function

Run the **show acl counters** command to display the ACL counters.

Syntax

show acl counters [*table-name*] [*rule-name*]

Parameter Description

table-name: The name of the ACL table.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show acl counters
RULE NAME      TABLE NAME       PRIO    PACKETS COUNT     BYTES COUNT    UPDATE TIME
----------     ----------       ----    --------------     ------------  -------------
RULE_1         CUSTOM           9999          7890943    1010075392  2023-03-21 06:48:47
```

```
DEFAULT_RULE CUSTOM          1              0            0  1970-01-01 00:00:00
RULE_1       TEST         9999        7878959   1008541568  2023-03-21 06:48:47
DEFAULT_RULE TEST            1              0            0  1970-01-01 00:00:00
```

```
admin@sonic:~$ show acl counters CUSTOM
RULE NAME     TABLE NAME       PRIO      PACKETS COUNT    BYTES COUNT    UPDATE TIME
----------    ------------   -----     -------------      ------------   --------------
RULE_1          CUSTOM       9999          50121379      6415571584   2023-03-21 06:48:57
DEFAULT_RULE    CUSTOM          1                 0               0    1970-01-01 00:00:00
```

```
admin@sonic:~$ show acl counters TEST RULE_1
RULE NAME      TABLE NAME       PRIO    PACKETS COUNT    BYTES COUNT    UPDATE TIME
-----------    ------------   ------   ---------------  -------------  ----------------
RULE_1         TEST             9999          92335015     11818917376   2023-03-21 06:49:07
```

1.10 show acl log-update interval

Function

Run the **show acl log-update interval** command to display the output interval of ACL matching logs.

Syntax

show acl log-update interval

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show acl log-update interval
acl log-update interval 1
```

1.11 show acl resources

Function

Run the **show acl resources** command to display the ACL resources.

Syntax

show acl resources { **group** | **table** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show acl resources table

Table Name      Table OID           Resource Name       Used Count      Available Count
------------  ----------------  ----------------  ------------  -----------------
CUSTOM          0x70000000009fb   acl_entry                    2               1534
CUSTOM          0x70000000009fb   acl_counter                  2              57850
```

```
admin@sonic:~$ show acl resources group

Stage     Bind Point      Resource Name       Used Count      Available Count
-------   ------------  ----------------  ------------  -----------------
INGRESS   PORT            acl_group                    1                255
INGRESS   PORT            acl_table                    2                  1
INGRESS   LAG             acl_group                    0                255
INGRESS   LAG             acl_table                    0                  1
INGRESS   VLAN            acl_group                    0                255
INGRESS   VLAN            acl_table                    0                  4
INGRESS   RIF             acl_group                    0                255
INGRESS   RIF             acl_table                    0                  4
INGRESS   SWITCH          acl_group                    0                255
INGRESS   SWITCH          acl_table                    0                  4
EGRESS    PORT            acl_group                    0                255
EGRESS    PORT            acl_table                    0                  2
EGRESS    LAG             acl_group                    0                255
EGRESS    LAG             acl_table                    0                  2
EGRESS    VLAN            acl_group                    0                255
EGRESS    VLAN            acl_table                    0                  2
EGRESS    RIF             acl_group                    0                255
EGRESS    RIF             acl_table                    0                  2
EGRESS    SWITCH          acl_group                    0                255
EGRESS    SWITCH          acl_table                    0                  2
```

1.12 show acl rule

Function

Run the **show acl rule** command to display all the ACL rules present in all the ACL tables or only the rules present in specified table "TABLE_NAME" or only the rule matching the RULE_ID option.

Output from the command gives the following information about the rules.

- Table name - ACL table name to which the rule belongs to.
- Rule name - ACL rule name
- Priority - Priority for this rule.
- Action - Action to be performed if the packet matches with this ACL rule.

It can be:

  - "DROP"/"FORWARD"("ACCEPT" for control plane ACL)

Users can choose to have a default permit rule or default deny rule. In case of default "deny all" rule, add the permitted rules on top of the deny rule. In case of the default "permit all" rule, users can add the deny rules on top of it. If users have not configured any rule, SONiC allows all traffic (which is "permit all").

- Match - The fields from the packet header that need to be matched against the same present in the incoming traffic.

Syntax

show acl rule [*table-name*] [*rule-id*]

Parameter Description

table-name: The name of the ACL table.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show acl rule

Table      Rule            Priority    Action      Match
-------  -----------  -------  --------  ----------------------------------------
CUSTOM     RULE_1        9999       DROP        DST_MAC: 00:e0:f8:00:00:0d/ff:ff:ff:ff:ff:ff
                                                 ETHER_TYPE: 2048
                                                 LOG_ACTION: LOG_SYSLOG
                                                 SRC_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
CUSTOM     RULE_2        9998      FORWARD    DST_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
                                                 LOG_ACTION: LOG_SYSLOG
```

```
                                                SRC_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
CUSTOM     DEFAULT_RULE   1        DROP        DST_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
                                                SRC_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
TEST       RULE_1         9999     DROP         DST_IP: 0.0.0.0/0
                                                LOG_ACTION: LOG_SYSLOG
                                                SRC_IP: 0.0.0.0/0
TEST       RULE_2         9998     DROP        DST_IP: 0.0.0.0/0
                                                LOG_ACTION: LOG_SYSLOG
                                                SRC_IP: 0.0.0.32/32
TEST       DEFAULT_RULE   1        DROP         ETHER_TYPE: 2048
```

```
admin@sonic:~$ show acl rule CUSTOM
Table      Rule           Priority     Action       Match
-------    -----------    --------     --------     ----------------------------------------
CUSTOM     RULE_1         9999         DROP         DST_MAC: 00:e0:f8:00:00:0d/ff:ff:ff:ff:ff:ff
                                                    ETHER_TYPE: 2048
                                                    LOG_ACTION: LOG_SYSLOG
                                                    SRC_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
CUSTOM     RULE_2         9998     FORWARD      DST_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
                                                    LOG_ACTION: LOG_SYSLOG
                                                    SRC_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
CUSTOM     DEFAULT_RULE   1        DROP        DST_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
                                                    SRC_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
```

```
admin@sonic:~$ show acl rule CUSTOM RULE_1
Table      Rule      Priority      Action      Match
-------    ------    -----  --    ------      ----------------------------------------
CUSTOM     RULE_1    9999      DROP         DST_MAC: 00:e0:f8:00:00:0d/ff:ff:ff:ff:ff:ff
                                            ETHER_TYPE: 2048
                                            LOG_ACTION: LOG_SYSLOG
                                            SRC_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
```

1.13 show acl table

Function

Run the **show acl table** command to display either all the ACL tables that are configured or only the specified "TABLE_NAME".

Output from the command displays the table name, type of the table, the cir and cbs, the dscp value, the status, the mode, the list of interface(s) to which the table is bound and the description about the table.

Syntax

show acl table [*table-name*]

Parameter Description

table-name: The name of the ACL table.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show acl table

Name    Type          Binding   Description   Stage   Dscp   CIR   CBS   Status   Mode
-----   ---------     -------   -----------   -----   -----  ---   ----  -----   --------
CTRL    CTRLPLANE      SSH        CTRL                                      N/A
CUSTOM  L2          Ethernet1   CUSTOM     ingress                    Active
TEST        L3          Ethernet1   TEST          ingress                    Active
Ethernet2
Ethernet3
TEST2       L3_QOS   Ethernet5   TEST2        ingress   10     100    200   Active
Ethernet6
TEST3       L3          Ethernet5   TEST3        egress                   Active    community
```

```
admin@sonic:~$ show acl table TEST
Name      Type      Binding      Description      Stage      Dscp      CIR      CBS      Status      Mode
------   ------   ---------   -------------   -------   ------   -----   -----   --------   ------
TEST      L3        Ethernet1   TEST             ingress                        Active
                    Ethernet2
                    Ethernet3
```

1 Qos Commands

Command	Function
config acl add table	Create new ACL tables.
config acl remove table	Delete an ACL table.
config acl update incremental	Configure the rules.
config interface qos default	Restore the queue rate limiting of interface or the port rate limiting to the default value.
config interface qos interface-rate-limit	Configure port rate limiting.
config interface qos queue-rate-limit	Configure queue rate limiting on interface.
config interface qos schedule	Configure the scheduling policy for the output queue of a port.
config interface qos schedule default	Restore the scheduling policy and weight of the port output queue to the default settings.
config interface trust-mode	Configure the trust mode of interface.
config qos clear	Clear all the QoS configuration from all the following QOS Tables in ConfigDB.
config qos map add	Configure qos map.
config qos map apply	Apply qos map to interface.
config qos map delete	Delete qos map.
config qos reload	Reload the QoS configuration.
show acl counters	Display the ACL statistics counters.
show acl rule	Display all the ACL rules present in all the ACL tables or only the rules present in specified table "TABLE_NAME" or only the rule matching the RULE_ID option.
show acl table	Display either all the ACL tables that are configured or only the specified "TABLE_NAME".

show buffer_pool persistent-watermark	Display the user persistent-watermark for all the buffer pools.
show buffer_pool watermark	Display the user watermark for all the buffer pools.
show interfaces qos interface-rate-limit	View the rate limiting of interface.
show interfaces qos map	View the priority mapping of packets applied to interface.
show interfaces qos queue-rate-limit	View the queue rate limiting on interface.
show interfaces trust-mode	View the trust mode of interface.
show pfc asymmetric	Display the status of asymmetric PFC for all interfaces or a given interface.
show pfc counters	Display the details of Rx & Tx priority-flow-control (pfc) for all ports. This command can be used to clear the counters using -c option.
show pfc priority	Display the lossless priorities for all interfaces or a given interface.
show priority-group	Display The user watermark or persistent-watermark for the Ingress "headroom" or "shared pool occupancy" per priority-group for all ports. Dropped packets per priority-group for all ports.
show qos map	View the packet priority mapping.
show queue counters	Display packet and byte counters for all queues of all ports or one specific-port given as argument.
show queue persistent-watermark	Display the user persistet-watermark for the queues (Egress shared pool occupancy per queue) for either the unicast queues or multicast queues for all ports.
show queue schedule	View the scheduling policy of the output queue of ports.
show queue watermark	Display the user watermark for the queues (Egress shared pool occupancy per queue) for either the unicast queues or multicast queues for all ports.

sonic-clear queue counters	Clear the statistics of packets in the queue.

1.1 config acl add table

Function

Run the **config acl add table** command to create new ACL tables.

You can use the high-capacity configuration mode and community configuration mode to create an ACL table. The distinction between the two modes applies only to the ACLs on the data plane.

Syntax

- high-capacity configuration mode:

config acl add table [*OPTIONS*] *table-name table-type* [**-d** *description*] [**-p** *ports*] [**-s** { **ingress** | **egress** }] [**-sp** *cir-cbs*] [**-sd** *dscp-value*] [**-ss** { **SSH** | **NTP** | **SNMP** }]

- community configuration mode:

config acl add table [*OPTIONS*] *table-name table-type* [**-d** *description*] [**-p** *ports*] [**-s** { **ingress** | **egress** }] [**-sp** *cir-cbs*] [**-sd** *dscp-value*] [**-ss** { **SSH** | **NTP** | **SNMP** }] **-m community**

Parameter Description

table-name: The name of the ACL table to create.

table-type: The type of ACL table to create (e.g. "L3", "L3V6", "MIRROR")

description: A description of the table for the user. (default is the table_name)

ports: A comma-separated list of ports/interfaces to add to the table. The behavior is as follows:

- Physical ports will be bound as physical ports
- Portchannels will be bound as portchannels - passing a portchannel member is invalid
- VLANs will be expanded into their members (e.g. "Vlan1000" will become "Ethernet0,Ethernet2,Ethernet4...")

stage: The stage this ACL table will be applied to, either ingress or egress. (default is ingress)

cir-cbs: The cir indicates the bandwidth limit per second (KBits). The cbs indicates the burst traffic limit (KBytes). This parameter is used for QoS ACL. (e.g. 1000000_2000)

dscp-value: The dscp value of the packet, range 0 to 63. This parameter is used for QoS ACL.

SSH | **NTP** | **SNMP:** The service type of CTRLPLANE ACL. This parameter is used for CTRLPLANE ACL.

Usage Guidelines

- ACL restrictions in high-capacity configuration mode
  - In high-capacity configuration mode, only one object (physical interface or portchannel interface) can be applied to the ACL in the egress direction.

- In high-capacity configuration mode, when an ACL is applied to portchannel, only one portchannel interface can be applied to an ACL.
- In high-capacity configuration mode, when an ACL is applied to vni, only one vni can be applied to an ACL.
- In high-capacity configuration mode, an ACL cannot be applied to both physical interfaces and portchannel interfaces.
- After an ACL is configured as high-capacity mode, it cannot be changed to the community mode. After an ACL is configured as the community mode, it cannot be changed to the high-capacity mode.

Examples

```
admin@sonic:~$ sudo config acl add table EXAMPLE L3 -p Ethernet1,Ethernet4 -s ingress
admin@sonic:~$ sudo config acl add table EXAMPLE_2 L3V6 -p Ethernet2 -s egress
admin@sonic:~$ sudo config acl add table EXAMPLE_3 L3_QOS -p Ethernet5 -s ingress -sp 1024_2048
-sd 30
admin@sonic:~$ sudo config acl add table EXAMPLE_4 L2_QOS -p Ethernet3 -s ingress -sd 28
admin@sonic:~$ sudo config acl add table EXAMPLE_5 L3V6_QOS -p Ethernet6 -s ingress -sp
1000_2000
admin@sonic:~$ sudo config acl add table EXAMPLE_6 CTRLPLANE -ss SSH
```

1.2 config acl remove table

Function

Run the **config acl remove table** command to delete an ACL table.

Syntax

config acl remove table [*OPTIONS*] *table-name* [**-p** *ports*] [**-up**] [**-ud**]

Parameter Description

table-name: The name of the ACL table to delete.

ports: A comma-separated list of ports/interfaces to add to the table. The behavior is as follows:

-ud: unset_dscp. The QoS DSCP parameters are deleted.

-up: unset_policer. The QoS policer parameters are deleted.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show acl table
Name      Type     Binding       Description      Stage     Dscp     CIR     CBS
------  ------  ----------  -------------  -------  ------  -----  -----
CUSTOM   L2       Ethernet1    CUSTOM           egress
TEST       L3       Ethernet49   TEST             ingress
```

```
admin@sonic:~$ sudo config acl remove table TEST
admin@sonic:~$ show acl table
Name      Type      Binding      Description      Stage      Dscp      CIR      CBS
------    ------    ---------    -------------    -------    ------    -----    -----
CUSTOM    L2        Ethernet1    CUSTOM             egress
```

```
admin@sonic:~$ show acl table
Name      Type      Binding      Description      Stage      Dscp      CIR      CBS
------    ------    ---------    -------------    -------    ------    -----    -----
TEST      L3_QOS    Ethernet1    TEST             ingress    30        1024     2048
admin@sonic:~$ sudo config acl remove table TEST -p Ethernet1
admin@sonic:~$ show acl table
Name      Type      Binding      Description      Stage      Dscp      CIR      CBS
------    ------    ---------    -------------    -------    ------    -----    -----
TEST      L3_QOS                 TEST                        30        1024     2048
```

```
admin@sonic:~$ show acl table
Name      Type      Binding      Description      Stage      Dscp      CIR      CBS
------    ------    ---------    -------------    -------    ------    -----    -----
TEST      L3_QOS    Ethernet1    TEST             ingress    30        1024     2048
admin@sonic:~$ sudo config acl remove table TEST -up -ud
admin@sonic:~$ show acl table
Name      Type      Binding      Description      Stage      Dscp      CIR      CBS
------    ------    ---------    -------------    -------    ------    -----    -----
TEST      L3_QOS    Ethernet1    TEST             ingress
```

1.3 config acl update incremental

Function

Run the **config acl update incremental** command to configure the rules.

Syntax

config acl update incremental [*OPTIONS*] *file-name*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config acl update incremental acl_rule.json
```

L3 ACL json example:

```
{
    "acl": {
        "acl-sets": {
            "acl-set": {
                "TEST2": {
                    "acl-entries": {
                        "acl-entry": {
                            "1": {
                                "actions": {
                                    "config": {
                                        "forwarding-action": "ACCEPT",
                                        "log-action": "LOG_SYSLOG"
                                        }
                                },
                                "config": {
                                    "sequence-id": 1
                                },
                                "icmp": {
                                    "config": {
                                        "type": "1",
                                        "code": "1"
                                    }
                                },
                                "ip": {
                                    "config": {
                                        "protocol":"IP_ICMP",
                                        "source-ip-address": "172.20.3.1/32",
                                        "destination-ip-address":"172.20.2.0/24"
                                    }
                                }
                            },
                             "2": {
                                "actions": {
                                    "config": {
                                        "forwarding-action": "ACCEPT"
                                    }
                                },
                                "config": {
                                    "sequence-id": 2
                                },
                                "ip": {
                                    "config": {
                                        "protocol": "IP_TCP",
                                        "source-ip-address": "1.1.1.1/32",
                                        "destination-ip-address": "2.2.2.2/32"
                                    }
```

```
                                    },
                                    "transport": {
                                        "config": {
                                            "source-port": "555",
                                            "destination-port": "2222",
                                            "tcp-flags": [
                                              "TCP_ACK",
                                              "TCP_SYN"
                                            ]
                                        }
                                    }
                                }
                            }
                        },
                        "config": {
                            "name": "TEST2"
                        }
                    }
                }
            }
        }
    }
}
```

L3 ACL json example Parameters:

- acl_rule.json: specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.
- forwarding-action(ACCEPT) : If this option is set, it indicates that the rule belongs to the allowed class.
- forwarding-action(REJECT) : If this option is configured, the keyword indicates that the rule is reject.
- forwarding-action(TRAP) : If this option is configured, this rule matches packets and sends a copy to the CPU. At the same time, the forwarded packets are discarded.
- forwarding-action(COPY) : If this option is configured, it indicates that the rule matches packets and sends a copy to the CPU. In addition, the packets forwarded are not affected.
- redirect-action(REDIRECT:target) : If this option is configured, it indicates that the rule belongs to the redirection class.To use the ACL redirection function, change the "forwarding-action" to "redirect-action".The redirection action must be configured in the "redirect-action:REDIRECT:target" format. The "target" indicates the redirected target in the following formats:
  - ipaddress (ipv6 supported)
  - port/portchannel

- ipaddress@port/portchannel
- ipaddress@vrfname
- ipaddress1,ipaddress2... (Next hop group)
- ipaddress1,ipaddress2... @port/portchannel/vrfname (Next hop group)

- protocol: indicates the IP protocol number. The value ranges from 0 to 255. For convenience, the system provides short names of common IP protocol numbers to replace specific IP protocol numbers, including IP_TCP, IP_UDP, and IP_ICMP.
- source-ip-address: If this parameter is specified, the IP packets sent from a host or from hosts within a certain IP network segment are to be matched.
- source-port: indicates the source port number of the matched packets. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- destination-ip-address: If this option is configured, the packets destined for a specific host or hosts on a specific IP network segment are to be matched.
- destination-port: indicates the destination port of the matched packet. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- tcp-flags: indicates the TCP FLAG bit. It includes TCP_FIN, TCP_SYN, TCP_RST, TCP_PSH, TCP_ACK, and TCP_URG.
- log-action: If this option is configured, the matching log is periodically generated if packets are matched.

L3V6 ACL json example:

```
{
    "acl": {
        "acl-sets": {
            "acl-set": {
                "TEST2": {
                    "acl-entries": {
                        "acl-entry": {
                            "1": {
                                "actions": {
                                    "config": {
                                        "forwarding-action": "ACCEPT",
                                        "log-action": "LOG_SYSLOG"
                                    }
                                },
                                "config": {
                                    "sequence-id": 1
                                },
                                "icmp": {
                                    "config": {
                                        "type": "1",
                                        "code": "1"
                                    }
                                },
```

```
                                    "ip": {
                                        "config": {
                                            "protocol":"IP_ICMP",
                                            "source-ip-address": "201::2/128",
                                            "destination-ip-address":"0::0/0"
                                        }
                                    }
                                },
                                "2": {
                                    "actions": {
                                        "config": {
                                            "forwarding-action": "ACCEPT"
                                        }
                                    },
                                    "config": {
                                        "sequence-id": 2
                                    },
                                    "ip": {
                                        "config": {
                                            "protocol": "IP_TCP",
                                            "source-ip-address": "200::1/128",
                                            "destination-ip-address": "0::/0"
                                        }
                                    },
                                    "transport": {
                                        "config": {
                                            "source-port": "555",
                                            "destination-port": "2222",
                                            "tcp-flags": [
                                              "TCP_ACK",
                                              "TCP_SYN"
                                            ]
                                        }
                                    }
                                }
                            }
                        },
                        "config": {
                            "name": "TEST2"
                        }
                    }
                }
            }
        }
}
```

L3V6 ACL json example Parameters:

- acl_rule.json: specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.
- forwarding-action(ACCEPT) : If this option is set, it indicates that the rule belongs to the allowed class.
- forwarding-action(REJECT) : If this option is configured, the keyword indicates that the rule is reject.
- forwarding-action(TRAP) : If this option is configured, this rule matches packets and sends a copy to the CPU. At the same time, the forwarded packets are discarded.
- forwarding-action(COPY) : If this option is configured, it indicates that the rule matches packets and sends a copy to the CPU. In addition, the packets forwarded are not affected.
- redirect-action(REDIRECT:target) : If this option is configured, it indicates that the rule belongs to the redirection class.To use the ACL redirection function, change the "forwarding-action" to "redirect-action".The redirection action must be configured in the "redirect-action:REDIRECT:target" format. The "target" indicates the redirected target in the following formats:
  - ipaddress (ipv6 supported)
  - port/portchannel
  - ipaddress@port/portchannel
  - ipaddress@vrfname
  - ipaddress1,ipaddress2... (Next hop group)
  - ipaddress1,ipaddress2... @port/portchannel/vrfname (Next hop group)
- protocol: indicates the IP protocol number. The value ranges from 0 to 255. For convenience, the system provides short names of common IP protocol numbers to replace specific IP protocol numbers, including IP_TCP, IP_UDP.
- source-ip-address: If this parameter is specified, the IPv6 packets sent from a host or from hosts within a certain IPv6 network segment are to be matched.
- source-port: indicates the source port number of the matched packets. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- destination-ip-address: If this option is configured, the IPv6 packets destined for a specific host or hosts on a specific IPv6 network segment are to be matched.
- destination-port: indicates the destination port of the matched packet. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- tcp-flags: indicates the TCP FLAG bit. It includes TCP_FIN, TCP_SYN, TCP_RST, TCP_PSH, TCP_ACK, and TCP_URG.
- log-action: If this option is configured, the matching log is periodically generated if packets are matched.

CTRLPLANE ACL json example:

```
{
```

```
    "acl": {
        "acl-sets": {
            "acl-set": {
                "TEST4": {
                    "acl-entries": {
                        "acl-entry": {
                            "1": {
                                "actions": {
                                    "config": {
                                        "forwarding-action": "REJECT",
                                        "log-action": "LOG_SYSLOG"
                                    }
                                },
                                "config": {
                                    "sequence-id": 10
                                },
                                "ip": {
                                    "config": {
                                        "source-ip-address": "192.168.2.2/32"
                                    }
                                },
                                "transport": {
                                    "config": {
                                        "destination-port": "2222"
                                    }
                                }
                            }
                        }
                    },
                    "config": {
                        "name": "CUSTOM"
                    }
                }
            }
        }
    }
}
```

CTRLPLANE ACL json example Parameters:

- acl_rule.json: specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.
- forwarding-action(ACCEPT) : If this option is set, it indicates that the rule belongs to the allowed class.

- forwarding-action(REJECT) : If this option is configured, the keyword indicates that the rule is reject.
- source-ip-address: If this parameter is specified, the IP packets sent by a host with the source IP address or the packets sent by hosts within a certain IP network segment match the IP packets sent by any host. The value can be an IPv4 or IPv6 address.
- destination-port: indicates the matched packet port number. This field does not need to be specified by default.
- tcp-flags: indicates the TCP FLAG bit. It includes TCP_FIN, TCP_SYN, TCP_RST, TCP_PSH, TCP_ACK, and TCP_URG.

#L2 ACL json example:

```
{
    "acl": {
        "acl-sets": {
            "acl-set": {
                "CUSTOM": {
                    "acl-entries": {
                        "acl-entry": {
                            "1": {
                                "actions": {
                                    "config": {
                                        "forwarding-action": "ACCEPT",
                                        "log-action": "LOG_SYSLOG"
                                    }
                                },
                                "config": {
                                    "sequence-id": 10
                                },
                                "l2": {
                                    "config": {
                                        "ethertype": "2048",
                                        "destination-mac": "00:e0:f8:00:00:0c",
                                        "destination-mac-mask": "ff:ff:ff:ff:ff:ff"
                                    }
                                }
                            }
                        }
                    },
                    "config": {
                        "name": "CUSTOM"
                    }
                }
            }
        }
    }
}
```

L2 ACL json example Parameters:

- acl_rule.json: specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.
- forwarding-action(ACCEPT) : If this option is set, it indicates that the rule belongs to the allowed class.
- forwarding-action(REJECT) : If this option is configured, the keyword indicates that the rule is reject.
- forwarding-action(TRAP) : If this option is configured, this rule matches packets and sends a copy to the CPU. At the same time, the forwarded packets are discarded.
- forwarding-action(COPY) : If this option is configured, it indicates that the rule matches packets and sends a copy to the CPU. In addition, the packets forwarded are not affected.
- redirect-action(REDIRECT:target) : If this option is configured, it indicates that the rule belongs to the redirection class.To use the ACL redirection function, change the "forwarding-action" to "redirect-action".The redirection action must be configured in the "redirect-action:REDIRECT:target" format. The "target" indicates the redirected target in the following formats:
  - ipaddress (ipv6 supported)
  - port/portchannel
  - ipaddress@port/portchannel
  - ipaddress@vrfname
  - ipaddress1,ipaddress2... (Next hop group)
  - ipaddress1,ipaddress2... @port/portchannel/vrfname (Next hop group)
- ether type: If configured, Layer 2 packets of the specified Ethernet type must be matched.
- source-mac: If this option is configured, it matches Layer 2 packets sent by a host with the source MAC address or packets sent by hosts within a certain MAC address segment.
- destination-mac: indicates that Layer 2 packets whose destination mac address is a host or packets whose destination MAC address is a host on a specific MAC address segment are to be matched.
- log-action: If this option is configured, the matching log is periodically generated if packets are matched.

L3_QOS ACL json example:

```
{
    "acl": {
        "acl-sets": {
            "acl-set": {
                "TEST2": {
                    "acl-entries": {
                        "acl-entry": {
```

```
                "1": {
                    "actions": {
                        "config": {
                            "forwarding-action": "ACCEPT",
                            "log-action": "LOG_SYSLOG"
                        }
                    },
                    "config": {
                        "sequence-id": 1
                    },
                    "icmp": {
                        "config": {
                            "type": "1",
                            "code": "1"
                        }
                    },
                    "ip": {
                        "config": {
                            "protocol":"IP_ICMP",
                            "source-ip-address": "172.20.3.1/32",
                            "destination-ip-address":"172.20.2.0/24"
                        }
                    }
                },
                "2": {
                    "actions": {
                        "config": {
                            "forwarding-action": "ACCEPT"
                        }
                    },
                    "config": {
                        "sequence-id": 2
                    },
                    "ip": {
                        "config": {
                            "protocol": "IP_TCP",
                            "source-ip-address": "1.1.1.1/32",
                            "destination-ip-address": "2.2.2.2/32"
                        }
                    },
                    "transport": {
                        "config": {
                            "source-port": "555",
                            "destination-port": "2222",
                            "tcp-flags": [
                              "TCP_ACK",
```

```
                                        "TCP_SYN"
                                    ]
                                }
                            }
                        }
                    },
                    "config": {
                        "name": "TEST2"
                    }
                }
            }
        }
    }
}
```

L3_QOS ACL json example Parameters:

- acl_rule.json: specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.
- forwarding-action(ACCEPT) : If this option is set, it indicates that the rule belongs to the allowed class.
- forwarding-action(REJECT) : If this option is configured, the keyword indicates that the rule is reject.
- protocol: indicates the IP protocol number. The value ranges from 0 to 255. For convenience, the system provides short names of common IP protocol numbers to replace specific IP protocol numbers, including IP_TCP, IP_UDP, and IP_ICMP.
- sourece-ip-address: If this parameter is specified, the IP packets sent from a host or from hosts within a certain IP network segment are to be matched.
- source-port: indicates the source port number of the matched packets. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- destination-ip-address: If this option is configured, the packets destined for a specific host or hosts on a specific IP network segment are to be matched.
- destination-port: indicates the destination port of the matched packet. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- tcp-flags: indicates the TCP FLAG bit. It includes TCP_FIN, TCP_SYN, TCP_RST, TCP_PSH, TCP_ACK, and TCP_URG.
- log-action: If this option is configured, the matching log is periodically generated if packets are matched.

L3V6_QOS ACL json example:

```
{
```

```
"acl": {
    "acl-sets": {
        "acl-set": {
            "TEST2": {
                "acl-entries": {
                    "acl-entry": {
                        "1": {
                            "actions": {
                                "config": {
                                    "forwarding-action": "ACCEPT",
                                    "log-action": "LOG_SYSLOG"
                                }
                            },
                            "config": {
                                "sequence-id": 1
                            },
                            "icmp": {
                                "config": {
                                    "type": "1",
                                    "code": "1"
                                }
                            },
                            "ip": {
                                "config": {
                                    "protocol":"IP_ICMP",
                                    "source-ip-address": "172.20.3.1/32",
                                    "destination-ip-address":"172.20.2.0/24"
                                }
                            }
                        },
                        "2": {
                            "actions": {
                                "config": {
                                    "forwarding-action": "ACCEPT"
                                }
                            },
                            "config": {
                                "sequence-id": 2
                            },
                            "ip": {
                                "config": {
                                    "protocol": "IP_TCP",
                                    "source-ip-address": "1.1.1.1/32",
                                    "destination-ip-address": "2.2.2.2/32"
                                }
                            },
```

```
                                    "transport": {
                                        "config": {
                                            "source-port": "555",
                                            "destination-port": "2222",
                                            "tcp-flags": [
                                              "TCP_ACK",
                                              "TCP_SYN"
                                            ]
                                        }
                                    }
                                }
                            }
                        },
                        "config": {
                            "name": "TEST2"
                        }
                    }
                }
            }
        }
}
```

L3V6_QOS ACL json example Parameters:

- acl_rule.json: specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.
- forwarding-action(ACCEPT) : If this option is set, it indicates that the rule belongs to the allowed class.
- forwarding-action(REJECT) : If this option is configured, the keyword indicates that the rule is reject.
- protocol: indicates the IP protocol number. The value ranges from 0 to 255. For convenience, the system provides short names of common IP protocol numbers to replace specific IP protocol numbers, including IP_TCP, IP_UDP.
- source-ip-address: If this parameter is specified, the IPv6 packets sent from a host or from hosts within a certain IPv6 network segment are to be matched.
- source-port: indicates the source port number of the matched packets. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- destination-ip-address: If this option is configured, the IPv6 packets destined for a specific host or hosts on a specific IPv6 network segment are to be matched.
- destination-port: indicates the destination port of the matched packet. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- tcp-flags: indicates the TCP FLAG bit. It includes TCP_FIN, TCP_SYN, TCP_RST, TCP_PSH,

TCP_ACK, and TCP_URG.

- log-action: If this option is configured, the matching log is periodically generated if packets are matched.

L2_QOS ACL json example:

```
{
    "acl": {
        "acl-sets": {
            "acl-set": {
                "CUSTOM": {
                    "acl-entries": {
                        "acl-entry": {
                            "1": {
                                "actions": {
                                    "config": {
                                        "forwarding-action": "ACCEPT",
                                        "log-action": "LOG_SYSLOG"
                                    }
                                },
                                "config": {
                                    "sequence-id": 10
                                },
                                "l2": {
                                    "config": {
                                        "ethertype": "2048",
                                        "destination-mac": "00:e0:f8:00:00:0c",
                                        "destination-mac-mask": "ff:ff:ff:ff:ff:ff"
                                    }
                                }
                            }
                        }
                    },
                    "config": {
                        "name": "CUSTOM"
                    }
                }
            }
        }
    }
}
```

L2_QOS ACL json example Parameters:

- acl_rule.json: specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is,

the packets are preferentially matched.

- forwarding-action(ACCEPT) : If this option is set, it indicates that the rule belongs to the allowed class.
- forwarding-action(REJECT) : If this option is configured, the keyword indicates that the rule is reject.
- ether type: If configured, Layer 2 packets of the specified Ethernet type must be matched.
- source-mac: If this option is configured, it matches Layer 2 packets sent by a host with the source MAC address or packets sent by hosts within a certain MAC address segment.
- destination-mac: indicates that Layer 2 packets whose destination mac address is a host or packets whose destination MAC address is a host on a specific MAC address segment are to be matched.
- log-action: If this option is configured, the matching log is periodically generated if packets are matched.

MIRROR ACL json example:

```
{
    "acl": {
        "acl-sets": {
            "acl-set": {
                "TEST2": {
                    "acl-entries": {
                        "acl-entry": {
                            "1": {
                                "actions": {
                                    "config": {
                                        "forwarding-action": "ACCEPT",
                                        "log-action": "LOG_SYSLOG"
                                    }
                                },
                                "config": {
                                    "sequence-id": 1
                                },
                                "icmp": {
                                    "config": {
                                        "type": "1",
                                        "code": "1"
                                    }
                                },
                                "ip": {
                                    "config": {
                                        "protocol":"IP_ICMP",
                                        "source-ip-address": "172.20.3.1/32",
                                        "destination-ip-address":"172.20.2.0/24"
                                    }
```

```
                    }
                },
                "2": {
                    "actions": {
                        "config": {
                            "forwarding-action": "ACCEPT"
                        }
                    },
                    "config": {
                        "sequence-id": 2
                    },
                    "icmp": {
                        "config": {
                            "type": "1",
                            "code": "1"
                        }
                    },
                    "ip": {
                        "config": {
                            "protocol": "IP_TCP",
                            "source-ip-address": "1.1.1.1/32",
                            "destination-ip-address": "2.2.2.2/32"
                        }
                    },
                    "transport": {
                        "config": {
                            "source-port": "555",
                            "destination-port": "2222",
                            "tcp-flags": [
                              "TCP_ACK",
                              "TCP_SYN"
                            ]
                        }
                    }
                }
            }
        },
        "config": {
            "name": "TEST2"
        }
    }
  }
 }
}
```

MIRROR ACL json example Parameters:

- acl_rule.json: specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.
- forwarding-action(ACCEPT) : If this option is configured, it indicates that the rule belongs to the allowed class. After this field is set to ACCEPT, the ACL RULE action of the MIRROR type in the ingress direction is converted to MIRROR_INGRESS_ACTION, indicating the traffic of the mirror ingress direction.
- protocol: indicates the IP protocol number. The value ranges from 0 to 255. For convenience, the system provides short names of common IP protocol numbers to replace specific IP protocol numbers, including IP_TCP, IP_UDP, and IP_ICMP.
- source-ip-address: If this parameter is specified, the IP packets sent from a host or from hosts within a certain IP network segment are to be matched.
- source-port: indicates the source port number of the matched packets. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- destination-ip-address: If this option is configured, the packets destined for a specific host or hosts on a specific IP network segment are to be matched.
- destination-port: indicates the destination port of the matched packet. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- tcp-flags: indicates the TCP FLAG bit. It includes TCP_FIN, TCP_SYN, TCP_RST, TCP_PSH, TCP_ACK, and TCP_URG.
- log-action: If this option is configured, the matching log is periodically generated if packets are matched.

MIRRORV6 ACL json example:

```
{
    "acl": {
        "acl-sets": {
            "acl-set": {
                "TEST2": {
                    "acl-entries": {
                        "acl-entry": {
                            "1": {
                                "actions": {
                                    "config": {
                                        "forwarding-action": "ACCEPT",
                                        "log-action": "LOG_SYSLOG"
                                    }
                                },
                                "config": {
                                    "sequence-id": 1
                                },
                                "icmp": {
                                    "config": {
```

```
                        "type": "1",
                        "code": "1"
                    }
                },
                "ip": {
                    "config": {
                        "protocol":"IP_ICMP",
                        "source-ip-address": "201::2/128",
                        "destination-ip-address":"0::0/0"
                    }
                }
            },
            "2": {
                "actions": {
                    "config": {
                        "forwarding-action": "ACCEPT"
                    }
                },
                "config": {
                    "sequence-id": 2
                },
                "icmp": {
                    "config": {
                        "type": "1",
                        "code": "1"
                    }
                },
                "ip": {
                    "config": {
                        "protocol": "IP_TCP",
                        "source-ip-address": "200::1/128",
                        "destination-ip-address": "0::/0"
                    }
                },
                "transport": {
                    "config": {
                        "source-port": "555",
                        "destination-port": "2222",
                        "tcp-flags": [
                          "TCP_ACK",
                          "TCP_SYN"
                        ]
                    }
                }
            }
        }
```

```
                    },
                    "config": {
                        "name": "TEST2"
                    }
                }
            }
        }
    }
}
```

MIRRORV6 ACL json example Parameters:

- acl_rule.json: specifies the imported json file name.
- sequence-id: indicates the sequence number of the rule entry. The value range is [1, 9000]. The sequence number determines the priority of the rule entry in the access list. The smaller the sequence number is, the larger the priority is. The higher the priority is, the packets are preferentially matched.
- forwarding-action(ACCEPT) : If this option is configured, it indicates that the rule belongs to the allowed class. After this field is set to ACCEPT, the ACL RULE action of the MIRROR type in the ingress direction is converted to MIRROR_INGRESS_ACTION, indicating the traffic of the mirror ingress direction.
- protocol: indicates the IP protocol number. The value ranges from 0 to 255. For convenience, the system provides short names of common IP protocol numbers to replace specific IP protocol numbers, including IP_TCP, IP_UDP, and IP_ICMP.
- source-ip-address: If this parameter is specified, the IP packets sent from a host or from hosts within a certain IP network segment are to be matched.
- source-port: indicates the source port number of the matched packets. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- destination-ip-address: If this option is configured, the packets destined for a specific host or hosts on a specific IP network segment are to be matched.
- destination-port: indicates the destination port of the matched packet. The value ranges from 0 to 65535. This option is available when the protocol type is IP_TCP or IP_UDP.
- tcp-flags: indicates the TCP FLAG bit. It includes TCP_FIN, TCP_SYN, TCP_RST, TCP_PSH, TCP_ACK, and TCP_URG.
- log-action: If this option is configured, the matching log is periodically generated if packets are matched.

1.4 config interface qos default

Function

Run the **config interface qos default** command to restore the queue rate limiting of interface or the port rate limiting to the default value.

Syntax

config interface qos default interface-rate-limit *interface-name*

config interface qos default queue-rate-limit *interface-name queue-id*

Parameter Description

interface-name: interface name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces qos interface-rate-limit
  Port           pir           pbs
  ----------   ---------   -----
  Ethernet1
  Ethernet2
  Ethernet3    200000000   2000
  Ethernet4
  Ethernet5
  Ethernet6
  Ethernet7
  Ethernet8
  Ethernet9
  Ethernet10   300000000
  Ethernet11
  Ethernet12
  Ethernet13
  Ethernet14
  Ethernet15
  Ethernet16
  Ethernet17
  Ethernet18
  Ethernet19
  Ethernet20
  Ethernet21
  Ethernet22
  Ethernet23
  Ethernet24
  Ethernet25
  Ethernet26
  Ethernet27
  Ethernet28
  Ethernet29
  Ethernet30
  Ethernet31
  Ethernet32
  Ethernet33
  Ethernet34
```

```
  Ethernet35
  Ethernet36
  Ethernet37
  Ethernet38
  Ethernet39
  Ethernet40
  Ethernet41
  Ethernet42
  Ethernet43
  Ethernet44
  Ethernet45
  Ethernet46
  Ethernet47
  Ethernet48
  Ethernet49
  Ethernet53
  Ethernet57
  Ethernet61
  Ethernet65
  Ethernet69
  Ethernet73
  Ethernet77

admin@sonic:~$ sudo config interface qos default interface-rate-limit Ethernet3
admin@sonic:~$ show interfaces qos interface-rate-limit
  Port            pir            pbs
  ----------   ---------   -----
  Ethernet1
  Ethernet2
  Ethernet3
  Ethernet4
  Ethernet5
  Ethernet6
  Ethernet7
  Ethernet8
  Ethernet9
  Ethernet10   300000000
  Ethernet11
  Ethernet12
  Ethernet13
  Ethernet14
  Ethernet15
  Ethernet16
  Ethernet17
  Ethernet18
  Ethernet19
```

```
  Ethernet20
  Ethernet21
  Ethernet22
  Ethernet23
  Ethernet24
  Ethernet25
  Ethernet26
  Ethernet27
  Ethernet28
  Ethernet29
  Ethernet30
  Ethernet31
  Ethernet32
  Ethernet33
  Ethernet34
  Ethernet35
  Ethernet36
  Ethernet37
  Ethernet38
  Ethernet39
  Ethernet40
  Ethernet41
  Ethernet42
  Ethernet43
  Ethernet44
  Ethernet45
  Ethernet46
  Ethernet47
  Ethernet48
  Ethernet49
  Ethernet53
  Ethernet57
  Ethernet61
  Ethernet65
  Ethernet69
  Ethernet73
  Ethernet77

admin@sonic:~$ show interfaces qos queue-rate-limit Ethernet1
  Port          queue-id      cir           cbs      pir           pbs
  ---------   ----------   ---------   -----   ---------   -----
  Ethernet1   0             200000000
  Ethernet1   1
  Ethernet1   2             200000000   2000    300000000   3000
  Ethernet1   3
  Ethernet1   4
```

```
Ethernet1   5
Ethernet1   6
Ethernet1   7
admin@sonic:~$ sudo config interface qos default queue-rate-limit Ethernet1 2
admin@sonic:~$ show interfaces qos queue-rate-limit Ethernet1
Port         queue-id      cir          cbs      pir      pbs
---------  ----------  ---------  -----  -----  -----
Ethernet1   0             200000000
Ethernet1   1
Ethernet1   2
Ethernet1   3
Ethernet1   4
Ethernet1   5
Ethernet1   6
Ethernet1   7
```

1.5 config interface qos interface-rate-limit

Function

Run the **config interface qos interface-rate-limit** command to configure port rate limiting.

Syntax

config interface qos interface-rate-limit *interface-name* **-pir** *pir-value* [**-pbs** *pbs-value*]

Parameter Description

interface-name: interface name.

Usage Guidelines

NOTE:

- PIR (Peak Information Rate): The maximum information rate. Measured in Kbit/s.
- PBS (Peak Burst Size): The size of the maximum burst. Measured in Kbytes.
- When configuring PIR/PBS as 0, it indicates that the corresponding rate or size is not limited.
- For M2-W6510-48V8C, M2-W6510-32C, M2-W6510-48GT4V, and M2-W6910-64C products, the maximum configurable port-based QoS rate limit is 106 Gbit/s.
- Setting PBS must be done before setting CBS.
- There is a deviation between the actual effect of port rate limiting and the configured rate limit value. The larger the byte size, the greater the precision. For packets of 64 bytes, the error can exceed 10%.

Examples

```
admin@sonic:~$ sudo config interface qos interface-rate-limit Ethernet3 -pir 200000000 -pbs 2000
admin@sonic:~$ show interfaces qos interface-rate-limit
  Port          pir          pbs
```

```
----------  ---------  -----
Ethernet1
Ethernet2
Ethernet3    200000000   2000
Ethernet4
Ethernet5
Ethernet6
Ethernet7
Ethernet8
Ethernet9
Ethernet10
Ethernet11
Ethernet12
Ethernet13
Ethernet14
Ethernet15
Ethernet16
Ethernet17
Ethernet18
Ethernet19
Ethernet20
Ethernet21
Ethernet22
Ethernet23
Ethernet24
Ethernet25
Ethernet26
Ethernet27
Ethernet28
Ethernet29
Ethernet30
Ethernet31
Ethernet32
Ethernet33
Ethernet34
Ethernet35
Ethernet36
Ethernet37
Ethernet38
Ethernet39
Ethernet40
Ethernet41
Ethernet42
Ethernet43
Ethernet44
Ethernet45
```

```
  Ethernet46
  Ethernet47
  Ethernet48
  Ethernet49
  Ethernet53
  Ethernet57
  Ethernet61
  Ethernet65
  Ethernet69
  Ethernet73
  Ethernet77

admin@sonic:~$ sudo config interface qos interface-rate-limit Ethernet10 -pir 300000000
admin@sonic:~$ show interfaces qos interface-rate-limit
  Port            pir            pbs
  ----------   ---------   -----
  Ethernet1
  Ethernet2
  Ethernet3    200000000   2000
  Ethernet4
  Ethernet5
  Ethernet6
  Ethernet7
  Ethernet8
  Ethernet9
  Ethernet10   300000000
  Ethernet11
  Ethernet12
  Ethernet13
  Ethernet14
  Ethernet15
  Ethernet16
  Ethernet17
  Ethernet18
  Ethernet19
  Ethernet20
  Ethernet21
  Ethernet22
  Ethernet23
  Ethernet24
  Ethernet25
  Ethernet26
  Ethernet27
  Ethernet28
  Ethernet29
  Ethernet30
```

```
Ethernet31
Ethernet32
Ethernet33
Ethernet34
Ethernet35
Ethernet36
Ethernet37
Ethernet38
Ethernet39
Ethernet40
Ethernet41
Ethernet42
Ethernet43
Ethernet44
Ethernet45
Ethernet46
Ethernet47
Ethernet48
Ethernet49
Ethernet53
Ethernet57
Ethernet61
Ethernet65
Ethernet69
Ethernet73
Ethernet77
```

1.6 config interface qos queue-rate-limit

Function

Run the **config interface qos queue-rate-limit** command to configure queue rate limiting on interface.

Syntax

config interface qos queue-rate-limit *interface-name queue-id* **-cir** *cir-value* [**-cbs** *cbs-value*] [**-pir** *pir-value*] [**-pbs** *pbs-value*]

Parameter Description

interface-name: interface name.

Usage Guidelines

NOTE:

- CIR (Committed Information Rate): The guaranteed information rate. Measured in Kbit/s.
- CBS (Committed Burst Size): The size of the guaranteed burst. Measured in Kbytes.

- PIR (Peak Information Rate): The maximum information rate. Measured in Kbit/s.
- PBS (Peak Burst Size): The size of the maximum burst. Measured in Kbytes.
- If both CIR and PIR are configured simultaneously, the value of CIR must be less than or equal to the value of PIR. If both CBS and PBS are configured simultaneously, the value of CBS must be less than or equal to the value of PBS.
- When configuring CIR/CBS/PIR/PBS as 0, it indicates that the corresponding rate or size is not limited.
- Setting CBS must be done before setting CIR.
- Setting PIR must be done before setting CIR.
- Setting PBS must be done before setting CBS.

- There is a deviation between the actual effect of queue rate limiting and the configured rate limit value. The larger the byte size, the greater the precision. For packets of 64 bytes, the error can exceed 10%.

Examples

```
admin@sonic:~$ sudo config interface qos queue-rate-limit Ethernet1 0 -cir 200000000
admin@sonic:~$ show interfaces qos queue-rate-limit Ethernet1
  Port         queue-id     cir          cbs     pir     pbs
  ---------  ----------  ---------  -----  -----  -----
  Ethernet1  0           200000000
  Ethernet1  1
  Ethernet1  2
  Ethernet1  3
  Ethernet1  4
  Ethernet1  5
  Ethernet1  6
  Ethernet1  7

admin@sonic:~$ sudo config interface qos queue-rate-limit Ethernet1 2 -cir 200000000 -cbs 2000 -
pir 300000000 -pbs 3000
admin@sonic:~$ show interfaces qos queue-rate-limit Ethernet1
  Port         queue-id     cir          cbs     pir          pbs
  ---------  ----------  ---------  -----  ---------  -----
  Ethernet1  0           200000000
  Ethernet1  1
  Ethernet1  2           200000000  2000   300000000  3000
  Ethernet1  3
  Ethernet1  4
  Ethernet1  5
  Ethernet1  6
  Ethernet1  7
```

1.7 config interface qos schedule

Function

Run the **config interface qos schedule** command to configure the scheduling policy for the output queue of a port.

Syntax

config interface qos schedule *interface-name* **sp**

config interface qos schedule *interface-name* **wrr** *tx0 tx1 tx2 tx3 tx4 tx5 tx6 tx7*

config interface qos schedule *interface-name* **dwrr** *tx0 tx1 tx2 tx3 tx4 tx5 tx6 tx7*

Parameter Description

interface-name: interface name.

tx0 tx1 tx2 tx3 tx4 tx5 tx6 tx7: indicates the weight assigned to the corresponding scheduling algorithm.

sp: Strict-Priority scheduling.

wrr: Weighted Round Robin scheduling.

dwrr: Dificit Round Robin scheduling.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface qos schedule Ethernet1 sp
  admin@sonic:~$ show queue schedule Ethernet1
  Port         TxQ     Mode        Weight
  ---------  -----  ------  --------
  Ethernet1   UC0     SP              0
  Ethernet1   UC1     SP              0
  Ethernet1   UC2     SP              0
  Ethernet1   UC3     SP              0
  Ethernet1   UC4     SP              0
  Ethernet1   UC5     SP              0
  Ethernet1   UC6     SP              0
  Ethernet1   UC7     SP              0

admin@sonic:~$ sudo config interface qos schedule Ethernet2 wrr 0 0 0 0 1 2 3 4
admin@sonic:~$ show queue schedule Ethernet2
  Port         TxQ     Mode        Weight
  ---------  -----  ------  --------
  Ethernet2   UC0     SP              0
  Ethernet2   UC1     SP              0
```

```
  Ethernet2   UC2      SP                0
  Ethernet2   UC3      SP                0
  Ethernet2   UC4      WRR               1
  Ethernet2   UC5      WRR               2
  Ethernet2   UC6      WRR               3
  Ethernet2   UC7      WRR               4
admin@sonic:~$ sudo config interface qos schedule Ethernet3 wrr 1 2 3 4 5 6 7 8
admin@sonic:~$ show queue schedule Ethernet3
  Port          TxQ      Mode        Weight
  ---------   -----   ------   --------
  Ethernet3   UC0      WRR               1
  Ethernet3   UC1      WRR               2
  Ethernet3   UC2      WRR               3
  Ethernet3   UC3      WRR               4
  Ethernet3   UC4      WRR               5
  Ethernet3   UC5      WRR               6
  Ethernet3   UC6      WRR               7
  Ethernet3   UC7      WRR               8

admin@sonic:~$ sudo config interface qos schedule Ethernet4 dwrr 1 2 3 4 5 6 7 8
admin@sonic:~$ show queue schedule Ethernet4
  Port          TxQ      Mode        Weight
  ---------   -----   ------   --------
  Ethernet4   UC0      DWRR              1
  Ethernet4   UC1      DWRR              2
  Ethernet4   UC2      DWRR              3
  Ethernet4   UC3      DWRR              4
  Ethernet4   UC4      DWRR              5
  Ethernet4   UC5      DWRR              6
  Ethernet4   UC6      DWRR              7
  Ethernet4   UC7      DWRR              8

admin@sonic:~$ sudo config interface qos schedule Ethernet5 dwrr 5 6 7 8 0 0 0 0
admin@sonic:~$ show queue schedule Ethernet5
  Port          TxQ      Mode        Weight
  ---------   -----   ------   --------
  Ethernet5   UC0      DWRR              5
  Ethernet5   UC1      DWRR              6
  Ethernet5   UC2      DWRR              7
  Ethernet5   UC3      DWRR              8
  Ethernet5   UC4      SP                0
  Ethernet5   UC5      SP                0
  Ethernet5   UC6      SP                0
  Ethernet5   UC7      SP                0
```

1.8 config interface qos schedule default

Function

Run the **config interface qos schedule default** command to restore the scheduling policy and weight of the port output queue to the default settings.

Syntax

config interface qos schedule *interface-name* **wrr 11111111**

Parameter Description

interface-name: interface name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show queue schedule Ethernet1
  Port          TxQ      Mode        Weight
  ---------   -----   ------   --------
  Ethernet1   UC0      SP               0
  Ethernet1   UC1      SP               0
  Ethernet1   UC2      SP               0
  Ethernet1   UC3      SP               0
  Ethernet1   UC4      DWRR             1
  Ethernet1   UC5      DWRR             2
  Ethernet1   UC6      DWRR             3
  Ethernet1   UC7      DWRR             4

admin@sonic:~$ sudo config interface qos schedule Ethernet1 wrr 11111111
admin@sonic:~$ show queue schedule Ethernet1
  Port          TxQ      Mode        Weight
  ---------   -----   ------   --------
  Ethernet1   UC0      WRR              1
  Ethernet1   UC1      WRR              1
  Ethernet1   UC2      WRR              1
  Ethernet1   UC3      WRR              1
  Ethernet1   UC4      WRR              1
  Ethernet1   UC5      WRR              1
  Ethernet1   UC6      WRR              1
  Ethernet1   UC7      WRR              1
```

1.9 config interface trust-mode

Function

Run the **config interface trust-mode** command to configure the trust mode of interface.

Syntax

config interface trust-mode *interface-name* { **dscp** | **dot1p** }

Parameter Description

interface-name: interface name.

Usage Guidelines

NOTE:

- dot1p mode: Trusts the 802.1p priority level carried by the packet and maps priority based on this level.
- dscp mode: Trusts the DSCP (Differentiated Services Code Point) priority level carried by the packet and maps priority based on this level.
- When the port trust mode switches from dscp mode to dot1p mode, the dscp-to-tc mapping template applied to the port will be removed.
- When the port trust mode switches from dot1p mode to dscp mode, the port's dscp-to-tc mapping will use the default template.
- In dscp trust mode, if the packet has a VLAN tag, the dot1p value of the outbound packet will be changed based on the dscp-to-tc mapping.

Examples

```
admin@sonic:~$ show interfaces trust-mode
          Port      trust-mode
  ----------  ------------
    Ethernet1           dot1p
    Ethernet2            dscp
    Ethernet3            dscp
    Ethernet4            dscp
    Ethernet5            dscp
    Ethernet6            dscp
    Ethernet7            dscp
    Ethernet8            dscp
    Ethernet9            dscp
   Ethernet10            dscp
   Ethernet11           dscp
   Ethernet12            dscp
   Ethernet13            dscp
   Ethernet14            dscp
   Ethernet15            dscp
   Ethernet16            dscp
```

```
  Ethernet17            dscp
  Ethernet18            dscp
  Ethernet19            dscp
  Ethernet20            dscp
  Ethernet21            dscp
  Ethernet22            dscp
  Ethernet23            dscp
  Ethernet24            dscp
  Ethernet25            dscp
  Ethernet26            dscp
  Ethernet27            dscp
  Ethernet28            dscp
  Ethernet29            dscp
  Ethernet30            dscp
  Ethernet31            dscp
  Ethernet32            dscp
  Ethernet33            dscp
  Ethernet34            dscp
  Ethernet35            dscp
  Ethernet36            dscp
  Ethernet37            dscp
  Ethernet38            dscp
  Ethernet39            dscp
  Ethernet40            dscp
  Ethernet41            dscp
  Ethernet42            dscp
  Ethernet43            dscp
  Ethernet44            dscp
  Ethernet45            dscp
  Ethernet46            dscp
  Ethernet47            dscp
  Ethernet48            dscp
  Ethernet49            dscp
  Ethernet53            dscp
  Ethernet57            dscp
  Ethernet61            dscp
  Ethernet65            dscp
  Ethernet69            dscp
  Ethernet73            dscp
  Ethernet77            dscp

admin@sonic:~$ sudo config interface trust-mode Ethernet10 dot1p
admin@sonic:~$ show interfaces trust-mode
          Port      trust-mode
  ----------  ------------
   Ethernet1           dot1p
```

```
  Ethernet2          dscp
  Ethernet3          dscp
  Ethernet4          dscp
  Ethernet5          dscp
  Ethernet6          dscp
  Ethernet7          dscp
  Ethernet8          dscp
  Ethernet9          dscp
 Ethernet10         dot1p
 Ethernet11          dscp
 Ethernet12          dscp
 Ethernet13          dscp
 Ethernet14          dscp
 Ethernet15          dscp
 Ethernet16          dscp
 Ethernet17          dscp
 Ethernet18          dscp
 Ethernet19          dscp
 Ethernet20          dscp
 Ethernet21          dscp
 Ethernet22          dscp
 Ethernet23          dscp
 Ethernet24          dscp
 Ethernet25          dscp
 Ethernet26          dscp
 Ethernet27          dscp
 Ethernet28          dscp
 Ethernet29          dscp
 Ethernet30          dscp
 Ethernet31          dscp
 Ethernet32          dscp
 Ethernet33          dscp
 Ethernet34          dscp
 Ethernet35          dscp
 Ethernet36          dscp
 Ethernet37          dscp
 Ethernet38          dscp
 Ethernet39          dscp
 Ethernet40          dscp
 Ethernet41          dscp
 Ethernet42          dscp
 Ethernet43          dscp
 Ethernet44          dscp
 Ethernet45          dscp
 Ethernet46          dscp
 Ethernet47          dscp
```

```
  Ethernet48              dscp
  Ethernet49              dscp
  Ethernet53              dscp
  Ethernet57              dscp
  Ethernet61              dscp
  Ethernet65              dscp
  Ethernet69              dscp
  Ethernet73              dscp
  Ethernet77              dscp

admin@sonic:~$ show interfaces trust-mode Ethernet1
      Port         trust-mode
  ---------   ------------
  Ethernet1             dot1p
admin@sonic:~$ sudo config interface trust-mode Ethernet1 dscp
admin@sonic:~$ show interfaces trust-mode Ethernet1
      Port         trust-mode
  ---------   ------------
  Ethernet1              dscp
```

1.10 config qos clear

Function

Run the **config qos clear** command to clear all the QoS configuration from all the following QOS Tables in ConfigDB.

(1) TC_TO_PRIORITY_GROUP_MAP,

(2) MAP_PFC_PRIORITY_TO_QUEUE,

(3) TC_TO_QUEUE_MAP,

(4) DSCP_TO_TC_MAP,

(5) MPLS_TC_TO_TC_MAP,

(6) SCHEDULER,

(7) PFC_PRIORITY_TO_PRIORITY_GROUP_MAP,

(8) PORT_QOS_MAP,

(9) WRED_PROFILE,

(10) QUEUE,

(11) CABLE_LENGTH,

(12) BUFFER_POOL,

(13) BUFFER_PROFILE,

(14) BUFFER_PG,

(15) BUFFER_QUEUE

Syntax

config qos clear

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config qos clear
```

1.11 config qos map add

Function

Run the **config qos map add** command to configure qos map.

Syntax

config qos map add tc-to-pg *tc-to-pg-name tc-value pg-value*

config qos map add pfc-to-queue *pfc-to-queue-name pfc-value queue-value*

config qos map add dot1p-to-tc *dot1p-to-tc-name dot1p-value tc-value*

config qos map add dscp-to-tc *dscp-to-tc-name dscp-value tc-value*

config qos map add tc-and-color-to-dot1p *tc_and_color_to_dot1p_name tc_value color_value dot1p_value*

config qos map add tc-and-color-to-dscp *tc_and_color_to_dscp_name tc_value color_valuedscp_value*

config qos map add tc-to-queue *tc_to_queue_name tc_value queue_value*

config qos map add dscp-to-color *dscp_to_color_name dscp_value color_value*

config qos map add dot1p-to-color *dot1p_to_color_name dot1p_value color_value*

Parameter Description

N/A

Usage Guidelines

NOTE:

- When configuring tc-to-pg, pfc-to-queue, dot1p-to-tc, tc-and-color-to-dot1p, tc-and-color-to-dscp, dscp-to-tc, tc-to-queue, dscp-to-color, and dot1p-to-color types of message priority mapping templates, it is not supported to configure or delete operations on the default template.
- The tc-and-color-to-dot1p and tc-and-color-to-dscp types of message priority mapping do not take effect on M2-W6910-64C, M2-W6920-4S, and M2-W6920-32QC2X

devices.

- On M2-W6920-4S, M2-W6920-32QC2X, M2-W6930-64QC, and M2-W6520-24DC8QC devices, the tc-to-pg mapping only works in a one-to-one correspondence. That is, TC value 0 maps to priority group 0, TC value 1 maps to priority group 1, TC value 2 maps to priority group 2, TC value 3 maps to priority group 3, TC value 4 maps to priority group 4, TC value 5 maps to priority group 5, TC value 6 maps to priority group 6, and TC value 7 maps to priority group 7.
- For dscp-to-tc, dot1p-to-tc, tc-and-color-to-dot1p, and tc-and-color-to-dscp, unspecified keys will be mapped to 0. For example, when configuring a dscp-to-tc map: sudo config qos map add dscp-to-tc test 0-3 1; dscp 4-7 will be mapped to tc0.

Examples

```
admin@sonic:~$ sudo config qos map add tc-to-pg tc-pg 0-7 1
admin@sonic:~$ show qos map tc-to-pg
  TC_TO_PG_MAP: tc-pg
  ----------------------------
    tc      pg
  ----   ----
    0       1
    1       1
    2       1
    3       1
    4       1
    5       1
    6       1
    7       1

  Num of maps: 1

admin@sonic:~$ sudo config qos map add pfc-to-queue pfc-queue 0-7 5
admin@sonic:~$ show qos map pfc-to-queue
  PFC_TO_QUEUE_MAP: default
  ----------------------------
    pfc      queue
  -----   -------
      0           0
      1           1
      2           2
      3           3
      4           4
      5           5
      6           6
      7           7

  PFC_TO_QUEUE_MAP: pfc-queue
  ----------------------------
    pfc      queue
```

```
  -----  -------
      0        5
      1        5
      2        5
      3        5
      4        5
      5        5
      6        5
      7        5

  Num of maps: 2

admin@sonic:~$ sudo config qos map add dot1p-to-tc dot1p-tc 0-5 3
admin@sonic:~$ show qos map dot1p-to-tc
  DOT1P_TO_TC_MAP: default
  ----------------------------
    dot1p     tc
  -------  ----
        0      0
        1      1
        2      2
        3      3
        4      4
        5      5
        6      6
        7      7

  DOT1P_TO_TC_MAP: dot1p-tc
  ----------------------------
    dot1p     tc
  -------  ----
        0      3
        1      3
        2      3
        3      3
        4      3
        5      3

  Num of maps: 2

admin@sonic:~$ sudo config qos map add dscp-to-tc dscp-tc 5 2
admin@sonic:~$ sudo config qos map add dscp-to-tc dscp-tc 15 3
admin@sonic:~$ sudo config qos map add dscp-to-tc dscp-tc 28 5
admin@sonic:~$ show qos map dscp-to-tc
  DSCP_TO_TC_MAP: default
  ----------------------------
```

```
  dscp      tc
------   ----
     0       0
     1       0
     2       0
     3       0
     4       0
     5       0
     6       0
     7       0
     8       1
     9       1
    10       1
    11       1
    12       1
    13       1
    14       1
    15       1
    16       2
    17       2
    18       2
    19       2
    20       2
    21       2
    22       2
    23       2
    24       3
    25       3
    26       3
    27       3
    28       3
    29       3
    30       3
    31       3
    32       4
    33       4
    34       4
    35       4
    36       4
    37       4
    38       4
    39       4
    40       5
    41       5
    42       5
    43       5
```

```
      44       5
      45       5
      46       5
      47       5
      48       6
      49       6
      50       6
      51       6
      52       6
      53       6
      54       6
      55       6
      56       7
      57       7
      58       7
      59       7
      60       7
      61       7
      62       7
      63       7

  DSCP_TO_TC_MAP: dscp-tc
  ----------------------------
    dscp     tc
  ------   ----
       5      2
      15      3
      28      5

  Num of maps: 2

admin@sonic:~$ sudo config qos map add tc-and-color-to-dscp tc-color-dscp 0-5 green
2
admin@sonic:~$ show qos map tc-and-color-to-dscp
TC_AND_COLOR_TO_DSCP_MAP: tc-color-dscp
----------------------------
  tc      color      dscp
----   -------   ------
  0      green          2
  1      green          2
  2      green          2
  3      green          2
  4      green          2
  5      green          2

Num of maps: 1
```

```
admin@sonic:~$ sudo config qos map add tc-and-color-to-dot1p tc-color-dot1p 0-7
yellow 3
admin@sonic:~$ show qos map tc-and-color-to-dot1p
TC_AND_COLOR_TO_DOT1P_MAP: tc-color-dot1p
------------------------------
  tc      color      dot1p
----   -------   -------
  0     yellow          3
  1    yellow           3
  2     yellow          3
  3     yellow          3
  4     yellow          3
  5     yellow          3
  6     yellow          3
  7     yellow          3

Num of maps: 1
admin@sonic:~$ sudo config qos map add dscp-to-color dscp-color 0-7 green
admin@sonic:~$ show qos map dscp-to-color
DSCP_TO_COLOR_MAP: dscp-color
------------------------------
  dscp    color
------   -------
     0    green
     1   green
     2    green
     3    green
     4    green
     5    green
     6    green
     7   green

Num of maps: 1
admin@sonic:~$ sudo config qos map add dot1p-to-color dot1p-color 0-7 yellow
admin@sonic:~$ show qos map dot1p-to-color
DOT1P_TO_COLOR_MAP: dot1p-color
------------------------------
  dot1p    color
-------   -------
       0    yellow
       1   yellow
       2    yellow
       3    yellow
       4    yellow
       5    yellow
       6    yellow
```

```
    7   yellow

Num of maps: 1
```

1.12 config qos map apply

Function

Run the **config qos map apply** command to apply qos map to interface.

Syntax

config qos map apply tc-to-pg *interface-name tc-to-pg-name*

config qos map apply pfc-to-queue *interface-name pfc-to-queue-name*

config qos map apply dot1p-to-tc *interface-name dot1p-to-tc-name*

config qos map apply dscp-to-tc *interface-name dscp-to-tc-name*

config qos map apply tc-and-color-to-dot1p *interface-name tc-and-color-to-dot1p-name*

config qos map apply tc-and-color-to-dscp *interface-name tc-and-color-to-dscp-name*

config qos map apply tc-to-queue *interface-name tc-to-queue-name*

Parameter Description

interface-name: interface name.

Usage Guidelines

NOTE:

- When configuring tc-queue mapping on M2-W6010-48GT4X, M2-W6510-48V8C, M2-W6510-32C, M2-W6910-64C, M2-W6920-4S, M2-W6930-64QC, M2-W6520-24DC8QC, M2-W6510-48GT4V, and M2-W6920-32QC2X devices, it only takes effect on unicast queues and does not take effect on multicast queues.
- When configuring port priority trust mode as dot1p mode, you cannot apply the dscp-to-tc mapping template to the port.
- On M2-W6920-4S, M2-W6930-64QC, M2-W6520-24DC8QC, and M2-W6920-32QC2X devices, only one pfc-to-queue type of message priority mapping can be applied to the port at maximum.
- The tc-and-color-to-dscp and tc-and-color-to-dot1p types of message priority mapping do not take effect on M2-W6910-64C, M2-W6920-4S, and M2-W6920-32QC2X devices.
- When applying QoS mapping tables on M2-W6510-48GT4V, M2-W6510-32C, M2-W6510-48V8C, M2-W6910-64C, M2-W6920-4S, M2-W6920-32QC2X, M2-W6520-24DC8QC, and M2-W6930-64QC devices, the original mapping table will be deleted first before reissuing, which may cause momentary packet enqueue errors.

Examples

```
admin@sonic:~$ show interfaces qos map apply Ethernet2
  Port          Map                    Profile
  ---------   ----------------   ---------
  Ethernet2   dot1p_to_tc_map    default
              dscp_to_tc_map     default
              pfc_to_queue_map   default
              tc_to_queue_map    default
  admin@sonic:~$ sudo config qos map apply dscp-to-tc Ethernet2 dscp-tc
  admin@sonic:~$ show interfaces qos map apply Ethernet2
  Port          Map                    Profile
  ---------   ----------------   ---------
  Ethernet2   dot1p_to_tc_map    default
              dscp_to_tc_map     dscp-tc
              pfc_to_queue_map   default
              tc_to_queue_map    default

admin@sonic:~$ show interfaces qos map apply Ethernet5
  Port          Map                    Profile
  ---------   ----------------   ---------
  Ethernet5   dot1p_to_tc_map    default
              dscp_to_tc_map     default
              pfc_to_queue_map   default
              tc_to_queue_map    default
  admin@sonic:~$ sudo config qos map apply dot1p-to-tc Ethernet5 dot1p-tc
  admin@sonic:~$ show interfaces qos map apply Ethernet5
  Port          Map                    Profile
  ---------   ----------------   ---------
  Ethernet5   dot1p_to_tc_map    dot1p-tc
              dscp_to_tc_map     default
              pfc_to_queue_map   default
              tc_to_queue_map    default

admin@sonic:~$ sudo config qos map apply tc-and-color-to-dot1p Ethernet10 tc-color-
dot1p
admin@sonic:~$ show interfaces qos map apply Ethernet10
Port           Map                            Profile
----------   -------------------------   --------------
Ethernet10   dot1p_to_tc_map               default
             dscp_to_tc_map                default
             pfc_to_queue_map               default
             tc_and_color_to_dot1p_map   tc-color-dot1p
             tc_to_queue_map               default
admin@sonic:~$ sudo config qos map apply tc-and-color-to-dot1p Ethernet10 default
admin@sonic:~$ show interfaces qos map apply Ethernet10
Port           Map                    Profile
```

```
----------  ----------------  ---------
Ethernet10  dot1p_to_tc_map    default
            dscp_to_tc_map     default
            pfc_to_queue_map   default
            tc_to_queue_map    default
```

1.13 config qos map delete

Function

Run the **config qos map delete** command to delete qos map.

Syntax

config qos map delete tc-to-pg *tc_to_pg_name*

config qos map delete pfc-to-queue *pfc_to_queue_name*

config qos map delete dot1p-to-tc *dot1p_to_tc_name*

config qos map delete dscp-to-tc *dscp_to_tc_name*

config qos map delete tc-and-color-to-dot1p *tc_and_color_to_dot1p_name*

config qos map delete tc-and-color-to-dscp *tc_and_color_to_dscp_name*

config qos map delete tc-to-queue *tc_to_queue_name*

config qos map delete dscp-to-color *dscp_to_color_name*

config qos map delete dot1p-to-color *dot1p_to_color_name*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show qos map tc-to-queue
  TC_TO_QUEUE_MAP: default
  ----------------------------
    tc      queue
  ----   -------
    0          0
    1          1
    2          2
    3          3
    4          4
    5          5
    6          6
```

```
    7           7

  TC_TO_QUEUE_MAP: tc-queue
  ------------------------------
    tc      queue
  ----   -------
    0           2
    1           2
    2           2
    3           2

  Num of maps: 2

admin@sonic:~$ sudo config qos map delete tc-to-queue tc-queue
admin@sonic:~$ show qos map tc-to-queue
  TC_TO_QUEUE_MAP: default
  ------------------------------
    tc      queue
  ----   -------
    0           0
    1           1
    2           2
    3           3
    4           4
    5           5
    6           6
    7           7

  Num of maps: 1

admin@sonic:~$ show qos map pfc-to-queue
  PFC_TO_QUEUE_MAP: default
  ------------------------------
    pfc      queue
  -----   -------
      0           0
      1           1
      2           2
      3           3
      4           4
      5           5
      6           6
      7           7

  PFC_TO_QUEUE_MAP: pfc-queue
  ------------------------------
```

```
    pfc      queue
  -----   -------
      0          5
      1          5
      2          5
      3          5
      4          5
      5          5
      6          5
      7          5

  Num of maps: 2

admin@sonic:~$ sudo config qos map delete pfc-to-queue pfc-queue
admin@sonic:~$ show qos map pfc-to-queue
  PFC_TO_QUEUE_MAP: default
  ----------------------------
    pfc      queue
  -----   -------
      0          0
      1          1
      2          2
      3          3
      4          4
      5          5
      6          6
      7          7

  Num of maps: 1

admin@sonic:~$ show qos map dscp-to-color
DSCP_TO_COLOR_MAP: dscp-color
----------------------------
  dscp   color
------   -------
     0   green
     1   green
     2   green
     3   green
     4   green
     5   green
     6   green
     7   green

Num of maps: 1
```

```
admin@sonic:~$ sudo config qos map delete dscp-to-color dscp-color
admin@sonic:~$ show qos map dscp-to-color
Num of maps: 0
```

1.14 config qos reload

Function

Run the **config qos reload** command to reload the QoS configuration.

QoS configuration has got two sets of configurations.

(1) Generic QOS Configuration - This gives complete list of all possible QOS configuration. Its given in the file /usr/share/sonic/templates/qos_config.j2 in the device.

Reference: https://github.com/Azure/sonic-buildimage/blob/master/files/build_templates/qos_config.j2

Users have flexibility to have platform specific qos configuration by placing the qos_config.j2 file at /usr/share/sonic/device/<platform>/<hwsku>/.

If users want to modify any of this loaded QOS configuration, they can modify this file in the device and then issue the "config qos reload" command.

(2) Platform specific buffer configuration. Every platform has got platform specific and topology specific (T0 or T1 or T2) buffer configuration at /usr/share/sonic/device/<platform>/<hwsku>/buffers_defaults_tx.j2

In addition to platform specific configuration file, a generic configuration file is also present at /usr/share/sonic/templates/buffers_config.j2.

Reference: https://github.com/Azure/sonic-buildimage/blob/master/files/build_templates/buffers_config.j2

Users can either modify the platform specific configuration file, or the generic configuration file and then issue this "config qos reload" command.

These configuration files are already loaded in the device as part of the reboot process. In case if users wants to modify any of these configurations, they need to modify the appropriate QOS tables and fields in these files and then use this reload command.

This command uses those modified buffers.json.j2 file & qos.json.j2 file and reloads the new QOS configuration.

If users have not made any changes in these configuration files, this command need not be executed.

Some of the example QOS configurations that users can modify are given below.

(1) TC_TO_PRIORITY_GROUP_MAP

(2) MAP_PFC_PRIORITY_TO_QUEUE

(3) TC_TO_QUEUE_MAP

(4) DSCP_TO_TC_MAP

(5) MPLS_TC_TO_TC_MAP

(6) SCHEDULER

(7) PFC_PRIORITY_TO_PRIORITY_GROUP_MAP

(8) PORT_QOS_MAP

(9) WRED_PROFILE

(10) CABLE_LENGTH

(11) BUFFER_QUEUE

Syntax

config qos reload

Parameter Description

N/A

Usage Guidelines

N/A

Examples

In this example, it uses the buffers.json.j2 file and qos.json.j2 file from platform specific folders.

When there are no changes in the platform specific configutation files, they internally use the file "/usr/share/sonic/templates/buffers_config.j2" and "/usr/share/sonic/templates/qos_config.j2" to generate the configuration.

```
admin@sonic:~$ sudo config qos reload
Running command: /usr/local/bin/sonic-cfggen -d -t /usr/share/sonic/device/x86_64-micas_m2-w6510-48gt4v-r0/M2-W6510-48GT4V/buffers.json.j2 >/tmp/buffers.json
Running command: /usr/local/bin/sonic-cfggen -d -t /usr/share/sonic/device/x86_64-micas_m2-w6510-48gt4v-r0/M2-W6510-48GT4V/qos.json.j2 -y /etc/sonic/sonic_version.yml >/tmp/qos.json
Running command: /usr/local/bin/sonic-cfggen -j /tmp/buffers.json --write-to-db
Running command: /usr/local/bin/sonic-cfggen -j /tmp/qos.json --write-to-db
```

1.15 show acl counters

Function

Run the **show acl counters** command to display the ACL statistics counters.

Syntax

show acl counters [*table-name*] [*rule-name*]

Parameter Description

table-name: The name of the ACL table.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show acl counters
RULE NAME      TABLE NAME       PRIO    PACKETS COUNT    BYTES COUNT    UPDATE TIME
----------     ----------       ----    --------------    ------------   -------------
RULE_1         CUSTOM           9999          7890943    1010075392    2023-03-21 06:48:47
DEFAULT_RULE CUSTOM               1                0              0    1970-01-01 00:00:00
RULE_1         TEST             9999          7878959    1008541568    2023-03-21 06:48:47
DEFAULT_RULE TEST                 1                0              0    1970-01-01 00:00:00
```

```
admin@sonic:~$ show acl counters CUSTOM
RULE NAME     TABLE NAME       PRIO      PACKETS COUNT     BYTES COUNT    UPDATE TIME
----------   ------------   -----     -------------      ------------   --------------
RULE_1          CUSTOM       9999          50121379       6415571584    2023-03-21 06:48:57
DEFAULT_RULE    CUSTOM          1                0              0     1970-01-01 00:00:00
```

```
admin@sonic:~$ show acl counters TEST RULE_1
RULE NAME      TABLE NAME       PRIO    PACKETS COUNT    BYTES COUNT    UPDATE TIME
-----------   ------------   ------   ---------------   -------------   ----------------
RULE_1         TEST             9999          92335015     11818917376    2023-03-21 06:49:07
```

1.16 show acl rule

Function

Run the **show acl rule** command to display all the ACL rules present in all the ACL tables or only the rules present in specified table "TABLE_NAME" or only the rule matching the RULE_ID option.

Output from the command gives the following information about the rules.

- Table name - ACL table name to which the rule belongs to.
- Rule name - ACL rule name
- Priority - Priority for this rule.
- Action - Action to be performed if the packet matches with this ACL rule.

It can be:

  - "DROP"/"FORWARD"("ACCEPT" for control plane ACL)

Users can choose to have a default permit rule or default deny rule. In case of default "deny all" rule, add the permitted rules on top of the deny rule. In case of the default "permit all" rule, users can add the deny rules on top of it. If users have not configured any rule, SONiC allows all traffic (which is "permit all").

- Match - The fields from the packet header that need to be matched against the same present in the incoming traffic.

Syntax

show acl rule [*table-name*] [*rule-id*]

Parameter Description

table-name: The name of the ACL table.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show acl rule

Table      Rule            Priority    Action      Match
-------  -----------  -------  --------  ----------------------------------------
CUSTOM     RULE_1        9999       DROP         DST_MAC: 00:e0:f8:00:00:0d/ff:ff:ff:ff:ff:ff
                                                 ETHER_TYPE: 2048
                                                 LOG_ACTION: LOG_SYSLOG
                                                 SRC_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
CUSTOM     RULE_2        9998      FORWARD    DST_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
                                                 LOG_ACTION: LOG_SYSLOG
                                                 SRC_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
CUSTOM     DEFAULT_RULE   1       DROP         DST_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
                                                 SRC_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
TEST       RULE_1          9999       DROP         DST_IP: 0.0.0.0/0
                                                 LOG_ACTION: LOG_SYSLOG
                                                 SRC_IP: 0.0.0.0/0
TEST       RULE_2          9998      DROP         DST_IP: 0.0.0.0/0
                                                 LOG_ACTION: LOG_SYSLOG
                                                 SRC_IP: 0.0.0.32/32
TEST       DEFAULT_RULE   1           DROP         ETHER_TYPE: 2048
```

```
admin@sonic:~$ show acl rule CUSTOM
Table      Rule            Priority      Action       Match
-------  -----------  --------  --------  ----------------------------------------
CUSTOM   RULE_1        9999       DROP       DST_MAC: 00:e0:f8:00:00:0d/ff:ff:ff:ff:ff:ff
                                              ETHER_TYPE: 2048
                                              LOG_ACTION: LOG_SYSLOG
                                              SRC_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
CUSTOM   RULE_2         9998     FORWARD     DST_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
                                              LOG_ACTION: LOG_SYSLOG
                                              SRC_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
CUSTOM    DEFAULT_RULE   1         DROP       DST_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
                                              SRC_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
```

```
admin@sonic:~$ show acl rule CUSTOM RULE_1
Table      Rule      Priority      Action      Match
-------   ------   ----- --   ------     ----------------------------------------
CUSTOM   RULE_1   9999      DROP       DST_MAC: 00:e0:f8:00:00:0d/ff:ff:ff:ff:ff:ff
                                       ETHER_TYPE: 2048
                                       LOG_ACTION: LOG_SYSLOG
                                       SRC_MAC: 00:00:00:00:00:00/00:00:00:00:00:00
```

1.17 show acl table

Function

Run the **show acl table** command to display either all the ACL tables that are configured or only the specified "TABLE_NAME".

Output from the command displays the table name, type of the table, the cir and cbs, the dscp value, the status, the mode, the list of interface(s) to which the table is bound and the description about the table.

Syntax

show acl table [*table-name*]

Parameter Description

table-name: The name of the ACL table.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show acl table

Name    Type          Binding   Description   Stage   Dscp   CIR   CBS   Status   Mode
-----  ---------    -------  ----------  -----  -----  ---  ----  -----  --------
CTRL    CTRLPLANE      SSH        CTRL                                    N/A
CUSTOM   L2          Ethernet1   CUSTOM     ingress                    Active
TEST        L3          Ethernet1   TEST          ingress                    Active
Ethernet2
Ethernet3
TEST2       L3_QOS   Ethernet5   TEST2        ingress   10     100    200   Active
Ethernet6
TEST3       L3          Ethernet5   TEST3        egress                   Active    community
```

1.18 show buffer_pool persistent-watermark

Function

Run the **show buffer_pool persistent-watermark** command to display the user persistent-watermark for all the buffer pools.

Syntax

show buffer_pool persistent-watermark

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show buffer_pool persistent-watermark
  Shared pool maximum occupancy:
                        Pool      Bytes
  --------------------  -------
  ingress_lossless_pool        0
                lossy_pool     2464
```

1.19 show buffer_pool watermark

Function

Run the **show buffer_pool watermark** command to display the user watermark for all the buffer pools.

Syntax

show buffer_pool watermark

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show buffer_pool watermark
  Shared pool maximum occupancy:
                        Pool      Bytes
  --------------------  -------
```

```
ingress_lossless_pool          0
                lossy_pool     2464
```

1.20 show interfaces qos interface-rate-limit

Function

Run the **show interfaces qos interface-rate-limit** command to view the rate limiting of interface.

Syntax

show interfaces qos interface-rate-limit [*interface-name*]

Parameter Description

interface-name: interface name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces qos interface-rate-limit
  Port            pir            pbs
  ----------   ---------   -----
  Ethernet1    200000000   2000
  Ethernet2
  Ethernet3
  Ethernet4
  Ethernet5
  Ethernet6
  Ethernet7
  Ethernet8
  Ethernet9
  Ethernet10
  Ethernet11
  Ethernet12
  Ethernet13
  Ethernet14
  Ethernet15
  Ethernet16
  Ethernet17
  Ethernet18
  Ethernet19
  Ethernet20
  Ethernet21
  Ethernet22
  Ethernet23
```

```
  Ethernet24
  Ethernet25   100000000   1500
  Ethernet26
  Ethernet27
  Ethernet28
  Ethernet29
  Ethernet30
  Ethernet31
  Ethernet32
  Ethernet33
  Ethernet34
  Ethernet35
  Ethernet36
  Ethernet37
  Ethernet38
  Ethernet39
  Ethernet40
  Ethernet41
  Ethernet42
  Ethernet43
  Ethernet44
  Ethernet45
  Ethernet46
  Ethernet47
  Ethernet48
  Ethernet49
  Ethernet53
  Ethernet57
  Ethernet61
  Ethernet65
  Ethernet69
  Ethernet73
  Ethernet77

admin@sonic:~$ show interfaces qos interface-rate-limit Ethernet1
  Port          pir           pbs
  ---------   ---------   -----
  Ethernet1   200000000   2000
```

1.21 show interfaces qos map

Function

Run the **show interfaces qos map** command to view the priority mapping of packets applied to interface.

Syntax

show interfaces qos map apply *interface_name* [**tc-to-pg** | **pfc-to-queue** | **dot1p-to-tc** | **dscp-to-tc** | **tc-to-queue** | **tc-and-color-to-dscp** | **tc-and-color-to-dot1p** | **dscp-to-color** | **dot1p-to-color**]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces qos map apply Ethernet5
  Port          Map                    Profile
  ---------   ----------------   ---------
  Ethernet5   dot1p_to_tc_map     default
              dscp_to_tc_map      default
              pfc_to_queue_map    default
              tc_to_queue_map     default
admin@sonic:~$ show interfaces qos map apply Ethernet5 dscp-to-tc
  Port          Map                  Profile
  ---------   --------------   ---------
  Ethernet5   dscp_to_tc_map   default
```

1.22 show interfaces qos queue-rate-limit

Function

Run the **show interfaces qos queue-rate-limit** command to view the queue rate limiting on interface.

Syntax

show interfaces qos queue-rate-limit *interface_name* [*queue-id*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces qos queue-rate-limit Ethernet1
  Port          queue-id      cir           cbs      pir           pbs
  ---------   ----------   ---------   -----   ---------   -----
  Ethernet1   0             200000000   2000    300000000   3000
```

```
  Ethernet1   1
  Ethernet1   2
  Ethernet1   3
  Ethernet1   4
  Ethernet1   5
  Ethernet1   6
  Ethernet1   7

admin@sonic:~$ show interfaces qos queue-rate-limit Ethernet1 0
  Port          queue-id      cir           cbs      pir           pbs
  ---------   ----------   ---------   -----   ---------   -----
  Ethernet1   0             200000000   2000    300000000   3000
```

1.23 show interfaces trust-mode

Function

Run the **show interfaces trust-mode** command to view the trust mode of interface.

Syntax

show interfaces trust-mode [*interface_name*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show interfaces trust-mode
          Port      trust-mode
  ----------   ------------
    Ethernet1            dot1p
    Ethernet2             dscp
    Ethernet3             dscp
    Ethernet4             dscp
    Ethernet5             dscp
    Ethernet6             dscp
    Ethernet7             dscp
    Ethernet8             dscp
    Ethernet9             dscp
  Ethernet10             dscp
  Ethernet11            dscp
  Ethernet12             dscp
  Ethernet13             dscp
```

```
  Ethernet14            dscp
  Ethernet15            dscp
  Ethernet16            dscp
  Ethernet17            dscp
  Ethernet18            dscp
  Ethernet19            dscp
  Ethernet20            dscp
  Ethernet21            dscp
  Ethernet22            dscp
  Ethernet23            dscp
  Ethernet24            dscp
  Ethernet25            dscp
  Ethernet26            dscp
  Ethernet27            dscp
  Ethernet28            dscp
  Ethernet29            dscp
  Ethernet30            dscp
  Ethernet31            dscp
  Ethernet32            dscp
  Ethernet33            dscp
  Ethernet34            dscp
  Ethernet35            dscp
  Ethernet36            dscp
  Ethernet37            dscp
  Ethernet38            dscp
  Ethernet39            dscp
  Ethernet40            dscp
  Ethernet41            dscp
  Ethernet42            dscp
  Ethernet43            dscp
  Ethernet44            dscp
  Ethernet45            dscp
  Ethernet46            dscp
  Ethernet47            dscp
  Ethernet48            dscp
  Ethernet49            dscp
  Ethernet53            dscp
  Ethernet57            dscp
  Ethernet61            dscp
  Ethernet65            dscp
  Ethernet69            dscp
  Ethernet73            dscp
  Ethernet77            dscp

admin@sonic:~$ show interfaces trust-mode Ethernet5
        Port       trust-mode
```

```
---------  ------------
Ethernet5             dscp

admin@sonic:~$ sudo config qos map add tc-to-queue tc-queue 0-3 2
  admin@sonic:~$ show qos map tc-to-queue
  TC_TO_QUEUE_MAP: default
  ------------------------------
    tc      queue
  ----   -------
    0           0
    1           1
    2           2
    3           3
    4           4
    5           5
    6           6
    7           7

  TC_TO_QUEUE_MAP: tc-queue
  ------------------------------
    tc      queue
  ----   -------
    0           2
    1           2
    2           2
    3           2

  Num of maps: 2
```

1.24 show pfc asymmetric

Function

Run the **show pfc asymmetric** command to display the status of asymmetric PFC for all interfaces or a given interface.

Syntax

show pfc asymmetric [*interface-name*]

Parameter Description

interface-name: interface name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show pfc asymmetric

  Interface      Asymmetric
  -----------  ------------
  Ethernet0      off
  Ethernet2      off
  Ethernet4      off
  Ethernet6      off
  Ethernet8      off
  Ethernet10     off
  Ethernet12     off
  Ethernet14     off

admin@sonic:~$ show pfc asymmetric Ethernet0

  Interface      Asymmetric
  -----------  ------------
  Ethernet0      off
```

1.25 show pfc counters

Function

Run the **show pfc counters** command to display the details of Rx & Tx priority-flow-control (pfc) for all ports. This command can be used to clear the counters using -c option.

Syntax

show pfc counters

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show pfc counters
    Port Rx      PFC0      PFC1      PFC2      PFC3      PFC4      PFC5      PFC6      PFC7
    -----------  ------  ------  ------  ------  ------  ------  ------  ------
    Ethernet0         0         0         0         0         0         0         0         0
    Ethernet4         0         0         0         0         0         0         0         0
    Ethernet8         0         0         0         0         0         0         0         0
    Ethernet12        0         0         0         0         0         0         0         0
```

```
    Port Tx     PFC0     PFC1     PFC2     PFC3     PFC4     PFC5     PFC6     PFC7
    -----------  ------  ------  ------  ------  ------  ------  ------  ------
    Ethernet0        0        0        0        0        0        0        0        0
    Ethernet4        0        0        0        0        0        0        0        0
    Ethernet8        0        0        0        0        0        0        0        0
Ethernet12        0        0        0        0        0        0        0        0
...
```

Note
PFC counters can be cleared by the user with the following command.

```
admin@sonic:~$ sonic-clear pfccounters
```

1.26 show pfc priority

Function

Run the **show pfc priority** command to display the lossless priorities for all interfaces or a given interface.

Syntax

show pfc priority [*interface-name*]

Parameter Description

interface-name: interface name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show pfc priority

  Interface      Lossless priorities
  -----------   ---------------------
  Ethernet0      3,4
  Ethernet2      3,4
  Ethernet8      3,4
  Ethernet10     3,4
  Ethernet16     3,4

admin@sonic:~$ show pfc priority Ethernet0

  Interface      Lossless priorities
```

```
-----------  --------------------
Ethernet0    3,4
```

1.27 show priority-group

Function

Run the **show priority-group** command to display The user watermark or persistent-watermark for the Ingress "headroom" or "shared pool occupancy" per priority-group for all ports. Dropped packets per priority-group for all ports.

Syntax

show priority-group { **watermark** | **persistent-watermark** } { **headroom** | **shared** }

show priority-group drop counters

Parameter Description

N/A

Usage Guidelines

In addition to user watermark("show queue|priority-group watermark ..."), a persistent watermark is available.

It hold values independently of user watermark. This way user can use "user watermark" for debugging, clear it, etc, but the "persistent watermark" will not be affected.

Examples

```
admin@sonic:~$ show priority-group watermark shared
  Ingress shared pool occupancy per PG:
        Port      PG0      PG1      PG2      PG3      PG4      PG5      PG6      PG7
  -----------  -------  -------  -------  -------  -------  -------  -------  -------
     Ethernet0        0        0        0        0        0        0        0        0
     Ethernet4        0        0        0        0        0        0        0        0
     Ethernet8        0        0        0        0        0        0        0        0
Ethernet12        0        0        0        0        0        0        0        0
```

Ingress headroom per PG.

```
admin@sonic:~$ show priority-group watermark headroom
```

Ingress shared pool occupancy per PG.

```
admin@sonic:~$ show priority-group persistent-watermark shared
```

Ingress headroom per PG.

```
admin@sonic:~$ show priority-group persistent-watermark headroom
```

Ingress dropped packets per PG.

```
admin@sonic:~$ show priority-group drop counters
```

```
  Ingress PG dropped packets:
      Port      PG0      PG1      PG2      PG3      PG4      PG5      PG6      PG7
-----------  -------  -------  -------  -------  -------  -------  -------  -------
     Ethernet0        0        0        0        0        0        0        0        0
     Ethernet4        0        0        0        0        0        0        0        0
     Ethernet8        0        0        0        0        0        0        0        0
     Ethernet12       0        0        0        0        0        0        0        0
```

1.28 show qos map

Function

Run the **show qos map** command to view the packet priority mapping.

Syntax

show qos map { **tc-to-pg** | **pfc-to-queue** | **dot1p-to-tc** | **dscp-to-tc** | **tc-to-queue** | **tc-and-color-to-dscp** | **tc-and-color-to-dot1p** | **dscp-to-color** | **dot1p-to-color** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show qos map tc-to-pg
  TC_TO_PG_MAP: tc-pg
  ------------------------------
    tc      pg
  ----   ----
    0       1
    1       1
    2       1
    3       1
    4       1
    5       1
    6       1
    7       1

  Num of maps: 1

admin@sonic:~$ show qos map pfc-to-queue
  PFC_TO_QUEUE_MAP: default
  ------------------------------
    pfc      queue
  -----   -------
```

```
      0            0
      1            1
      2            2
      3            3
      4            4
      5            5
      6            6
      7            7

  Num of maps: 1

admin@sonic:~$ show qos map dot1p-to-tc
  DOT1P_TO_TC_MAP: default
  ----------------------------
    dot1p      tc
  -------   ----
        0       0
        1       1
        2       2
        3       3
        4       4
        5       5
        6       6
        7       7

  Num of maps: 1

admin@sonic:~$ show qos map dscp-to-tc
  DSCP_TO_TC_MAP: default
  ----------------------------
    dscp      tc
  ------   ----
       0       0
       1       0
       2       0
       3       0
       4       0
       5       0
       6       0
       7       0
       8       1
       9       1
      10       1
      11       1
      12       1
      13       1
```

```
14      1
15      1
16      2
17      2
18      2
19      2
20      2
21      2
22      2
23      2
24      3
25      3
26      3
27      3
28      3
29      3
30      3
31      3
32      4
33      4
34      4
35      4
36      4
37      4
38      4
39      4
40      5
41      5
42      5
43      5
44      5
45      5
46      5
47      5
48      6
49      6
50      6
51      6
52      6
53      6
54      6
55      6
56      7
57      7
58      7
59      7
```

```
      60       7
      61       7
      62       7
      63       7

  Num of maps: 1

admin@sonic:~$ show qos map tc-to-queue
  TC_TO_QUEUE_MAP: default
  ----------------------------
    tc      queue
  ----   -------
    0           0
    1           1
    2           2
    3           3
    4           4
    5           5
    6           6
    7           7

  Num of maps: 1

admin@sonic:~$ show qos map tc-and-color-to-dscp
TC_AND_COLOR_TO_DSCP_MAP: tc-color-dscp
-----------------------------
  tc      color      dscp
----   -------   ------
  0      green          2
  1      green          2
  2      green          2
  3      green          2
  4      green          2
  5      green          2

Num of maps: 1
admin@sonic:~$ show qos map tc-and-color-to-dot1p
TC_AND_COLOR_TO_DOT1P_MAP: tc-color-dot1p
-----------------------------
  tc      color      dot1p
----   -------   -------
  0     yellow          3
  1     yellow          3
  2     yellow          3
  3     yellow          3
  4     yellow          3
```

```
  5    yellow          3
  6    yellow          3
  7    yellow          3

Num of maps: 1
admin@sonic:~$ show qos map dscp-to-color
DSCP_TO_COLOR_MAP: dscp-color
------------------------------
  dscp   color
------   -------
     0   green
     1   green
     2   green
     3   green
     4   green
     5   green
     6   green
     7   green

Num of maps: 1
admin@sonic:~$ show qos map dot1p-to-color
DOT1P_TO_COLOR_MAP: dot1p-color
------------------------------
  dot1p   color
-------   -------
       0   yellow
       1   yellow
       2   yellow
       3   yellow
       4   yellow
       5   yellow
       6   yellow
       7   yellow

Num of maps: 1
```

1.29 show queue counters

Function

Run the **show queue counters** command to display packet and byte counters for all queues of all ports or one specific-port given as argument.

Note
That port specific clear is not supported.

Syntax

show queue counters [*interface_name*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show queue counters
      Port      TxQ      Counter/pkts      Counter/bytes      Drop/pkts      Drop/bytes
----------  -------  --------------  ---------------  -----------  ------------
 Ethernet1      UC0                 0                 0            0             0
 Ethernet1      UC1                 0                 0            0             0
 Ethernet1      UC2                 0                 0            0             0
 Ethernet1      UC3                 0                 0            0             0
 Ethernet1      UC4                 0                 0            0             0
 Ethernet1      UC5                 0                 0            0             0
 Ethernet1      UC6                 0                 0            0             0
 Ethernet1      UC7                 0                 0            0             0
 Ethernet1      UC8                 0                 0            0             0
 Ethernet1      UC9                 0                 0            0             0
 Ethernet1     MC10                 0                 0            0             0
 Ethernet1     MC11                 0                 0            0             0
 Ethernet1     MC12                 0                 0            0             0
 Ethernet1     MC13                 0                 0            0             0
 Ethernet1     MC14                 0                 0            0             0
 Ethernet1     MC15                 0                 0            0             0
 Ethernet1     MC16                 0                 0            0             0
 Ethernet1     MC17                 0                 0            0             0
 Ethernet1     MC18                 0                 0            0             0
 Ethernet1     MC19                 0                 0            0             0
 ...
      Port      TxQ      Counter/pkts      Counter/bytes      Drop/pkts      Drop/bytes
----------  -------  --------------  ---------------  -----------  ------------
Ethernet55      UC0                 0                 0            0             0
Ethernet55      UC1                 0                 0            0             0
Ethernet55      UC2                 0                 0            0             0
Ethernet55      UC3                 0                 0            0             0
Ethernet55      UC4                 0                 0            0             0
Ethernet55      UC5                 0                 0            0             0
Ethernet55      UC6                 0                 0            0             0
Ethernet55      UC7                 0                 0            0             0
Ethernet55      UC8                 0                 0            0             0
```

```
Ethernet55     UC9            0              0              0              0
Ethernet55     MC10           0              0              0              0
Ethernet55     MC11           0              0              0              0
Ethernet55     MC12           0              0              0              0
Ethernet55     MC13           0              0              0              0
Ethernet55     MC14           0              0              0              0
Ethernet55     MC15           0              0              0              0
Ethernet55     MC16           0              0              0              0
Ethernet55     MC17           0              0              0              0
Ethernet55     MC18           0              0              0              0
Ethernet55     MC19           0              0              0              0
...
```

Optionally, you can specify an interface name in order to display only that particular interface.

```
admin@sonic:~$ show queue counters Ethernet2
      Port    TxQ    Counter/pkts    Counter/bytes    Drop/pkts    Drop/bytes
---------  -----  --------------  ---------------  -----------  ------------
 Ethernet2    UC0              0                0            0             0
 Ethernet2    UC1              0                0            0             0
 Ethernet2    UC2              0                0            0             0
 Ethernet2    UC3              0                0            0             0
 Ethernet2    UC4              0                0            0             0
 Ethernet2    UC5              0                0            0             0
 Ethernet2    UC6              0                0            0             0
 Ethernet2    UC7              0                0            0             0
 Ethernet2    UC8              0                0            0             0
 Ethernet2    UC9              0                0            0             0
 Ethernet2   MC10              0                0            0             0
 Ethernet2   MC11              0                0            0             0
 Ethernet2   MC12              0                0            0             0
 Ethernet2   MC13              0                0            0             0
 Ethernet2   MC14              0                0            0             0
 Ethernet2   MC15              0                0            0             0
 Ethernet2   MC16              0                0            0             0
 Ethernet2   MC17              0                0            0             0
 Ethernet2   MC18              0                0            0             0
 Ethernet2   MC19              0                0            0             0
```

Note

Queue counters can be cleared by the user with the following command.

```
admin@sonic:~$ sonic-clear queuecounters
```

1.30 show queue persistent-watermark

Function

Run the **show queue persistent-watermark** command to display the user persistet-watermark for the queues (Egress shared pool occupancy per queue) for either the unicast queues or multicast queues for all ports.

Syntax

show queue persistent-watermark { **unicast** | **multicast** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show queue persistent-watermark unicast
  Egress shared pool occupancy per unicast queue:
       Port      UC0      UC1      UC2      UC3      UC4      UC5      UC6      UC7
  -----------  -------  -------  -------  -------  -------  -------  -------  -------
     Ethernet0      N/A      N/A      N/A      N/A      N/A      N/A      N/A      N/A
     Ethernet4      N/A      N/A      N/A      N/A      N/A      N/A      N/A      N/A
     Ethernet8      N/A      N/A      N/A      N/A      N/A      N/A      N/A      N/A
Ethernet12      N/A      N/A      N/A      N/A      N/A      N/A      N/A      N/A
```

Egress shared pool occupancy per multicast queue.

```
admin@sonic:~$ show queue persistent-watermark multicast
```

Note
"user watermark", "persistent watermark" and "ingress dropped packets" can be cleared by user.

```
admin@sonic:~$ sonic-clear queue persistent-watermark unicast
admin@sonic:~$ sonic-clear queue persistent-watermark multicast
admin@sonic:~$ sonic-clear priority-group persistent-watermark shared
admin@sonic:~$ sonic-clear priority-group persistent-watermark headroom
admin@sonic:~$ sonic-clear priority-group drop counters
```

1.31 show queue schedule

Function

Run the **show queue schedule** command to view the scheduling policy of the output queue of ports.

Syntax

show queue schedule [*interface-name*]

Parameter Description

Interface-name: Interface name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show queue schedule
  Port          TxQ     Mode        Weight
  ---------   -----   ------   --------
  Ethernet1   UC0      WRR              1
  Ethernet1   UC1     WRR              1
  Ethernet1   UC2      WRR              1
  Ethernet1   UC3      WRR              1
  Ethernet1   UC4      WRR              1
  Ethernet1   UC5      WRR              1
  Ethernet1   UC6      WRR              1
  Ethernet1   UC7      WRR              1
  ...
  Port          TxQ     Mode        Weight
  ----------   -----   ------   --------
  Ethernet48   UC0      WRR              1
  Ethernet48   UC1     WRR              1
  Ethernet48   UC2      WRR              1
  Ethernet48   UC3      WRR              1
  Ethernet48   UC4      WRR              1
  Ethernet48   UC5      WRR              1
  Ethernet48   UC6      WRR              1
  Ethernet48   UC7      WRR              1
  ...

admin@sonic:~$ show queue schedule Ethernet1
  Port          TxQ     Mode        Weight
  ---------   -----   ------   --------
  Ethernet1   UC0      WRR              1
```

```
  Ethernet1   UC1     WRR              1
  Ethernet1   UC2     WRR              1
  Ethernet1   UC3     WRR              1
  Ethernet1   UC4     WRR              1
  Ethernet1   UC5     WRR              1
  Ethernet1   UC6     WRR              1
  Ethernet1   UC7     WRR              1
```

1.32 show queue watermark

Function

Run the **show queue watermark** command to display the user watermark for the queues (Egress shared pool occupancy per queue) for either the unicast queues or multicast queues for all ports.

Syntax

show queue watermark { **multicast** | **unicast** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show queue watermark unicast
  Egress shared pool occupancy per unicast queue:
          Port     UC0     UC1     UC2     UC3     UC4     UC5     UC6     UC7
  -----------  -----  -----  -----  -----  -----  -----  -----  -----
     Ethernet0       0       0       0       0       0       0       0       0
     Ethernet4       0       0       0       0       0       0       0       0
     Ethernet8       0       0       0       0       0       0       0       0
    Ethernet12       0       0       0       0       0       0       0       0
```

Egress shared pool occupancy per multicast queue.

```
admin@sonic:~$ show queue watermark multicast
```

1.33 sonic-clear queue counters

Function

Run the **sonic-clear queue counters** command to clear the statistics of packets in the queue.

Syntax

sonic-clear queue counters

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show queue counters Ethernet50
      Port    TxQ    Counter/pkts    Counter/bytes    Drop/pkts    Drop/bytes
----------  -----  --------------  ---------------  -----------  ------------
 Ethernet50    UC0             219            25035            0             0
 Ethernet50    UC1               0                0            0             0
 Ethernet50    UC2               0                0            0             0
 Ethernet50    UC3               0                0            0             0
 Ethernet50    UC4               0                0            0             0
 Ethernet50    UC5               0                0            0             0
 Ethernet50    UC6               0                0            0             0
 Ethernet50    UC7               0                0            0             0
 Ethernet50    UC8               0                0            0             0
 Ethernet50    UC9               0                0            0             0
 Ethernet50   MC10               0                0            0             0
 Ethernet50   MC11               0                0            0             0
 Ethernet50   MC12               0                0            0             0
 Ethernet50   MC13               0                0            0             0
 Ethernet50   MC14               0                0            0             0
 Ethernet50   MC15               0                0            0             0
 Ethernet50   MC16               0                0            0             0
 Ethernet50   MC17               0                0            0             0
 Ethernet50   MC18               0                0            0             0
 Ethernet50   MC19               0                0            0             0

admin@sonic:~$ sudo sonic-clear queue counters
admin@sonic:~$ show queue counters Ethernet50
      Port    TxQ    Counter/pkts    Counter/bytes    Drop/pkts    Drop/bytes
----------  -----  --------------  ---------------  -----------  ------------
 Ethernet50    UC0               0                0            0             0
 Ethernet50    UC1               0                0            0             0
 Ethernet50    UC2               0                0            0             0
 Ethernet50    UC3               0                0            0             0
 Ethernet50    UC4               0                0            0             0
 Ethernet50    UC5               0                0            0             0
 Ethernet50    UC6               0                0            0             0
```

Ethernet50	UC7	0	0	0	0
Ethernet50	UC8	0	0	0	0
Ethernet50	UC9	0	0	0	0
Ethernet50	MC10	0	0	0	0
Ethernet50	MC11	0	0	0	0
Ethernet50	MC12	0	0	0	0
Ethernet50	MC13	0	0	0	0
Ethernet50	MC14	0	0	0	0
Ethernet50	MC15	0	0	0	0
Ethernet50	MC16	0	0	0	0
Ethernet50	MC17	0	0	0	0
Ethernet50	MC18	0	0	0	0
Ethernet50	MC19	0	0	0	0

1 IGMP Snooping Commands

Command	Function
config igmp-snooping	Configure IGMP Snooping VLAN.
config igmp-snooping fast-leave	Configure VLAN-based IGMP Snooping fast leave.
config igmp-snooping last-member-query-interval	Configure a VLAN-based IGMP Snooping last member query interval in milliseconds.
config igmp-snooping mrouter	Configure VLAN-based mrouter interface.
config igmp-snooping querier	Configure VLAN-based IGMP Snooping querier.
config igmp-snooping query-interval	Configure a VLAN-based IGMP Snooping query interval in seconds.
config igmp-snooping query-max-response-time	Configure the maximum response time of VLAN-based IGMP Snooping query in seconds.
config igmp-snooping static-group	Configure VLAN-based static member interfaces.
config igmp-snooping version	Configure a VLAN-based IGMP Snooping version.
show igmp-snooping all	Display IGMP Snooping configuration on all VLANs.
show igmp-snooping groups all	Display L2MC entries on all VLANs.
show igmp-snooping groups vlan	Display L2MC entries specific to a VLAN.
show igmp-snooping vlan	Display IGMP Snooping configuration specific to a VLAN.

1.1 config igmp-snooping

Function

Run the **config igmp-snooping** command to configure IGMP Snooping VLAN.

Devices running IGMP Snooping provide multicast services based on VLANs. Multicast streams can only be forwarded within the VLAN to which they belong, and user hosts can only apply for multicast streams within the VLAN to which they belong.

Syntax

config igmp-snooping [*OPTIONS*] { **enable** | **disable** } *vlan-id*

Parameter Description

OPTIONS:

- -s, --redis-unix-socket-path TEXT:

  unix socket path for redis connection
- -h, -?, --help:

  Show this message and exit.

Vlan-id: VLAN ID , for example, 10.

enable: Enable IGMP for a VLAN.

disable: Disable IGMP for a VLAN.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config igmp-snooping enable 10
admin@sonic:~$ sudo config igmp-snooping disable 10
```

1.2 config igmp-snooping fast-leave

Function

Run the **config igmp-snooping fast-leave** command to configure VLAN-based IGMP Snooping fast leave.

After the port fast leave function is enabled, when a port of the device receives a Leave message (including IGMPv2 Leave message and IGMPv3 INCLUDE type Report message without any source address), it is immediately removed from the corresponding forwarding entry for a multicast group. After that, when the device receives the corresponding specific group query packets and multicast data packets, the device will no longer forward them to the port.

Syntax

config igmp-snooping fast-leave { **enable** | **disable** } *vlan-id*

Parameter Description

Vlan-id: VLAN ID , for example, 10.

enable: Enable IGMP for a VLAN.

disable: Disable IGMP for a VLAN.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config igmp-snooping fast-leave enable 10
admin@sonic:~$ sudo config igmp-snooping fast-leave disable 10
```

1.3 config igmp-snooping last-member-query-interval

Function

Run the **config igmp-snooping last-member-query-interval** command to configure a VLAN-based IGMP Snooping last member query interval in milliseconds.

When the querier receives an IGMP leave message, it verifies that the multicast group has no remaining listeners by sending a set of group-specific queries at a configured interval. If the querier does not receive a response to the query, it deletes the multicast and stops forwarding multicast traffic. This command configures the interval for sending specific multicast or specific group source query messages to the interface.

Syntax

config igmp-snooping last-member-query-interval *vlan-id time*

Parameter Description

Vlan-id: VLAN ID, for example, 10.

time: IGMP Snooping last member query interval in milliseconds, the value range is from 100 to 25500.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config igmp-snooping last-member-query-interval 10 1000
```

1.4 config igmp-snooping mrouter

Function

Run the **config igmp-snooping mrouter** command to configure VLAN-based mrouter interface.

The role of the routing connection port is to receive upstream multicast data and guide the forwarding of IGMP Report/Leave messages. When an interface is configured as a static routing interface, the interface will never age out and can forward IGMP Report/Leave messages to the upstream IGMP querier stably for a long time.

Syntax

config igmp-snooping mrouter { **add** | **del** } *vlan-id interface-name*

Parameter Description

addl: Add router interface for VLAN.

del: Remove router interface for VLAN.

Vlan-id: VLAN ID, for example, 10.

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config igmp-snooping mrouter add 10 Ethernet1
admin@sonic:~$ sudo config igmp-snooping mrouter del 10 Ethernet1
```

1.5 config igmp-snooping querier

Function

Run the **config igmp-snooping querier** command to configure VLAN-based IGMP Snooping querier.

On a Layer 3 multicast network, the Layer 3 multicast device acts as a querier and runs the IGMP protocol to maintain group membership. Layer 2 multicast devices only need to listen to IGMP messages to establish and maintain forwarding entries to implement Layer 2 multicast. However, in a scenario where the multicast source and the user host are on the same Layer 2 network, the query item function cannot be implemented because the Layer 2 device does not support IGMP. To solve this problem, enable the IGMP Snooping querier on the Layer 2 device, send IGMP Query messages to the user host instead of the Layer 3 multicast device, and monitor and maintain the IGMP Report messages answered by the user to establish Layer 2 multicast forwarding entry.

Syntax

config igmp-snooping querier { **enable** | **disable** } *vlan-id*

Parameter Description

Vlan-id: VLAN ID , for example, 10.

enable: Enable IGMP Querier for a VLAN.

disable: Disable IGMP fast-leave for a VLAN.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config igmp-snooping querier enable 10
admin@sonic:~$ sudo config igmp-snooping querier disable 10
```

1.6 config igmp-snooping query-interval

Function

Run the **config igmp-snooping query-interval** command to configure a VLAN-based IGMP Snooping query interval in seconds.

The IGMP Snooping querier sends query messages periodically.

Syntax

config igmp-snooping query-interval *vlan-id time*

Parameter Description

Vlan-id: VLAN ID , for example, 10.

time: IGMP Snooping query interval, The value rangeis from 1 to 18000.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config igmp-snooping query-interval 10 125
```

1.7 config igmp-snooping query-max-response-time

Function

Run the **config igmp-snooping query-max-response-time** command to configure the maximum response time of VLAN-based IGMP Snooping query in seconds.

After receiving the query message from the device, the host directly connected to the device needs to respond to the Report message within the maximum response time. This function allows you to configure the maximum response time on the device, requiring the

host to respond to the Report message after receiving the query message sent by the device. If the host does not respond to the Report message within the maximum response time, the device will consider that there are no group members in the directly connected network segment and delete the group information.

Syntax

config igmp-snooping query-max-response-time *vlan-id time*

Parameter Description

Vlan-id: VLAN ID, for example, 10.

time: Maximum response time of IGMP Snooping query, the value range is from 1 to 25.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config igmp-snooping query-max-response-time 10 10
```

1.8 config igmp-snooping static-group

Function

Run the **config igmp-snooping static-group** command to configure VLAN-based static member interfaces.

Configure the interface connected with the member host as a static member port. Then the member host can receive the multicast stream of the specified multicast group regardless of whether it joins the multicast group, and the static member port will never age out.

Syntax

config igmp-snooping static-group { **add** | **del** } *vlan-id interface-name ip-addr*

Parameter Description

addl: Add static-group for VLAN.

del: Remove static-group for VLAN.

Vlan-id: VLAN ID, for example, 10.

interface-name: Interface name, for example, Ethernet1.

ip-addr:

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ config igmp-snooping static-group add 10 Ethernet2 224.1.1.1
admin@sonic:~$ config igmp-snooping static-group del 10 Ethernet2 224.1.1.1
```

1.9 config igmp-snooping version

Function

Run the **config igmp-snooping version** command to configure a VLAN-based IGMP Snooping version.

Configuring the IGMP Snooping version can specify the version of IGMP messages that IGMP Snooping can process. IGMP Snooping v3 can process all information of IGMPv1, IGMPv2 and IGMPv3 messages. IGMP Snooping v2 only performs simple processing on IGMPv3 and does not process the source information carried in the packets.

Syntax

config igmp-snooping version *vlan-id version*

Parameter Description

Vlan-id: VLAN ID, for example, 10.

version: IGMP Snooping protocol version, the value range is from 1 to 3.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config igmp-snooping version 10 2
```

1.10 show igmp-snooping all

Function

Run the **show igmp-snooping all** command to display IGMP Snooping configuration on all VLANs.

Syntax

show igmp-snooping all

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
root@sonic:/home/admin/ll# show igmp-snooping all

    Vlan ID: 1
    Multicast Router ports:
    Querier - false
    IGMP Operation mode: IGMPv2
    Is Fast-Leave Enabled: Disabled
    Max Response time = 10
    Query Interval = 125
    Last Member Query Interval = 1000


    Vlan ID: 10
    Multicast Router ports: Ethernet1
    Querier - false
    IGMP Operation mode: IGMPv2
    Is Fast-Leave Enabled: Disabled
    Max Response time = 10
    Query Interval = 125
    Last Member Query Interval = 1000

    Total number of entries:      2
```

1.11 show igmp-snooping groups all

Function

Run the **show igmp-snooping groups all** command to display L2MC entries on all VLANs.

Syntax

show igmp-snooping groups all

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show igmp-snooping groups all

    Vlan ID : 1
    --------------
    Total number of entries: 0
```

```
Vlan ID : 10
--------------
Mrouters Ports:
    Ethernet1(static)
1 (*, 224.1.1.1)
    Members Ports:
        Ethernet2(static)
Total number of entries: 1
```

1.12 show igmp-snooping groups vlan

Function

Run the **show igmp-snooping groups vlan** command to display L2MC entries specific to a VLAN.

Syntax

show igmp-snooping groups vlan *vlan-id*

Parameter Description

vlan-id: VLAN ID, for example, 10.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show igmp-snooping groups vlan 10

    Vlan ID : 10
    --------------
    Mrouters Ports:
        Ethernet1(static)
    1 (*, 224.1.1.1)
        Members Ports:
            Ethernet2(static)
    Total number of entries: 1
```

1.13 show igmp-snooping vlan

Function

Run the **show igmp-snooping vlan** command to display IGMP Snooping configuration specific to a VLAN.

Syntax

show igmp-snooping vlan *vlan-id*

Parameter Description

vlan-id: VLAN ID, for example, 10.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show igmp-snooping vlan 10
    Vlan ID: 10
    Multicast Router ports: Ethernet1
    Querier - false
    IGMP Operation mode: IGMPv2
    Is Fast-Leave Enabled: Disabled
    Max Response time = 10
    Query Interval = 125
    Last Member Query Interval = 1000
```

1 AAA Commands

Command	Function
aaa authentication failthrough	Either enable or disable the failthrough option.
aaa authentication login	Either configure whether AAA should use local database or remote tacacs+ database for user authentication.
config username	Configure a local user. It is an interactive command. An interactive page will be displayed asking you to enter the password.
remove username	Delete a local user.
show aaa	Display the AAA settings currently present in the network node.
show username	Shows the configured users, including local users, tacacs users and radius users, and so on.

1.1 aaa authentication failthrough

Function

Run the **aaa authentication failthrough** command to either enable or disable the failthrough option.

Syntax

sudo config aaa authentication failthrough { **enable** | **disable** | **default** }

Parameter Description

enable: This allows the AAA module to process with local authentication if remote authentication fails.

disable: This disallows the AAA module to proceed further if remote authentication fails.

default: This re-configures the default value, which is "enable".

Usage Guidelines

This command is useful when user has configured more than one tacacs+ server and when user has enabled tacacs+ authentication.

When authentication request to the first server fails, this configuration allows to continue the request to the next server.

When this configuration is enabled, authentication process continues through all servers configured.

When this is disabled and if the authentication request fails on first server, authentication process will stop and the login will be disallowed.

Examples

```
admin@sonic:~$ sudo config aaa authentication failthrough enable
```

1.2 aaa authentication login

Function

Run the **aaa authentication login** command to either configure whether AAA should use local database or remote tacacs+ database for user authentication.

By default, AAA uses local database for authentication. New users can be added/deleted using the linux commands (Note that the configuration done using linux commands are not preserved during reboot).

Syntax

sudo config aaa authentication login { **tacacs+** | **local** | **default** }

Parameter Description

tacacs+: Enables remote authentication based on tacacs+.

local: Disables remote authentication and uses local authentication.

default: Reset back to default value, which is only "local" authentication.

Usage Guidelines

Admin can enable remote tacacs+ server based authentication by selecting the AUTH_PROTOCOL as tacacs+ in this command.

Admins need to configure the tacacs+ server accordingly and ensure that the connectivity to tacacas+ server is available via the management interface.

Once if the admins choose the remote authentication based on tacacs+ server, all user logins will be authenticated by the tacacs+ server.

If the authentication fails, AAA will check the "failthrough" configuration and authenticates the user based on local database if failthrough is enabled.

Examples

```
admin@sonic:~$ sudo config aaa authentication login tacacs+
```

1.3 config username

Function

Run the **config username** command to configure a local user. It is an interactive command. An interactive page will be displayed asking you to enter the password.

Syntax

sudo config username add *name* **-ek**

Parameter Description

name: The name of the username to create.

Usage Guidelines

- The root account cannot be configured with a password.
- The default admin and root accounts cannot be deleted.

Examples

```
admin@sonic:~$ sudo config username add test001 -ek
Please input your password:
Please confirm your password:
admin@sonic:~$
admin@sonic:~$ show username
Index       Username          Type
-------    ----------     ------------
    1          test001             cli-user
    2           admin                default-user
    3           tacacsuser     remote-user
```

Note
You can modify the password for the admin user or other users using the following method. Use the 'config save' command to save the configuration for it to take effect.

```
admin@sonic:~$ sudo config username add admin -ek
Please input your password:
Please confirm your password:
admin@sonic:~$ sudo config save -y
Running command: vtysh -c "write" -> success
Running command: /usr/local/bin/sonic-cfggen -d --print-data > /etc/sonic/config_db.json
admin@sonic:~$
```

1.4 remove username

Function

Run the **remove username** command to delete a local user.

Syntax

sudo config username delete *name*

Parameter Description

name: The name of the username to create.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show username
Index       Username          Type
-------    ----------    ------------
    1          test001              cli-user
    2           admin               default-user
admin@sonic:~$ sudo config username delete test001
admin@sonic:~$ show username
Index       Username          Type
-------    ----------    ------------
    1          admin              default-user
```

1.5 show aaa

Function

Run the **show aaa** command to display the AAA settings currently present in the network node.

Syntax

show aaa

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show aaa
AAA authentication login local (default)
AAA authentication failthrough True (default)
AAA authentication fallback True (default)
```

1.6 show username

Function

Run the **show username** command to shows the configured users, including local users, tacacs users and radius users, and so on.

Syntax

show username

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show username
Index       Username          Type
-------    ----------     ------------
    1          test001              cli-user
    2          admin                default-user
    3          tacacsuser       remote-user
```

1 RADIUS Commands

Command	Function
config radius add	Add a RADIUS server to the radius server list.
config radius authtype	Modify the global value for the RADIUS authtype.
config radius default	Reset the global value for authtype, passkey, timeout, nasip, sourceip, or retransmit to default value.
config radius delete	Delete the configured radius server.
config radius nasip	Set the NAS-ip-address attribute used by the NAS to send RADIUS packets.
config radius passkey	Modify the global value for the RADIUS passkey.
config radius retransmit	Set the number of retransmission times for RADIUS authentication request packets.
config radius sourceip	Set the source IP address for the device to communicate with the RADIUS server.
config radius statistics	Enable or disable RADIUS statistics.
config radius timeout	Modify the global value for the RADIUS timeout.
show radius	Display the global configuration fields and the list of all radius servers and their corresponding configurations.

1.1 config radius add

Function

Run the **config radius add** command to add a RADIUS server to the radius server list.

Note that more than one radius (maximum of seven) can be added in the device.

When user tries to login, tacacs client shall contact the servers one by one.

When any server times out, device will try the next server one by one based on the priority value configured for that server.

When this command is executed, the configured radius server addresses are updated in /etc/pam.d/common-auth-sonic configuration file which is being used by radius service.

Syntax

sudo config radius add { *ipv4-address* | *ipv6-address* } [**-r** *retransmit*] [**-p** *priority-integer*] [**-t** *timeout-integer*] [**-k** *shared-secret*] [**-a** *auth-type* { **chap** | **pap** | **mschapv2** }] [**-o** *auth-port*] [**-s** *source-interface*] [**-m** | **--use-mgmt-vrf**]

Parameter Description

ipv4_address: RADIUS server IP address.

ipv6_address: RADIUS server IP address.

retransmit: Number of retransmission times for communicating with the RADIUS server, default 3.

priority-integer: Priority, priority range 1 to 64, default 1.

timeout-integer: Transmission timeout interval in seconds, range 1 to 60, default 5.

shared-secret: Shared key for the server. If no shared key is configured, use global configuration. When this option is specified, the key is entered interactively.

auth-type: Authentication type, "chap" or "pap" or "mschapv2", default is "pap".

auth-port: UDP port range is 1 to 65535, default 1812.

source-interface: Source interface that communicates with the radius server.

use-mgmt-vrf: This means that the server is part of Management vrf, default is "no vrf".

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config radius add 172.31.240.109 -t 10 -k -a chap -p 2
Please input your password:
Please confirm your password:
```

Example Server Configuration in /etc/pam.d/common-auth-sonic configuration file:

```
# root user can only be authenticated locally. Jump to local.
auth       [success=1 default=ignore]          pam_succeed_if.so user = root
# For the RADIUS servers, on success jump to the cache the MPL(Privilege)
auth       [success=2 new_authtok_reqd=done default=ignore]            pam_radius_auth.so
conf=/etc/pam_radius_auth.d/172.31.240.109_1812.conf privilege_level protocol=chap retry=3
client_id=sonic statistics=172.31.240.109 try_first_pass
# Local
auth       [success=done new_authtok_reqd=done default=ignore]        pam_unix.so nullok
try_first_pass
auth       requisite           pam_deny.so
# Cache MPL(Privilege)
auth       [success=1 default=ignore]          pam_exec.so /usr/sbin/cache_radius
```

1.2 config radius authtype

Function

Run the **config radius authtype** command to modify the global value for the RADIUS authtype.

When user has not configured server specific authtype, this global value shall be used for that server.

Syntax

sudo config radius authtype { **chap** | **pap** | **mschapv2** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config radius authtype chap
```

1.3 config radius default

Function

Run the **config radius default** command to reset the global value for authtype, passkey, timeout, nasip, sourceip, or retransmit to default value.

Default for authtype is "pap", default for passkey is EMPTY_STRING and default for timeout is 5 seconds.

Syntax

sudo config radius default { **authtype** | **passkey** | **timeout** | **nasip** | **sourceip** | **retransmit** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

This will reset the global authtype back to the default value “pap”.

```
admin@sonic:~$ sudo config radius default authtype
```

1.4 config radius delete

Function

Run the **config radius delete** command to delete the configured radius server.

Syntax

sudo config radius delete { *ipv4-address* | *ipv6-address* }

Parameter Description

ip_address: RADIUS server IP address.

ipv6_address: RADIUS server IP address.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config radius delete 172.31.240.109
```

1.5 config radius nasip

Function

Run the **config radius nasip** command to set the NAS-ip-address attribute used by the NAS to send RADIUS packets.

Syntax

sudo config radius nasip { *nas-ip* | *IPv6-address* }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config radius nasip 172.31.32.50
```

1.6 config radius passkey

Function

Run the **config radius passkey** command to modify the global value for the RADIUS passkey.

When user has not configured server specific passkey, this global value shall be used for that server.

Syntax

sudo config radius passkey -k

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config radius passkey -k
Please input your password:
Please confirm your password:
```

1.7 config radius retransmit

Function

Run the **config radius retransmit** command to set the number of retransmission times for RADIUS authentication request packets.

Syntax

sudo config radius retransmit *retry_attempts*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config radius retransmit 5
```

1.8 config radius sourceip

Function

Run the **config radius sourceip** command to set the source IP address for the device to communicate with the RADIUS server.

Syntax

sudo config radius radius sourceip { *ipv4-address* | *ipv6-address* }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config radius sourceip 172.31.32.50
```

1.9 config radius statistics

Function

Run the **config radius statistics** command to enable or disable RADIUS statistics.

Syntax

sudo config radius statistics { **enable** | **disable** | **default** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config radius statistics enable
```

1.10 config radius timeout

Function

Run the **config radius timeout** command to modify the global value for the RADIUS timeout.

When user has not configured server specific timeout, this global value shall be used for that server.

Syntax

sudo config radius [**default**] **timeout** [*timeout_value_in_seconds*]

Parameter Description

default: When the optional keyword "default" is specified, timeout_value_in_seconds parameter wont be used; default value of 5 is used.

timeout_value_in_seconds: Valid values for timeout is 1 to 60 seconds.

Usage Guidelines

N/A

Examples

To configure non-default timeout value.

```
admin@sonic:~$ admin@sonic:~$ sudo config radius timeout 60
```

1.11 show radius

Function

Run the **show radius** command to display the global configuration fields and the list of all radius servers and their corresponding configurations.

Syntax

show radius

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show radius
RADIUS global auth_type pap (default)
RADIUS global retransmit 3 (default)
RADIUS global timeout 5 (default)
RADIUS global passkey ******
RADIUS global statistics True

RADIUS_SERVER address 172.31.240.109
                      auth_port 1812
```

```
priority 1
```

1 TACACS Commands

Command	Function
config tacacs add	Add a TACACS+ server to the tacacs server list.
config tacacs authtype	Modify the global value for the TACACS+ authtype.
config tacacs default	Reset the global value for authtype or passkey or timeout to default value.
config tacacs delete	Delete the tacacs+ servers configured.
config tacacs passkey	Modify the global value for the TACACS+ passkey.
config tacacs timeout	Modify the global value for the TACACS+ timeout.
show tacacs	Display the global configuration fields and the list of all tacacs servers and their corresponding configurations.

1.1 config tacacs add

Function

Run the **config tacacs add** command to add a TACACS+ server to the tacacs server list.

Note that more than one tacacs+ (maximum of seven) can be added in the device.

When user tries to login, tacacs client shall contact the servers one by one.

When any server times out, device will try the next server one by one based on the priority value configured for that server.

When this command is executed, the configured tacacs+ server addresses are updated in /etc/pam.d/common-auth-sonic configuration file which is being used by tacacs service.

Syntax

sudo config tacacs add *ip-address* [**-t** | **--timeout** *seconds*] [**-ek** | **--encrypted-key** *secret*] [**-a** | **--type** *type*] [**-o** | **--port** *port*] [**-p** | **--pri** *priority*] [**-m** | **--use-mgmt-vrf**]

Parameter Description

ip-address: TACACS+ server IP address.

seconds: Transmission timeout interval in seconds, range 1 to 60, default 5.

secret: Shared key for the server. If no shared key is configured, use global configuration. When this option is specified, the key is entered interactively.

type: Authentication type, "chap" or "pap" or "mschap" or "login", default is "pap".

port: TCP port range is 1 to 65535, default 49.

priority: priority range 1 to 64, default 1.

use-mgmt-vrf: This means that the server is part of Management vrf, default is "no vrf".

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config tacacs add 172.31.240.110 -t 10 -ek -a chap -o 50 -p 9
Please input your password:
Please confirm your password:
admin@sonic:~$
```

Example Server Configuration in /etc/pam.d/common-auth-sonic configuration file:

```
auth       [success=done new_authtok_reqd=done default=ignore]        pam_tacplus.so
server=10.11.12.14:50 secret=testing789 login=mschap timeout=10    try_first_pass
auth       [success=done new_authtok_reqd=done default=ignore]        pam_tacplus.so
server=10.11.12.24:50 secret=testing789 login=mschap timeout=987654321098765433211
     0987    try_first_pass
```

```
auth      [success=done new_authtok_reqd=done default=ignore]       pam_tacplus.so
server=10.0.0.9:49 secret= login=mschap timeout=5    try_first_pass
auth      [success=done new_authtok_reqd=done default=ignore]       pam_tacplus.so
server=10.0.0.8:49 secret= login=mschap timeout=5    try_first_pass
auth      [success=done new_authtok_reqd=done default=ignore]       pam_tacplus.so
server=10.11.12.13:50 secret=testing789 login=mschap timeout=10    try_first_pass
auth      [success=done new_authtok_reqd=done default=ignore auth_err=die]
pam_tacplus.so server=172.31.240.109:49 secret=U2FsdGVkX1+cytzC2jlD2K8v0ljpZjnrWsA/hbb/PBE=
login=pap timeout=5     try_first_pass
auth      [success=1 default=ignore]         pam_unix.so nullok try_first_pass
```

Note
In the above example, the servers are stored (sorted) based on the priority value configured for the server.

1.2 config tacacs authtype

Function

Run the **config tacacs authtype** command to modify the global value for the TACACS+ authtype.

When user has not configured server specific authtype, this global value shall be used for that server.

Syntax

sudo config tacacs authtype { **chap** | **pap** | **login** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config tacacs authtype chap
```

1.3 config tacacs default

Function

Run the **config tacacs default** command to reset the global value for authtype or passkey or timeout to default value.

Default for authtype is “pap”, default for passkey is EMPTY_STRING and default for timeout is 5 seconds.

Syntax

sudo config tacacs default { **authtype** | **passkey** | **timeout** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

This will reset the global authtype back to the default value "pap".

```
admin@sonic:~$ sudo config tacacs default authtype
```

1.4 config tacacs delete

Function

Run the **config tacacs delete** command to delete the tacacs+ servers configured.

Syntax

sudo config tacacs delete *ip_address*

Parameter Description

ip-address: TACACS+ server IP address.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config tacacs delete 10.11.12.13
```

1.5 config tacacs passkey

Function

Run the **config tacacs passkey** command to modify the global value for the TACACS+ passkey.

When user has not configured server specific passkey, this global value shall be used for that server.

Syntax

sudo config tacacs encrypted-passkey -ek

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config tacacs encrypted-passkey -ek
Please input your password:
Please confirm your password:
```

1.6 config tacacs timeout

Function

Run the **config tacacs timeout** command to modify the global value for the TACACS+ timeout.

When user has not configured server specific timeout, this global value shall be used for that server.

Syntax

sudo config tacacs [**default**] **timeout** [*timeout_value_in_seconds*]

Parameter Description

default: When the optional keyword "default" is specified, timeout_value_in_seconds parameter wont be used; default value of 5 is used.

timeout_value_in_seconds: Valid values for timeout is 1 to 60 seconds.

Usage Guidelines

N/A

Examples

To configure non-default timeout value.

```
admin@sonic:~$ sudo config tacacs timeout 60
```

1.7 show tacacs

Function

Run the **show tacacs** command to display the global configuration fields and the list of all tacacs servers and their corresponding configurations.

Syntax

show tacacs

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show tacacs
TACPLUS global auth_type pap (default)
TACPLUS global timeout 5 (default)
TACPLUS global passkey ******

TACPLUS_SERVER address 172.31.240.109
                       priority 1
                       tcp_port 49
```

1 RSTP Commands

Note
The STP function is not suitable for use in scenarios that already have anti-loop functions, such as VXLAN scenarios and MCLAG scenarios.STP and RSTP are for global Layer 2 interfaces and do not consider VLANs.

Command	Function
config spanning-tree forward-delay	Configure STP bridge forward delay, and forward-delay-value must be 2*(forward-delay-value-1) >= max-age-value >= 2*(hello-time-value +1).
config spanning-tree hello	Configure STP bridge hello time, and hello-value must be 2*(forward-delay-value-1) >= max-age-value >= 2*(hello-time-value +1).
config spanning-tree interface autoedge	Configure STP port autoedge.
config spanning-tree interface bpdufilter	Configure STP port bpdufilter.
config spanning-tree interface bpduguard	Configure STP port bpdufilter.
config spanning-tree interface cost	Configure STP port path_cost.
config spanning-tree interface priority	Configure STP port priority, and port priority_value must be multiple of 16.
config spanning-tree max-age	Configure STP bridge max-age, and max-age-value must be 2*(forward-delay-value-1) >= max-age-value >= 2*(hello-time-value +1).
config spanning-tree priority	Configure STP bridge priority, and priority_value must be multiple of 4096.
config spanning-tree version	Configure the STP mode.
debug spanning-tree loglevel	Display the STP log level.
show runningconfiguration spanning-tree	Display the STP view configuration.
show spanning-tree	Display brief STP information. It displays the Common and Internal Spanning Tree (CIST) information.
show spanning-tree interface	Display brief STP information. It displays

	the CIST interface information.
sonic-clear spanning-tree statistics	Clear the statistics for the Spanning Tree Protocol.
sonic-clear spanning-tree statistics interface	Clear the statistics for the STP port. For a single interface, provide the interface name with the sub-command.

1.1 config spanning-tree forward-delay

Function

Run the **config spanning-tree forward-delay** command to configure STP bridge forward delay, and forward-delay-value must be 2*(forward-delay-value-1) >= max-age-value >= 2*(hello-time-value +1).

In STP, forward delay is a parameter that determines the time a switch spends in the listening and learning states before forwarding packets. When a switch receives a Bridge Protocol Data Unit (BPDU) and determines that it is not the root bridge, it moves into the listening state, during which it listens for BPDU messages from other switches. After a period of time, the switch moves into the learning state, during which it learns the MAC addresses of devices connected to its ports. Finally, the switch moves into the forwarding state, during which it forwards packets. The forward delay parameter is used to ensure that the network topology is stable before forwarding packets, and the default value is 15 seconds.

Syntax

config spanning-tree forward-delay *forward-delay-value*

Parameter Description

forward-delay-value: STP bridge forward delay, the value range is from 4 to 30.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config spanning-tree forward-delay 15
```

1.2 config spanning-tree hello

Function

Run the **config spanning-tree hello** command to configure STP bridge hello time, and hello-value must be 2*(forward-delay-value-1) >= max-age-value >= 2*(hello-time-value +1).

In STP, hello time is the interval at which switches send Bridge Protocol Data Unit (BPDU) messages to each other. BPDU messages are used to establish the network topology and calculate the tree. Switches exchange BPDU messages to determine the root bridge and port states. Hello time determines how often switches send BPDU messages, or how frequently switches update their information about the network topology. By default, hello time is set to 2 seconds, but it can be adjusted as needed.

Syntax

config spanning-tree hello *hello-value*

Parameter Description

hello-value: STP bridge hello time, the value range is from 1 to 10.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config spanning-tree hello 2
```

1.3 config spanning-tree interface autoedge

Function

Run the **config spanning-tree interface autoedge** command to configure STP port autoedge.

In STP, autoedge is a feature that allows a port to automatically transition to the forwarding state if it is connected to an end device, such as a computer or printer. End devices do not generate BPDU messages, so autoedge allows the switch to quickly recognize that the port is not part of the spanning tree and can forward packets immediately. If the switch later receives a BPDU on an autoedge port, the port will transition to the blocking state and participate in the spanning tree. Autoedge is enabled by default on STP-enabled switches.

Syntax

config spanning-tree interface autoedge { **enable** | **disable** } *interface-name*

Parameter Description

enable: Enable STP port automatic edge.

disable: Disable STP port automatic edge.

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config spanning-tree interface autoedge enable Ethernet49
```

1.4 config spanning-tree interface bpdufilter

Function

Run the **config spanning-tree interface bpdufilter** command to configure STP port bpdufilter.

In STP, bpdufilter is a feature that allows a port to discard all incoming BPDU messages. This can be useful in situations where a switch is connected to a non-STP aware device, such as

a server or router, and the switch port should not participate in the spanning tree. By enabling bpdufilter on the port, the switch will not receive or process any BPDU messages on that port. However, enabling bpdufilter on a port can also create a potential loop on the network if the non-STP aware device generates its own BPDU messages. Bpdufilter should be used with caution and only in specific situations where it is necessary.

Syntax

config spanning-tree interface bpdufilter { **enable** | **disable** } *interface-name*

Parameter Description

enable: Enable STP port bpdufilter.

disable: Disable STP port bpdufilter.

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config spanning-tree interface bpdufilter disable Ethernet49
```

1.5 config spanning-tree interface bpduguard

Function

Run the **config spanning-tree interface bpduguard** command to configure STP port bpdufilter.

In STP, bpdufilter is a feature that allows a port to discard all incoming BPDU messages. This can be useful in situations where a switch is connected to a non-STP aware device, such as a server or router, and the switch port should not participate in the spanning tree. By enabling bpdufilter on the port, the switch will not receive or process any BPDU messages on that port. However, enabling bpdufilter on a port can also create a potential loop on the network if the non-STP aware device generates its own BPDU messages. Bpdufilter should be used with caution and only in specific situations where it is necessary.

Syntax

config spanning-tree interface bpduguard { **enable** | **disable** } *interface-name*

Parameter Description

enable: Enable STP port bpduguard.

disable: Disable STP port bpduguard.

Interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config spanning-tree interface bpduguard disable Ethernet49
```

1.6 config spanning-tree interface cost

Function

Run the **config spanning-tree interface cost** command to configure STP port path_cost.

In STP, path_cost is a parameter that is used to determine the cost of a particular path through the network. The path_cost is calculated based on the bandwidth of the link between switches. The formula for calculating path_cost is 10^8/bandwidth, where bandwidth is measured in bits per second. The path_cost is used in the selection of root and designated ports, as well as in the calculation of the shortest path to the root bridge. By default, the path_cost is set to 20000.

Syntax

config spanning-tree interface cost *interface-name cost-value*

Parameter Description

interface-name: Interface name, for example, Ethernet1.

cost-value: The range is from 2 to 200000000.

Usage Guidelines

interface-name: Interface name, for example, Ethernet1.

cost-value: STP port path_cost, the value range is from 2 to 200000000.

Examples

```
admin@sonic:~$ sudo config spanning-tree interface cost Ethernet49 20000
```

1.7 config spanning-tree interface priority

Function

Run the **config spanning-tree interface priority** command to configure STP port priority, and port priority_value must be multiple of 16.

In STP, port priority is a parameter that is used to determine the priority of a port on a switch. Port priority is used in the election of designated ports, which are the ports that are responsible for forwarding traffic on a segment. The port with the lowest port priority on a segment becomes the designated port. If two ports have the same port priority, the port with the lower port number becomes the designated port. Port priority can be manually configured on each port, or it can be automatically assigned based on the switch model and firmware. The default port priority value for STP is 128.

Syntax

config spanning-tree interface priority *interface-name priority-value*

Parameter Description

interface-name: Interface name, for example, Ethernet1.

priority-value: STP port priority, the value range is from 0 to 240.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config spanning-tree interface priority Ethernet49 128
```

1.8 config spanning-tree max-age

Function

Run the **config spanning-tree max-age** command to configure STP bridge max-age, and max-age-value must be 2*(forward-delay-value-1) >= max-age-value >= 2*(hello-time-value +1).

In STP, max-age is a parameter that determines the maximum time a switch will consider a BPDU valid. The default value is 20 seconds.

Syntax

config spanning-tree max-age *max-age-value*

Parameter Description

max-age-value: The maximum validity time of BPDU messages, the value range is from 6 to 40.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config spanning-tree max-age 20
```

1.9 config spanning-tree priority

Function

Run the **config spanning-tree priority** command to configure STP bridge priority, and priority_value must be multiple of 4096.

In STP, priority is a parameter that is used to determine the priority of a switch on the network. The priority value is used in the election of the root bridge, and the switch with the lowest priority value becomes the root bridge. If two switches have the same priority, the switch with the lower MAC address becomes the root bridge. Priority values can be manually configured on each switch, or they can be automatically assigned based on the switch model and firmware. The default priority value for STP is 32768.

Syntax

config spanning-tree priority *priority-value*

Parameter Description

priority-value: STP bridge priority, the value range is from 0 to 61440. .

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config spanning-tree priority 32768
```

1.10 config spanning-tree version

Function

Run the **config spanning-tree version** command to configure the STP mode.

STP is a protocol used to prevent loops on a network by creating a tree-like topology. STP achieves this by selecting a root bridge and disabling some of the links on the network to create a loop-free topology. Rapid Spanning Tree Protocol (RSTP) is a protocol used to prevent loops on a network by creating a tree-like topology. It is an improvement over the original STP in that it has a faster convergence time, meaning it can quickly adapt to changes in the network topology.

Syntax

config spanning-tree version { **stp** | **rstp** }

Parameter Description

stp: Spanning Tree Protocol.

rstp: Rapid Spanning Tree Protocol.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config spanning-tree version rstp
```

1.11 debug spanning-tree loglevel

Function

Run the **debug spanning-tree loglevel** command to display the STP log level.

Syntax

debug spanning-tree loglevel { **DEBUG** | **INFO** | **ERROR** }

Parameter Description

loglevel: Log level, for example, DEBUG

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo debug spanning-tree loglevel DEBUG
```

1.12 show runningconfiguration spanning-tree

Function

Run the **show runningconfiguration spanning-tree** command to display the STP view configuration.

Syntax

show runningconfiguration spanning-tree

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration spanning-tree
    "STP":
    {
            "GLOBAL": {
                    "force_version": "rstp",
                    "forward_delay": "15",
                    "hello_time": "2",
                    "max_age": "20",
                    "priority": "32768"
            }
    }
    "STP_PORT":
    {
            "Ethernet49": {
                    "autoedge": "disable",
```

```
                "bpdu_filter": "disable",
                "bpdu_guard": "disable",
                "path_cost": "500",
                "priority": "128"
        }
}
```

1.13 show spanning-tree

Function

Run the **show spanning-tree** command to display brief STP information. It displays the Common and Internal Spanning Tree (CIST) information.

Syntax

show spanning-tree

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show spanning-tree
  Bridge CIST info
  enabled                yes
  bridge id              8.000.C0:B8:E6:C0:AB:B3
  designated root 8.000.C0:B8:E6:C0:AB:B3
  regional root      8.000.C0:B8:E6:C0:AB:B3
  root port              none
  path cost          0                   internal path cost      0
  max age            20                  bridge max age          20
  forward delay 15                   bridge forward delay 15
  tx hold count 6                    max hops                20
  hello time         2                   ageing time             300
  force protocol version         rstp
  time since topology change 836
  topology change count          0
  topology change                no
  topology change port           None
  last topology change port      None
```

1.14 show spanning-tree interface

Function

Run the **show spanning-tree interface** command to display brief STP information. It displays the CIST interface information.

Syntax

show spanning-tree interface [*interface-name*]

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show spanning-tree interface
    Bridge:Ethernet49 CIST info
    enabled                yes                          role
Designated
    port id                8.002                        state
forwarding
    external port cost 500                              admin external cost     0
    internal port cost 500                              admin internal cost     0
    designated root        8.000.C0:B8:E6:C0:AB:B3 dsgn external cost       0
    dsgn regional root 8.000.C0:B8:E6:C0:AB:B3 dsgn internal cost       0
    designated bridge      8.000.C0:B8:E6:C0:AB:B3 designated port          8.002
    admin edge port        no                           auto edge port          yes
    oper edge port         yes                          topology change ack     no
    point-to-point         yes                          admin point-to-point auto
    restricted role        no                           restricted TCN          no
    port hello time        2                            disputed                no
    bpdu guard port        no                           bpdu guard error        no
    network port           no                           BA inconsistent         no
    bpdu filter port       no                           Num RX BPDU Filtered 0
    Num TX BPDU            1239                         Num TX TCN              0
    Num RX BPDU            0                            Num RX TCN
0
    Num Transition FWD 1                                Num Transition BLK      1
    Rcvd BPDU              no                           Rcvd STP
no
    Rcvd RSTP              no                           Send RSTP
yes
```

```
    Rcvd TC Ack                   no                                  Rcvd TCN
no
    Bridge:Ethernet51 CIST info
    enabled                       yes                                 role
Designated
    port id                       8.003                               state
forwarding
    external port cost 500                                    admin external cost     0
    internal port cost 500                                    admin internal cost     0
    designated root           8.000.C0:B8:E6:C0:AB:B3 dsgn external cost        0
    dsgn regional root 8.000.C0:B8:E6:C0:AB:B3 dsgn internal cost        0
    designated bridge     8.000.C0:B8:E6:C0:AB:B3 designated port          8.003
    admin edge port           no                                  auto edge port          yes
    oper edge port            yes                                 topology change ack     no
    point-to-point            yes                                 admin point-to-point auto
    restricted role           no                                  restricted TCN          no
    port hello time           2                                   disputed                no
    bpdu guard port           no                                  bpdu guard error        no
    network port              no                                  BA inconsistent         no
    bpdu filter port          no                                  Num RX BPDU Filtered 0
    Num TX BPDU               1239                                Num TX TCN              0
    Num RX BPDU               0                                   Num RX TCN
0
    Num Transition FWD 1                                          Num Transition BLK      1
    Rcvd BPDU                 no                                  Rcvd STP
no
    Rcvd RSTP                 no                                  Send RSTP
yes
    Rcvd TC Ack               no                                  Rcvd TCN
no

admin@sonic:~$ show spanning-tree interface Ethernet49
    Bridge:Ethernet49 CIST info
    enabled                       yes                                 role
Designated
    port id                       8.002                               state
forwarding
    external port cost 500                                    admin external cost     0
    internal port cost 500                                    admin internal cost     0
    designated root           8.000.C0:B8:E6:C0:AB:B3 dsgn external cost        0
    dsgn regional root 8.000.C0:B8:E6:C0:AB:B3 dsgn internal cost        0
    designated bridge     8.000.C0:B8:E6:C0:AB:B3 designated port          8.002
    admin edge port           no                                  auto edge port          yes
    oper edge port            yes                                 topology change ack     no
    point-to-point            yes                                 admin point-to-point auto
    restricted role           no                                  restricted TCN          no
```

```
    port hello time          2                                  disputed                        no
    bpdu guard port          no                                 bpdu guard error          no
    network port             no                                 BA inconsistent           no
    bpdu filter port       no                                   Num RX BPDU Filtered 0
    Num TX BPDU              1239                               Num TX TCN                      0
    Num RX BPDU              0                                  Num RX TCN
0
    Num Transition FWD 1                                        Num Transition BLK      1
    Rcvd BPDU                no                                 Rcvd STP
no
    Rcvd RSTP                no                                 Send RSTP
yes
    Rcvd TC Ack              no                                 Rcvd TCN
no
```

1.15 sonic-clear spanning-tree statistics

Function

Run the **sonic-clear spanning-tree statistics** command to clear the statistics for the Spanning Tree Protocol.

This command is used to clear all the counters and statistics related to STP, including the number of packets received and transmitted, the number of topology changes, and the number of BPDU messages sent and received. This command can be useful for troubleshooting STP-related issues, as it allows the user to start with a fresh set of statistics and counters.

Syntax

sonic-clear spanning-tree statistics

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo sonic-clear spanning-tree statistics
```

1.16 sonic-clear spanning-tree statistics interface

Function

Run the **sonic-clear spanning-tree statistics interface** command to clear the statistics for the STP port. For a single interface, provide the interface name with the sub-command.

Syntax

sonic-clear spanning-tree statistics interface *interface-name*

Parameter Description

interface-name: Interface name, for example, Ethernet1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo sonic-clear spanning-tree statistics interface Ethernet49
```

1 SSH Commands

Command	Function
config ssh	Display the global SSH configuration.
config ssh banner	Configure an SSH banner.
config ssh port set	Set the port of the SSH service.
config ssh port unset	Unset the port of the SSH service.
show ssh config	Display the global SSH configuration.

1.1 config ssh

Function

Run the **config ssh** command to display the global SSH configuration.

Syntax

config ssh { **enable** | **disable** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config ssh enable
    Restarting sshd-config service...
```

1.2 config ssh banner

Function

Run the **config ssh banner** command to configure an SSH banner.

Syntax

config ssh banner *path*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config ssh banner /etc/sonic/banner
    Restarting sshd-config service...
```

1.3 config ssh port set

Function

Run the **config ssh port set** command to set the port of the SSH service.

Syntax

config ssh port set *port-num*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config ssh port set 10022
    Restarting sshd-config service...
```

1.4 config ssh port unset

Function

Run the **config ssh port unset** command to unset the port of the SSH service.

Syntax

config ssh port unset

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config ssh port unset
    Restarting sshd-config service...
```

1.5 show ssh config

Function

Run the **show ssh config** command to display the global SSH configuration.

Syntax

show ssh config

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ssh config
    sshd status: enable
    sshd port: 22
    sshd banner: None
```

1 CoPP Commands

Command	Function
config copp algorithm	Specify the rate-limiting algorithm for protocol.
config copp bandwidth	Specify the packet type and set the CPU bandwidth for sending the packet.
config copp packet_action	Configure how protocol packets are processed.
config copp queue	Configure the protocol priority queue.
config copp trap	Configure the protocol-specific trap attributes.
show copp group	Display the CoPP group configuration.
show copp statistics	Display CoPP statistics.
show copp trap	Display the CoPP trap configuration.
sonic-clear copp statistics	Clear CoPP statistics.

1.1 config copp algorithm

Function

Run the **config copp algorithm** command to specify the rate-limiting algorithm for protocol.

Syntax

sudo config copp algorithm *packet-type* { **sr_tcm** | **tr_tcm** | **storm** } { **blind** | **aware** } [{ **-g** | **--green_action** } *green-action*] [{ **-y** | **--yellow_action** } *yellow-action*] [{ **-r** | **--red_action** } *red-action*]

Parameter Description

packet-type: Protocol type.

mode: Rate-limiting algorithm.

color: Working mode of the rate-limiting algorithm

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config copp algorithm arp sr_tcm blind
admin@sonic:~$ show copp group arp_group
trap_group       queue  trap_action       trap_priority  meter_type     mode     color  cbs
cir  pbs     pir     green_action     yellow_action     red_action
-----------  -------  -------------  ---------------  ------------  ------  ------------  --
---  -----  -----  --------------  ---------------  ------------
arp_group           5  copy                          5  packets       sr_tcm   blind 1500 1500
NA       NA      NA              drop              drop
```

1.2 config copp bandwidth

Function

Run the **config copp bandwidth** command to specify the packet type and set the CPU bandwidth for sending the packet.

Syntax

sudo config copp bandwidth *packet-type* [**-cir** *cir-value*] [**-cbs** *cbs-value*] [**-pir** *pir-value*] [**-pbs** *pbs-value*] [{ **-m** | **--meter_type** } { **packets** | **bytes** }]

Parameter Description

packet-type: Protocol type.

cir-value: Committed information rate.

cbs-value: Committed burst size.

pir-value: Peak information rate.

pbs-value: Peak burst size.

meter_type: Statistical unit of the speed limiting algorithm packets or bytes.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config copp bandwith arp -cir 2000 -cbs 20000 -pir 3000 -pbs 30000
admin@sonic:~$ show copp group arp_group
trap_group        queue   trap_action        trap_priority   meter_type      mode      color   cbs
cir      pbs      pir   green_action      yellow_action      red_action
------------  -------  -------------  ---------------  ------------  ------  ------------  --
---  -----  -----  --------------  ---------------  ------------
arp_group              5   copy                           5   packets         sr_tcm   blind     20000
2000   30000    3000   trap              drop               drop
```

1.3 config copp packet_action

Function

Run the **config copp packet_action** command to configure how protocol packets are processed.

Syntax

sudo config copp packet_action *packet-type packet-action*

Parameter Description

packet-type: Protocol type.

packet-action: Packet processing mode, including drop, forward, copy, copy_cancel, trap, log, deny, and transit.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config copp packet_action arp trap
admin@sonic:~$ show copp group arp_group
trap_group        queue   trap_action        trap_priority   meter_type      mode      color   cbs
cir   pbs      pir      green_action      yellow_action      red_action
------------  -------  -------------  ---------------  ------------  ------  -------  -----  -
----  -----  -----  --------------  ---------------  ------------
```

```
arp_group           5   trap                        5   packets        sr_tcm   blind      1500
1500   NA       NA       NA                drop               drop
```

1.4 config copp queue

Function

Run the **config copp queue** command to configure the protocol priority queue.

Syntax

sudo config copp packet_action *packet-type queue*

Parameter Description

packet-type: Protocol type.

queue: Priority queue, range 0 to 7.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config copp queue arp 5
admin@sonic:~$ show copp group arp_group
trap_group        queue   trap_action        trap_priority   meter_type      mode      color   cbs
cir   pbs      pir      green_action      yellow_action      red_action
------------  -------  -------------  ---------------  ------------  ------  -------  -----  -
----  -----  -----  --------------  ---------------  ------------
arp_group           5   trap                        5   packets        sr_tcm   blind   1500    1500
NA       NA       NA                drop               drop
```

1.5 config copp trap

Function

Run the **config copp trap** command to configure the protocol-specific trap attributes.

Syntax

sudo config copp trap { **add** | **del** } *packet-type*

sudo config copp trap set *packet-type* [{ **-t** | **--trap_ids** } *trap_ids*] [{ **-g** | **--group** } *packet-group*] [{ **-a** | **--always_enabled** } { **true** | **false** }]

Parameter Description

packet-type: Protocol type.

trap-ids: Protocol.

packet-group: Group to which the protocol belongs.

always_enabled: Install protocols which have no associated feature.

Usage Guidelines

- The statistical results of COPP packets may differ from the actual values. The packet rate is calculated as packets per acquisition period, and the final statistical value may differ due to the deviation of the software acquisition period.
- Multiple users send protocol packets to the switch at the same time. If the packet flow exceeds the protocol rate limit, packets of some users may be discarded within a period of time because the packet loss mechanism of the rate limit is random.
- For the M2-W6520-24QC8DC, M2-W6930-64QC, M2-W6510-48GT4V, and M2-W6920-32QC2X, NTP, FTP, TACPLUS, and ICMP packets are collected to ip2me.
- When the ip2me packets in the environment exceed the COPP rate limit, all service packets sent to the CPU through ip2me may be lost due to COPP rate limit. (ip2me packets are those that match routes and are sent to the local device.)
- Packets that are TACAS authenticated by AAA are also sent to the CPU through ip2me. If the number of ip2me packets exceeds the COPP rate limit, authentication packets may be discarded due to COPP rate limit. Intermittent authentication failure may occur.
- For the M2-W6520-24QC8DC, COPP counter statistics are not supported when Community SAI is used.
- For the M2-W6930-64QC and M2-W6920-32QC2X, the bandwidth cannot be modified using the COPP sflow counter command.
- For the M2-W6520-24QC8DC, M2-W6930-64QC, and M2-W6920-32QC2X, COPP sflow counter statistics are not supported.

Examples

```
admin@sonic:~$ sudo config copp trap set arp -a false
admin@sonic:~$ show copp trap
name      trap_ids                        trap_group      always_enabled
------   --------------------------   ------------   ----------------
arp       arp_req,arp_resp                arp_group       false
bfd       bfd,bfdv6                      bfd_group       NA

admin@sonic:~$ sudo config copp trap del arp
admin@sonic:~$ show copp trap
name      trap_ids                        trap_group      always_enabled
------   --------------------------   ------------   ----------------
bfd       bfd,bfdv6                      bfd_group          NA
bgp       bgp,bgpv6                      bgp_group          NA
```

1.6 show copp group

Function

Run the **show copp group** command to display the CoPP group configuration.

Syntax

show copp group

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show copp group
trap_group           queue  trap_action  trap_priority  meter_type  mode  color cbs
cir  pbs  pir  green_action  yellow_action  red_action
---------------  -------  -------------  ---------------  ------------  ------  -------  ----
-  -----  -----  -----  --------------  ---------------  ------------
arp_group              5  copy           5                packets     sr_tcm  blind  1500
1500  NA  NA  trap  drop  drop
bfd_group              7  trap           7                packets     sr_tcm  NA     3000
3000  NA  NA  NA  drop  drop
bgp_group              6  trap           6                packets     sr_tcm  NA     1500
1500  NA  NA  NA  drop  drop
default                0  trap           NA               packets     sr_tcm  NA     1500
1500  NA  NA  NA  drop  drop
dhcp_group             4  trap           4                packets     sr_tcm  NA     300
300  NA  NA  NA  drop  drop
dhcpv6_group           3  trap           3                packets     sr_tcm  NA     1500
1500  NA  NA  NA  drop  drop
dhcpv6_l2_group        3  trap           3                packets     sr_tcm  NA     1500
1500  NA  NA  NA  drop  drop
ip2me_group            2  trap           2                packets     sr_tcm  NA     2000
2000  NA  NA  NA  drop  drop
isis_group             3  trap           3                packets     sr_tcm  NA     1500
1500  NA  NA  NA  drop  drop
lacp_group             7  trap           7                packets     sr_tcm  NA     300
300  NA  NA  NA  drop  drop
lldp_group             3  trap           3                packets     sr_tcm  NA     300
300  NA  NA  NA  drop  drop
nat_group              1  trap           1                packets     sr_tcm  NA     1500
1500  NA  NA  NA  drop  drop
nd_group               5  copy           5                packets     sr_tcm  NA     1500
1500  NA  NA  NA  drop  drop
ospf6_group            6  trap           6                packets     sr_tcm  NA     1500
1500  NA  NA  NA  drop  drop
ospf_group             6  trap           6                packets     sr_tcm  NA     1500
1500  NA  NA  NA  drop  drop
```

```
pim_group              6   trap          6              packets       sr_tcm   NA     1500
1500   NA      NA      NA              drop            drop
sflow_group            1   trap          10             bytes         storm    NA     8000
8000   NA      NA      NA              NA              drop
snmp_group             4   trap          4              packets       sr_tcm   NA     300
300    NA      NA      NA              drop            drop
ssh_group              4   trap          4              packets       sr_tcm   NA     300
300    NA      NA      NA              drop            drop
stp_group              3   trap          3              packets       sr_tcm   NA     300
300    NA      NA      NA              drop            drop
udld_group             4   trap          4              packets       sr_tcm   NA     300
300    NA      NA      NA              drop            drop
vrrp_group             7   trap          7              packets       sr_tcm   NA     300
300    NA      NA      NA              drop            drop
```

1.7 show copp statistics

Function

Run the **show copp statistics** command to display CoPP statistics.

Syntax

show copp statistics [{ **-t** | **--type** } { **count** | **rate** }] [{ **-m** | **--meter** } { **packet** | **byte** }] [{ **-p** | **--protocol** } *packet-group*]

Parameter Description

packet-group: Group to which the protocol belongs.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show copp statistics
Packet Type          Total Packets Rate     Green Packets Rate     Yellow Packets Rate     Red
Packets Rate
---------------  --------------------  --------------------  ----------------------  --------
----------
lldp_group                         0                     0                       0         0
bgp_group                          0                     0                       0         0
ospf_group                         0                     0                       0         0
default                            0                     0                       0         0
bfd_group                          0                     0                       0         0
pim_group                          0                     0                       0         0
ospf6_group                        0                     0                       0         0
arp_group                          0                     0                       0         0
isis_group                         0                     0                       0         0
```

```
stp_group                                0                        0                        0          0
vrrp_group                               0                        0                        0          0
snmp_group                               0                        0                        0
0
lacp_group                               0                        0                        0          0
ip2me_group                              0                        0                        0
0
dhcpv6_group                             0                        0                        0
0
dhcpv6_l2_group                          0                        0                        0
0
admin@sonic:~$ show copp    statistics -t count -m packet -p arp_group
Packet Type         Total Packets       Green Packets       Yellow Packets       Red Packets
-------------   ---------------   ---------------   ----------------   -------------
arp_group              10                  10                  0                  0
```

1.8 show copp trap

Function

Run the **show copp trap** command to display the CoPP trap configuration.

Syntax

show copp trap

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show copp trap
name          trap_ids                    trap_group          always_enabled
---------   -------------------------   ---------------   ----------------
arp           arp_req,arp_resp            arp_group           true
bfd           bfd,bfdv6                    bfd_group           NA
bgp           bgp,bgpv6                    bgp_group           NA
dhcp          dhcp                        dhcp_group           NA
dhcpv6        dhcpv6                        dhcpv6_group       true
dhcpv6_l2   dhcpv6_l2                     dhcpv6_l2_group    true
ip2me         ip2me                         ip2me_group       true
isis          isis                        isis_group          true
lacp          lacp                         lacp_group         true
lldp          lldp                        lldp_group           NA
```

```
nat          src_nat_miss,dest_nat_miss   nat_group          NA
nd           neigh_discovery              nd_group           NA
ospf         ospf                         ospf_group         NA
ospf6        ospf6                        ospf6_group        NA
pim          pim                          pim_group          NA
sflow        sample_packet                sflow_group        NA
snmp         snmp                         snmp_group         NA
ssh          ssh                          ssh_group          NA
stp          stp                          stp_group          NA
udld         udld                         udld_group         NA
vrrp         vrrp,vrrpv6                  vrrp_group         NA
```

1.9 sonic-clear copp statistics

Function

Run the **sonic-clear copp statistics** command to clear CoPP statistics.

Syntax

sudo sonic-clear copp statistics [*packet-group*]

Parameter Description

packet-group: Group to which the protocol belongs.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show copp statistics -t count
Packet Type          Total Packets     Green Packets     Yellow Packets     Red Packets
---------------  ---------------  ---------------  ----------------  -------------
lldp_group             19425            19425              0              0
bgp_group                  0                0              0              0
ospf_group                 0                0              0              0
default                    0                0              0              0
bfd_group                  0                0              0              0
pim_group                  0                0              0              0
ospf6_group                0                0              0              0
arp_group                 16               16              0              0
isis_group             40093            40093              0              0
stp_group               9550             9550              0              0
vrrp_group                 0                0              0              0
snmp_group                 0                0              0              0
lacp_group                 0                0              0              0
ip2me_group                0                0              0              0
```

```
dhcpv6_group                0                0                0                0
dhcpv6_l2_group           525              525                0                0
admin@sonic:~$ sudo sonic-clear copp statistics lldp_group

admin@sonic:~$ show copp statistics -t count
Packet Type          Total Packets     Green Packets     Yellow Packets     Red Packets
---------------  ---------------  ---------------  ----------------  -------------
lldp_group                   2                2                 0              0
bgp_group                    0                0                 0              0
ospf_group                   0                0                 0              0
default                      0                0                 0              0
bfd_group                    0                0                 0              0
pim_group                    0                0                 0              0
ospf6_group                  0                0                 0              0
arp_group                   16               16                 0              0
isis_group               40093            40093                 0              0
stp_group                 9550             9550                 0              0
vrrp_group                   0                0                 0              0
snmp_group                   0                0                 0              0
lacp_group                   0                0                 0              0
ip2me_group                  0                0                 0              0
dhcpv6_group                 0                0                 0              0
dhcpv6_l2_group            525              525                 0              0

admin@sonic:~$ sonic-clear copp statistics

admin@sonic:~$ show copp statistics -t count
Packet Type          Total Packets     Green Packets     Yellow Packets     Red Packets
---------------  ---------------  ---------------  ----------------  -------------
lldp_group                   0                0                 0              0
bgp_group                    0                0                 0              0
ospf_group                   0                0                 0              0
default                      0                0                 0              0
bfd_group                    0                0                 0              0
pim_group                    0                0                 0              0
ospf6_group                  0                0                 0              0
arp_group                    0                0                 0              0
isis_group                   0                0                 0              0
stp_group                    0                0                 0              0
vrrp_group                   0                0                 0              0
snmp_group                   0                0                 0              0
lacp_group                   0                0                 0              0
ip2me_group                  0                0                 0              0
dhcpv6_group                 0                0                 0              0
dhcpv6_l2_group              0                0                 0              0
```

1 M-LAG Commands

Command	Function
config mclag	Set MCLAG.
config mclag keepalive-interval	The MCLAG keepalive interval.
config mclag member	Set an MCLAG member interface.
config mclag session-timeout	Set the MCLAG session timeout.
show mclag config	Display the MCLAG configuration.
show mclag summary	Display the MCLAG summary.

1.1 config mclag

Function

Run the **config mclag** command to set MCLAG.

Syntax

config mclag add *domain-id source-ip-addr peer-ip-addr peer-ifname*

config mclag del *domain-id*

Parameter Description

add: Add MCLAG domain.

domain-id: MCLAG domain ID.

source-ip-addr: MCLAG domain local IP.

peer-ip-addr: MCLAG domain peer IP.

peer-ifname: Interface of the backup link in the MCLAG domain in a Layer 2 scenario.

del: Delete MCLAG domain.

Usage Guidelines

Under normal circumstances, there is no difference in the packet forwarding function between the active and standby devices. Only during synchroniaton configuration, the active device shall prevail.

Examples

```
admin@sonic:~$ sudo config mclag add 1 10.10.10.10 20.20.20.20 PortChannel20
admin@sonic:~$ sudo config mclag del 1
```

1.2 config mclag keepalive-interval

Function

Run the **config mclag keepalive-interval** command to the MCLAG keepalive interval.

Syntax

config mclag keepalive-interval *domain-id time-in-secs*

Parameter Description

domain-id: MCLAG domain ID.

time-in-secs: Time in second.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config mclag keepalive-interval 1 10
```

1.3 config mclag member

Function

Run the **config mclag member** command to set an MCLAG member interface.

Syntax

config mclag member { **add** | **del** } *domain-id portchannel-name*

Parameter Description

add: Add member MCLAG interfaces from MCLAG domain.

del: Delete member MCLAG interfaces from MCLAG domain.

domain-id: MCLAG domain ID.

portchannel-name: Downlink interface of the MCLAG domain.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config mclag member add 1 PortChannel30
```

1.4 config mclag session-timeout

Function

Run the **config mclag session-timeout** command to set the MCLAG session timeout.

Syntax

config mclag session-timeout *domain-id time-in-secs*

Parameter Description

domain-id: MCLAG domain ID.

time-in-secs: Time in second.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config mclag session-timeout 1 10
```

1.5 show mclag config

Function

Run the **show mclag config** command to display the MCLAG configuration.

Syntax

show mclag config

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show mclag config
    domain id: 1
    Local ip: 10.10.10.10
    Peer ip: 20.20.20.20
    Peer link:
    Mclag interfaces: PortChannel30
    Keepactive interval: 1
    Session timeout: 15
```

1.6 show mclag summary

Function

Run the **show mclag summary** command to display the MCLAG summary.

Syntax

show mclag summary

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show mclag summary
    The MCLAG's keepalive is: OK
    MCLAG info sync is: complete
    Domain id: 1
```

```
Local Ip: 10.10.10.10
Peer Ip: 20.20.20.20
Peer Link Interface: PortChannel20
Keepalive time: 1
sesssion Timeout : 15
Peer Link Mac: 58:69:6c:fb:22:08
Role: Standby
MCLAG Interface: PortChannel30
Loglevel: NOTICE
```

1 VRRP Commands

Command	Function
config interface vrrp add	Add a VRRP instance on an interface.
config interface vrrp adv_interval	Configure a VRRP advertisement interval for a VRRP instance.
config interface vrrp backup_forward	Enable or disable the VRRP instance to forward service traffic even if the VRRP instance is in the backup state.
config interface vrrp ip add	Add a virtual IP address to a VRRP instance on an interface.
config interface vrrp ip remove	Remove a virtual IP address from a VRRP instance on an interface.
config interface vrrp pre_empt	Enable or disable preemption of a master VRRP router by a higher-priority VRRP router.
config interface vrrp priority	Configure a priority for a VRRP instance.
config interface vrrp remove	Remove a VRRP instance from an interface.
config interface vrrp shutdown	Bring the VRRP instance into administrative shutdown mode.
config interface vrrp startup	Bring the VRRP instance into administrative up mode.
config interface vrrp track_interface add	Add a track interface to a VRRP instance.
show vrrp interface	Display the VRRP information specific to the interface.
show vrrp summary	Display a summary of VRRP information.
show vrrp vrid	Display the VRRP information specific to the VRID.

1.1 config interface vrrp add

Function

Run the **config interface vrrp add** command to add a VRRP instance on an interface.

Syntax

config interface vrrp add *interface-name vrrp-id*

Parameter Description

interface-name: Interface name, for example, Ethernet1.

vrrp-id: VRRP instance ID.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface vrrp add Ethernet51 5
```

1.2 config interface vrrp adv_interval

Function

Run the **config interface vrrp adv_interval** command to configure a VRRP advertisement interval for a VRRP instance.

Syntax

config interface vrrp adv_interval *interface-name vrrp-id interval*

Parameter Description

interface-name: Routed interface name.

vrrp-id: VRRP instance ID.

interval: VRRP advertisement interval.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface vrrp adv_interval Ethernet51 5 1200
```

1.3 config interface vrrp backup_forward

Function

Run the **config interface vrrp backup_forward** command to enable or disable the VRRP instance to forward service traffic even if the VRRP instance is in the backup state.

Syntax

config interface vrrp backup_forward *interface-name vrrp-id* { **disabled** | **enabled** }

Parameter Description

interface-name: Routed interface name.

vrrp-id: VRRP instance ID.

disabled: Disable traffic forwarding even if the VRRP instance is in the backup state.

enabled: Enable traffic forwarding even if the VRRP instance is in the backup state.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface vrrp backup_forward Ethernet51 5 enabled
```

1.4 config interface vrrp ip add

Function

Run the **config interface vrrp ip add** command to add a virtual IP address to a VRRP instance on an interface.

Syntax

config interface vrrp ip add *interface-name vrrp-id ip-addr*

Parameter Description

interface-name: Routed interface name.

vrrp-id: VRRP instance ID.

ip-addr: VRRP instance IP address.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface vrrp ip add Ethernet51 5 10.10.10.10/24
```

1.5 config interface vrrp ip remove

Function

Run the **config interface vrrp ip remove** command to remove a virtual IP address from a VRRP instance on an interface.

Syntax

config interface vrrp ip remove *interface-name vrrp-id ip-addr*

Parameter Description

interface-name: Routed interface name.

vrrp-id: VRRP instance ID.

ip-addr: VRRP instance IP address.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface vrrp ip remove Ethernet51 5 10.10.10.10/24
```

1.6 config interface vrrp pre_empt

Function

Run the **config interface vrrp pre_empt** command to enable or disable preemption of a master VRRP router by a higher-priority VRRP router.

Syntax

config interface vrrp pre_empt *interface-name vrrp-id* { **disabled** | **enabled** }

Parameter Description

interface-name: Routed interface name.

vrrp-id: VRRP instance ID.

disabled: Disable preemption of a VRRP router.

enabled: Enable preemption of a VRRP router.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface vrrp pre_empt Ethernet51 5 enabled
```

1.7 config interface vrrp priority

Function

Run the **config interface vrrp priority** command to configure a priority for a VRRP instance.

Syntax

config interface vrrp priority *interface-name vrrp-id priority*

Parameter Description

interface-name: Routed interface name.

vrrp-id: VRRP instance ID.

priority: VRRP advertisement priority.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface vrrp priority Ethernet51 5 120
```

1.8 config interface vrrp remove

Function

Run the **config interface vrrp remove** command to remove a VRRP instance from an interface.

Syntax

config interface vrrp remove *interface-name vrrp-id*

Parameter Description

interface-name: Routed interface name.

vrrp-id: VRRP instance ID.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface vrrp remove Ethernet51 5
```

1.9 config interface vrrp shutdown

Function

Run the **config interface vrrp shutdown** command to bring the VRRP instance into administrative shutdown mode.

Syntax

config interface vrrp shutdown *interface-name vrrp-id*

Parameter Description

interface-name: Routed interface name.

vrrp-id: VRRP instance ID.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface vrrp shutdown Ethernet51 5
```

1.10 config interface vrrp startup

Function

Run the **config interface vrrp startup** command to bring the VRRP instance into administrative up mode.

Syntax

config interface vrrp startup *interface-name vrrp-id*

Parameter Description

interface-name: Routed interface name.

vrrp-id: VRRP instance ID.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface vrrp startup Ethernet51 5
```

1.11 config interface vrrp track_interface add

Function

Run the **config interface vrrp track_interface add** command to add a track interface to a VRRP instance.

Syntax

config interface vrrp track_interface add *interface-name vrrp-id track-interface weight*

Parameter Description

interface-name: Routed interface name.

vrrp-id: VRRP instance ID.

track-interface: Interface name of a track interface.

weight: Weight of a track interface.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface vrrp track_interface add Ethernet51 5 Ethernet4 20
```

1.12 show vrrp interface

Function

Run the **show vrrp interface** command to display the VRRP information specific to the interface.

Syntax

show vrrp interface [*OPTIONS*] *interface-name vrid*

Parameter Description

OPTIONS:

- --verbose:

  Enable verbose output
- -h, -?, --help:

  Show this message and exit.

interface-name: Routed interface name.

vrid: VRRP instance ID.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vrrp interface Ethernet53

  Virtual Router ID                5
  Protocol Version                 3
  Autoconfigured                   No
  Shutdown                         No
  Interface                        Ethernet53
  VRRP interface (v4)              Vrrp4-5
  VRRP interface (v6)              None
  Primary IP (v4)                  10.0.0.98
  Primary IP (v6)                  ::
  Virtual MAC (v4)                 00:00:5e:00:01:05
  Virtual MAC (v6)                 00:00:5e:00:02:05
  Status (v4)                      Master
  Status (v6)                      Initialize
  Priority                         100
  Effective Priority (v4)          100
  Effective Priority (v6)          100
  Preempt Mode                     Yes
  Accept Mode                      Yes
  Advertisement Interval           1000 ms
  Master Advertisement Interval (v4)  1000 ms
  Master Advertisement Interval (v6)  0 ms
  Advertisements Tx (v4)           1
  Advertisements Tx (v6)           0
  Advertisements Rx (v4)           0
  Advertisements Rx (v6)           0
  Gratuitous ARP Tx (v4)           1
  Neigh. Adverts Tx (v6)           0
  State transitions (v4)           2
  State transitions (v6)           0
  Skew Time (v4)                   600 ms
  Skew Time (v6)                   0 ms
  Master Down Interval (v4)        3600 ms
  Master Down Interval (v6)        0 ms
  IPv4 Addresses                   1
  ..............................   11.11.11.11
  IPv6 Addresses                   0
```

1.13 show vrrp summary

Function

Run the **show vrrp summary** command to display a summary of VRRP information.

Syntax

show vrrp summary [*OPTIONS*]

Parameter Description

OPTIONS:

- --verbose:
  Enable verbose output
- -h, -?, --help:
  Show this message and exit.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vrrp summary
Interface       VRID    Configured Priority     Priority    IPv4    IPv6  State (v4)     State (v6)
----------  ------  --------------------  ----------  ------  ------  ------------  ------------
Ethernet2       10                   100         100       0       0  Backup          Backup
Ethernet53       5                   100         100       1       0  Master          Backup
```

1.14 show vrrp vrid

Function

Run the **show vrrp vrid** command to display the VRRP information specific to the VRID.

Syntax

show vrrp vrid [*OPTIONS*] *vrid*

Parameter Description

OPTIONS:

- --verbose:
  Enable verbose output
- -h, -?, --help:
  Show this message and exit.

vrid: VRRP instance ID.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vrrp vrid 5

  Virtual Router ID                 5
  Protocol Version                  3
  Autoconfigured                    No
  Shutdown                          No
  Interface                         Ethernet53
  VRRP interface (v4)               Vrrp4-5
  VRRP interface (v6)               None
  Primary IP (v4)                   10.0.0.98
  Primary IP (v6)                   ::
  Virtual MAC (v4)                  00:00:5e:00:01:05
  Virtual MAC (v6)                  00:00:5e:00:02:05
  Status (v4)                       Master
  Status (v6)                       Initialize
  Priority                          100
  Effective Priority (v4)           100
  Effective Priority (v6)           100
  Preempt Mode                      Yes
  Accept Mode                       Yes
  Advertisement Interval            1000 ms
  Master Advertisement Interval (v4)  1000 ms
  Master Advertisement Interval (v6)  0 ms
  Advertisements Tx (v4)            1
  Advertisements Tx (v6)            0
  Advertisements Rx (v4)            0
  Advertisements Rx (v6)            0
  Gratuitous ARP Tx (v4)            1
  Neigh. Adverts Tx (v6)            0
  State transitions (v4)            2
  State transitions (v6)            0
  Skew Time (v4)                    600 ms
  Skew Time (v6)                    0 ms
  Master Down Interval (v4)         3600 ms
  Master Down Interval (v6)         0 ms
  IPv4 Addresses                    1
  ..................................  11.11.11.11
  IPv6 Addresses                    0
```

1 BFD Commands

Notes
Refer [FRR Command Reference](https://docs.frrouting.org/en/latest/) to know more BFD commands.

1 ECMP Commands

Command	Function
config load-balance ecmp	Configure ECMP load balancing.
config load-balance lag	Configure LAG load balancing.
show load_balance ecmp	Display the ECMP configuration.
show load_balance lag	Display the LAG configuration.

1.1 config load-balance ecmp

Function

Run the **config load-balance ecmp** command to configure ECMP load balancing.

Syntax

config load-balance ecmp [*OPTIONS*] { **enhanced** { **hash-seed** *value* | **ipv4** | **ipv6** } | **hash-algorithm** { **CRC** | **XOR** | **RANDOM** | **CRC_32LO** | **CRC_32HI** | **CRC_CCITT** | **CRC_XOR** } }

Parameter Description

hash-seed: ecmp hash_seed configuration.

value: the value range is from 0 to 4294967295.

ipv4: ecmp ipv4_field configuration.

ipv6: ecmp ipv6_field configuration.

CRC: CRC hash algorithm.

XOR: XOR hash algorithm.

RANDOM: RANDOM hash algorithm.

CRC_32LO: CRC_32LO hash algorithm.

CRC_32HI: CRC_32HI hash algorithm.

CRC_CCITT: CRC_CCITT hash algorithm.

CRC_XOR: CRC_XOR hash algorithm.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config load-balance ecmp enhanced hash-seed 10
admin@sonic:~$ sudo config load-balance ecmp hash-algorithm XOR
```

1.2 config load-balance lag

Function

Run the **config load-balance lag** command to configure LAG load balancing.

Syntax

config load-balance lag [*OPTIONS*] { **enhanced** { **hash-seed** *value* | **ipv4** | **ipv6 }** | **hash-algorithm** { **CRC** | **XOR** | **RANDOM** | **CRC_32LO** | **CRC_32HI** | **CRC_CCITT** | **CRC_XOR** } }

Parameter Description

hash-seed: lag hash_seed configuration.

value: the value range is from 0 to 4294967295.

ipv4: lag ipv4_field configuration.

ipv6: lag ipv6_field configuration.

CRC: CRC hash algorithm.

XOR: XOR hash algorithm.

RANDOM: RANDOM hash algorithm.

CRC_32LO: CRC_32LO hash algorithm.

CRC_32HI: CRC_32HI hash algorithm.

CRC_CCITT: CRC_CCITT hash algorithm.

CRC_XOR: CRC_XOR hash algorithm.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config load-balance lag enhanced hash-seed 10
admin@sonic:~$ sudo config load-balance lag hash-algorithm XOR
```

1.3 show load_balance ecmp

Function

Run the **show load_balance ecmp** command to display the ECMP configuration.

Syntax

show load_balance ecmp

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show load_balance ecmp
Hash Algorithm : CRC
IPV4 Field : dst-ip,l4-dst-port,l4-src-port,protocol,src-ip
IPV6 Field : dst-ip,l4-dst-port,l4-src-port,protocol,src-ip
```

```
Hash Seed      : 0
```

1.4 show load_balance lag

Function

Run the **show load_balance lag** command to display the LAG configuration.

Syntax

show load balance lag

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show load_balance lag
    Hash Algorithm : CRC
    IPV4 Field : dst-ip,l4-dst-port,l4-src-port,protocol,src-ip
    IPV6 Field : dst-ip,l4-dst-port,l4-src-port,protocol,src-ip
    Hash Seed      : 0
```

1 Mirroring Commands

Command	Function
config mirror_session	Add or remove mirroring sessions.
config mirror_session span add	Configure the following fields that are used while forwarding the mirrored packets.
show mirror_session	Display all the mirror sessions that are configured.

1.1 config mirror_session

Function

Run the **config mirror_session** command to add or remove mirroring sessions.

Syntax

config mirror_session erspan add [*session-name*] [*src-ip*] [*dst_ip*] [*dscp*] [*ttl*] [*gre-type*] [*queue*] [**policer** *policer-name*] [*source-port-list*] [*direction*]

- The following command is also supported to be backward compatible. This command will be deprecated in future releases.

  config mirror_session add [*session-name*] [*src-ip*] [*dst_ip*] [*dscp*] [*ttl*] [*gre-type*] [*queue*]

Parameter Description

N/A

Usage Guidelines

Mirror session is identified by "session_name". This command supports configuring both SPAN/ERSPAN sessions. In SPAN user can configure mirroring of list of source ports/LAG to destination port in ingress/egress/both directions. In ERSPAN user can configure mirroring of list of source ports/LAG to a destination IP. Both SPAN/ERSPAN support ACL based mirroring and can be used in ACL configurations.

While adding a new ERSPAN session, users need to configure the following fields that are used while forwarding the mirrored packets.

- source IP address,
- destination IP address,
- DSCP (QoS) value with which mirrored packets are forwarded
- TTL value
- optional - GRE Type in case if user wants to send the packet via GRE tunnel. GRE type could be anything; it could also be left as empty; by default, it is 0x8949.
- optional - Queue in which packets shall be sent out of the device. Valid values 0 to 7 for most of the devices. Users need to know their device and the number of queues supported in that device.
- optional - Policer which will be used to control the rate at which frames are mirrored.
- optional - List of source ports which can have both Ethernet and LAG ports.
- optional - Direction - Mirror session direction when configured along with Source port. (Supported rx/tx/both. default direction is both)

Examples

```
admin@sonic:~$ sudo config mirror_session add mrr_legacy 1.2.3.4 20.21.22.23 8 100 0x6558 0
admin@sonic:~$ show mirror_session
```

```
Name            Status      SRC IP       DST IP          GRE       DSCP      TTL      Queue      Policer
Monitor Port      SRC Port      Direction
---------     --------  --------   -----------  ------  ------  -----  -------  ---------  ----
----------  ----------  -----------
mrr_legacy    inactive   1.2.3.4      20.21.22.23    0x6558   8          100      0
admin@sonic:~$ sudo config mirror_session erspan add mrr_abcd 1.2.3.4 20.21.22.23 8 100 0x6558 0
admin@sonic:~$ show mirror_session
Name          Status      SRC IP       DST IP          GRE       DSCP      TTL      Queue      Policer      Monitor
Port      SRC Port      Direction
---------  --------  --------   -----------  ------  ------  -----  -------  ---------  -----
---------  ----------  -----------
mrr_abcd    inactive   1.2.3.4      20.21.22.23    0x6558   8          100      0
admin@sonic:~$
admin@sonic:~$ sudo config mirror_session erspan add mrr_port 1.2.3.4 20.21.22.23 8 100 0x6558 0
Ethernet10
admin@sonic:~$ show mirror_session
Name          Status      SRC IP       DST IP          GRE       DSCP      TTL      Queue      Policer      Monitor
Port      SRC Port      Direction
---------  --------  --------   -----------  ------  ------  -----  -------  ---------  -----
---------  ----------  -----------
mrr_port    inactive   1.2.3.4      20.21.22.23    0x6558   8          100      0
Ethernet10    both
admin@sonic:~$
```

1.2 config mirror_session span add

Function

Run the **config mirror_session span add** command to configure the following fields that are used while forwarding the mirrored packets.

Syntax

config mirror_session span add [*session-name*] [*dst-port*] [*source-port-list*] [*direction*] [*queue*] [**policer** *policer-name*]

Parameter Description

N/A

Usage Guidelines

While adding a new SPAN session, users need to configure the following fields that are used while forwarding the mirrored packets.

- destination port,
- optional - List of source ports- List of source ports which can have both Ethernet and LAG ports.
- optional - Direction - Mirror session direction when configured along with Source port.

(Supported rx/tx/both. default direction is both)

- optional - Queue in which packets shall be sent out of the device. Valid values 0 to 7 for most of the devices. Users need to know their device and the number of queues supported in that device.
- optional - Policer which will be used to control the rate at which frames are mirrored.

limit information:

- For the M2-W6520-24QC8DC, M2-W6930-64QC, M2-W6510-48GT4V, M2-W6920-32QC2X, and M2-W6930-64QC, in a mirroring session where mirrored packets are broadcast or multicast packets, if a packet is broadcast to multiple ports and multiple ports are mirrored at the egress, only one packet is mirrored.
- When the destination port is congested (for example, when a 100 Mbps destination port monitors a 1000 Mbps source port), the source port sends Pause frames.
- The routed interface takes effect based on a VLAN, that is, a routed interface occupies a VLAN. The packets received by the routed interface are tagged with the VLAN ID, and the ingress mirroring does not change the packet content. As a result, when the source interface is a routed interface and the destination interface is a trunk interface, the packets mirrored by the destination interface are tagged with the ID of the VLAN associated with the destination interface.
- The mirror function does not take effect for the packets sent by the control plane.
- For the M2-W6520-24QC8DC, M2-W6920-32QC2X, and M2-W6930-64QC, if egress mirroring is configured and the mirrored packets are multicast packets, the packets output by the destination interface are the multicast packets before routing.
- For the M2-W6510 series, if egress mirroring is configured and the mirrored packets are multicast packets, the packets output by the destination interface are the multicast packets before routing.
- When the ERSPAN mirroring source is an outbound packet from a Layer 3 interface, an internal VLAN tag assigned by the routing function is added. Mirrored packets carry the VLAN tag.

Examples

```
admin@sonic:~$ sudo config mirror_session span add port0 Ethernet10
Ethernet4,Ethernet8
admin@sonic:~$ show mirror_session
Name          Status          DST Port          SRC Port                              Direction
Queue          Policer
------      --------      ----------      -------------------      -----------          --
-----      -------
port0         active          Ethernet10      Ethernet4,Ethernet8      both
```

1.3 show mirror_session

Function

Run the **show mirror_session** command to display all the mirror sessions that are configured.

Syntax

show mirror_session

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show mirror_session
ERSPAN Sessions
Name          Status      SRC IP       DST IP      GRE      DSCP      TTL      Queue      Policer      Monitor
Port      SRC Port      Direction
------       --------   --------    --------   -----   ------   -----   -------   ---------   -----------
----   ----------   -----------
everflow0    active      10.1.0.32    10.0.0.7
SPAN Sessions
Name      Status      DST Port      SRC Port      Direction      Queue      Policer
------   --------   ----------   ----------   -----------   -------   ---------
port0     active      Ethernet10    Ethernet20    rx
```

1 sflow Commands

Command	Function
config sflow agent-id	Add/delete the sFlow agent-id.
config sflow collector add	Add a sFlow collector.
config sflow collector del	Delete a sFlow collector with the given name.
config sflow	Start and sample will start on all interfaces which have sFlow enabled at the interface level (see “config sflow interface…”).
config sflow interface disable	Disable sflow at an interface level.
config sflow interface enable	Enable sflow at an interface level.
config sflow interface sample-rate	Configure the sample-rate for a specific interface.
config sflow polling-interval	Set the counter polling interval.
show sflow	Display the global sFlow configuration that includes the admin state, collectors, the Agent ID and counter polling interval.
show sflow interface	Display the per-interface sflow admin status and the sampling rate.

1.1 config sflow agent-id

Function

Run the **config sflow agent-id** command to add/delete the sFlow agent-id.

This setting is global (applicable to both collectors) and optional. Only a single agent-id is allowed. If agent-id is not specified (with this CLI), an appropriate IP that belongs to the switch is used as the agent-id based on some simple heuristics.

Syntax

config sflow agent-id { **add** | **del** } *interface-name*

Parameter Description

interface-name: specify the interface name whose ipv4 or ipv6 address will be used as the agent-id in sFlow datagrams.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config sflow agent-id add lo
```

1.2 config sflow collector add

Function

Run the **config sflow collector add** command to add a sFlow collector.

Syntax

config sflow collector add *collector-name* [*ipv4-address* | *ipv6-address*] [**port** *number*]

Parameter Description

collector-name: unique name of the sFlow collector

ipv4-address: IP address of the collector in dotted decimal format for IPv4

ipv6-address: x: x: x: x::x format for IPv6 address of the collector (where :: notation specifies successive hexadecimal fields of zeros)

port (OPTIONAL): specifies the UDP port of the collector (the range is from 0 to 65535. The default is 6343.)

Usage Guidelines

Note that a maximum of 2 collectors is allowed.

Examples

```
admin@sonic:~$ sudo config sflow collector add collector_A 10.11.46.2
```

1.3 config sflow collector del

Function

Run the **config sflow collector del** command to delete a sFlow collector with the given name.

Syntax

config sflow collector del *collector-name*

Parameter Description

collector-name: unique name of the sFlow collector

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config sflow collector del collector_A
```

1.4 config sflow

Function

Run the **config sflow** command to start and sample will start on all interfaces which have sFlow enabled at the interface level (see “config sflow interface…”).

When sflow is disabled globally, sampling is stopped on all relevant interfaces and sflow daemon is stopped.

Syntax

config sflow { **enable** | **disable** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config sflow enable
```

1.5 config sflow interface disable

Function

Run the **config sflow interface disable** command to disable sflow at an interface level.

By default, sflow is enabled on all interfaces at the interface level. Use this command to explicitly disable sFlow for a specific interface. Note that this configuration deals only with sFlow flow samples and not counter samples.

Syntax

config sflow interface disable *interface-name*

Parameter Description

interface-name: specify the interface for which sFlow flow samples have to be enabled. The "all" keyword is used as a convenience to enable sflow at the interface level for all the interfaces.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config sflow interface disable Ethernet40
```

1.6 config sflow interface enable

Function

Run the **config sflow interface enable** command to enable sflow at an interface level.

By default, sflow is enabled on all interfaces at the interface level. Use this command to explicitly disable sFlow for a specific interface. An interface is sampled if sflow is enabled globally as well as at the interface level. Note that this configuration deals only with sFlow flow samples and not counter samples.

Syntax

config sflow interface enable *interface-name* [*sample-stage*]

Parameter Description

interface-name: specify the interface for which sFlow flow samples have to be enabled. The "all" keyword is used as a convenience to enable sflow at the interface level for all the interfaces.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config sflow interface enable Ethernet40 ingress
```

1.7 config sflow interface sample-rate

Function

Run the **config sflow interface sample-rate** command to configure the sample-rate for a specific interface.

Syntax

config sflow interface sample-rate *interface-name value*

Parameter Description

interface-name: specify the interface for which the sampling rate value is to be set.

value: value is the average number of packets skipped before the sample is taken. "The sampling rate specifies random sampling probability as the ratio of packets observed to samples generated. For example a sampling rate of 256 specifies that, on average, 1 sample will be generated for every 256 packets observed." Valid range 256:8388608.

Usage Guidelines

The default sample rate for any interface is (ifSpeed / 1e6) where ifSpeed is in bits/sec. So, the default sample rate based on interface speed is:

1-in-1000 for a 1G link

1-in-10,000 for a 10G link

1-in-40,000 for a 40G link

1-in-50,000 for a 50G link

1-in-100,000 for a 100G link

It is recommended not to change the defaults. This CLI is to be used only in case of exceptions (e.g., to set the sample-rate to the nearest power-of-2 if there are hardware restrictions in using the defaults)

Examples

```
admin@sonic:~$ sudo config sflow interface sample-rate Ethernet32 1000
```

1.8 config sflow polling-interval

Function

Run the **config sflow polling-interval** command to set the counter polling interval.

Syntax

config sflow polling-interval *value*

Parameter Description

value: 0-300 seconds. Set polling-interval to 0 to disable counter polling. Default is 20 seconds.

Usage Guidelines

- Unknown unicast flooding may occur, making the egress information of packets unreliable. Therefore, the egress information obtained from ingress sampling of unknown unicast packets is unreliable. The egress information obtained from egress sampling of unknown unicast packets is also unreliable, and is set to 0 by default.
- When sFlow sampling is enabled and the port traffic consists of COPP packets, due to the higher priority of COPP over sFlow sampling, the packets cannot be forwarded to the designated CPU queue and cannot be rate-limited.

Examples

```
admin@sonic:~$ sudo config sflow polling-interval 30
```

1.9 show sflow

Function

Run the **show sflow** command to display the global sFlow configuration that includes the admin state, collectors, the Agent ID and counter polling interval.

Syntax

show sflow

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show sflow

sFlow Global Information:
sFlow Admin State:              up
sFlow Polling Interval:       default(20s)
sFlow AgentID:                  default
Collectors configured:        2
  Name: 1                       IP addr: 172.168.1.3                                  UDP port: 6343     VRF:
default
  Name: 2                       IP addr: 172.168.1.2                                  UDP port: 6343     VRF:
default
```

1.10 show sflow interface

Function

Run the **show sflow interface** command to display the per-interface sflow admin status and the sampling rate.

Syntax

show sflow interface

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show sflow interface

sFlow interface configurations
+-------------+---------------+-----------------+------------------+
| Interface   | Admin State   |   Sampling Rate | Sampling Stage   |
+=============+===============+=================+==================+
| Ethernet1   | down          |           25000 | ingress          |
+-------------+---------------+-----------------+------------------+
| Ethernet2   | down          |           25000 | ingress          |
+-------------+---------------+-----------------+------------------+
| Ethernet3   | down          |           25000 | ingress          |
+-------------+---------------+-----------------+------------------+
| Ethernet4   | down          |           25000 | ingress          |
+-------------+---------------+-----------------+------------------+
| Ethernet5   | down          |           25000 | ingress          |
+-------------+---------------+-----------------+------------------+
| Ethernet6   | down          |           25000 | ingress          |
+-------------+---------------+-----------------+------------------+
...
+-------------+---------------+-----------------+------------------+
| Ethernet52  | down          |          100000 | ingress          |
+-------------+---------------+-----------------+------------------+
| Ethernet53  | down          |          100000 | ingress          |
+-------------+---------------+-----------------+------------------+
| Ethernet54  | down          |          100000 | ingress          |
+-------------+---------------+-----------------+------------------+
| Ethernet55  | down          |          100000 | ingress          |
+-------------+---------------+-----------------+------------------+
```

```
| Ethernet56   | down          |          100000 | ingress          |
+--------------+---------------+-----------------+------------------+
```

1 NTP Commands

Command	Function
config ntp add	Add a NTP server address.
config ntp add_src	Add a NTP source.
config ntp del	Delete a configured NTP server address.
config ntp del_src	Delete a configured NTP source.
show ntp	Display a list of NTP peers known to the server as well as a summary of their state.

1.1 config ntp add

Function

Run the **config ntp add** command to add a NTP server address.

Note
That only one NTP server address can be added in the device. So, if you repeat this command, it will overwrite the previous configuration.

Syntax

sudo config ntp add *server-addr*

Parameter Description

server-addr: IP address (include IPv4 and IPv6) or a domain address of a NTP server.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config ntp add 9.9.9.9
NTP server 9.9.9.9 added to configuration
Restarting ntp-config service...
admin@sonic:~$ sudo config ntp add ntp.ntsc.ac.cn
NTP server ntp.ntsc.ac.cn added to configuration
Restarting ntp-config service...
```

1.2 config ntp add_src

Function

Run the **config ntp add_src** command to add a NTP source.

If you want to specify a source interface, the interface must be configured with an IP address. If you want to specify a source IP address, the IP address must be configured in the device.

Note
That only one NTP source can be added in the device. So, if you repeat this command, it will overwrite the previous configuration.

Syntax

sudo config ntp add_src *src*

Parameter Description

src: It can be an interface name or an IP address. The interface can be eth0, Vlan, PortChannel, Ethernet and Loopback. IP address includes IPv4 address and IPv6 address.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config ntp add_src 172.28.145.251
172.28.145.250 has been configured as ntp source
Restarting ntp-config service...
admin@sonic:~$ sudo config ntp add_src eth0
eth0 has been configured as ntp source
Restarting ntp-config service...
```

1.3 config ntp del

Function

Run the **config ntp del** command to delete a configured NTP server address.

Syntax

sudo config ntp del *address*

Parameter Description

address: IP address (include IPv4 and IPv6) or a domain address of a NTP server.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config ntp del 9.9.9.9
9.9.9.9 has been removed from ntp source
Restarting ntp-config service...
```

1.4 config ntp del_src

Function

Run the **config ntp del_src** command to delete a configured NTP source.

Syntax

sudo config ntp del_src *src*

Parameter Description

src: It can be an interface name or an IP address. The interface can be eth0, Vlan, PortChannel, Ethernet and Loopback. IP address includes IPv4 address and IPv6 address.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config ntp del_src 172.28.145.250
172.28.145.250 has been removed from ntp source
Restarting ntp-config service...
```

1.5 show ntp

Function

Run the **show ntp** command to display a list of NTP peers known to the server as well as a summary of their state.

Syntax

show ntp

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ntp
MGMT_VRF_CONFIG is not present.
 remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*172.28.145.251  LOCAL(0)   6 u    59   64  377    0.136  -63445. 144.447

NTP SERVER :
     172.28.145.251
Source Interface : unspecified
```

1 FTP Server Commands

Command	Function
config ftp-server disable	Disable FTP server function.
config ftp-server enable	Enable FTP server function.
config ftp-server login-times	Set the maximum number of FTP login attempts allowed.
config ftp-server max-sessions	Set the maximum number of FTP clients that can be concurrently connected to the FTP server.
config ftp-server timeout	Set the idle timeout duration of the FTP server for online clients in seconds.
show ftp-server	Display the status of FTP server function, maximum number of login attempts allowed, maximum number of sessions, and idle timeout duration.

1.1 config ftp-server disable

Function

Run the **config ftp-server disable** command to disable FTP server function.

Syntax

config ftp-server disable

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config ftp-server disable
Restarting vsftpd-config service...
```

1.2 config ftp-server enable

Function

Run the **config ftp-server enable** command to enable FTP server function.

Syntax

config ftp-server enable

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config ftp-server enable
Restarting vsftpd-config service...
```

1.3 config ftp-server login-times

Function

Run the **config ftp-server login-times** command to set the maximum number of FTP login attempts allowed.

The default value is 1, which means if an incorrect user name or password is entered once, the session is terminated. If the configured value is greater than 1, the client needs to use the "user' command to re-enter the user name and password after a login failure.

Syntax

config ftp-server login-times *login-times*

Parameter Description

login-times: The value ranges from 1 to 10. The default value is 1.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config ftp-server login-times 5
Restarting vsftpd-config service...
```

1.4 config ftp-server max-sessions

Function

Run the **config ftp-server max-sessions** command to set the maximum number of FTP clients that can be concurrently connected to the FTP server.

Syntax

config ftp-server max-sessions *max-sessions*

Parameter Description

max-sessions: The value ranges from 1 to 20. The default value is 10.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config ftp-server max-sessions 5
Restarting vsftpd-config service...
```

1.5 config ftp-server timeout

Function

Run the **config ftp-server timeout** command to set the idle timeout duration of the FTP server for online clients in seconds.

When the idle timeout duration expires, the client is disconnected from the FTP server.

Syntax

config ftp-server timeout *timeout*

Parameter Description

timeout: The value ranges from 1 to 3600. The default value is 600.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config ftp-server timeout 300
Restarting vsftpd-config service...
```

1.6 show ftp-server

Function

Run the **show ftp-server** command to display the status of FTP server function, maximum number of login attempts allowed, maximum number of sessions, and idle timeout duration.

Syntax

show ftp-server

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ftp-server
enable : Y
timeout : 300 s
max sessions : 10
login_times : 1
```

1 FTP Commands

Command	Function
binary/ascii	Switch the data transfer mode between binary and ascii.
ftp	Log in a FTP server.
get	Download files.
put	Upload files.
passive	Switch the FTP connection mode between passive and active.
rstatus	Display FTP server information.
status	Display FTP client information.

1.1 binary/ascii

Function

Run the **binary/ascii** command to switch the data transfer mode between binary and ascii.

Syntax

binary

ascii

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ ftp 10.110.197.248
Connected to 10.110.197.248.
220 (vsFTPd 3.0.3)
Name (10.110.197.248:admin): admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary
200 Switching to Binary mode.
ftp>
ftp> ascii
200 Switching to ASCII mode.
ftp>
```

1.2 ftp

Function

Run the **ftp** command to log in a FTP server.

Syntax

ftp *server-address*

Parameter Description

server-address: FTP server address.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ ftp 10.110.197.248
Connected to 10.110.197.248.
220 (vsFTPd 3.0.3)
Name (10.110.197.248:admin): admin
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> user
(username) admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

1.3 get

Function

Run the **get** command to download files.

Syntax

get *remote-file-path local-file-path*

Parameter Description

local-file-path: File path on FTP client.

remote-file-path: File path on FTP Server.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ ftp 10.110.197.248
Connected to 10.110.197.248.
220 (vsFTPd 3.0.3)
Name (10.110.197.248:admin): admin
331 Please specify the password.
```

```
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get sonic/server_file.txt /home/admin/test/server_file.txt
local: /home/admin/test/server_file.txt remote: sonic/server_file.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for sonic/server_file.txt (171 bytes).
226 Transfer complete.
171 bytes received in 0.00 secs (762.5214 kB/s)
ftp>
```

1.4 put

Function

Run the **put** command to upload files.

Syntax

put *local-file-path remote-file-path*

Parameter Description

local-file-path: File path on FTP client.

remote-file-path: File path on FTP Server.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ ftp 10.110.197.248
Connected to 10.110.197.248.
220 (vsFTPd 3.0.3)
Name (10.110.197.248:admin): admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put /home/admin/test/client_file.txt sonic/client_file.txt
local: /home/admin/test/client_file.txt remote: sonic/client_file.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
171 bytes sent in 0.00 secs (5.2606 MB/s)
ftp>
```

1.5 passive

Function

Run the **passive** command to switch the FTP connection mode between passive and active.

Syntax

passive

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ ftp 10.110.197.248
Connected to 10.110.197.248.
220 (vsFTPd 3.0.3)
Name (10.110.197.248:admin): admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> passive
Passive mode on.
ftp> passive
Passive mode off.
ftp>
```

1.6 rstatus

Function

Run the **rstatus** command to display FTP server information.

Syntax

rstatus

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ ftp 172.28.48.112
Connected to 172.28.48.112.
220 (vsFTPd 3.0.3)
Name (172.28.48.112:admin): sdk
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> rstatus
211-FTP server status:
     Connected to ::ffff:172.20.37.43
     Logged in as sdk
     TYPE: ASCII
     No session bandwidth limit
     Session timeout in seconds is 300
     Control connection is plain text
     Data connections will be plain text
     At session startup, client count was 1
     vsFTPd 3.0.3 - secure, fast, stable
211 End of status
ftp>
```

1.7 status

Function

Run the **status** command to display FTP client information.

Syntax

status

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ ftp 172.28.48.112
Connected to 172.28.48.112.
```

```
220 (vsFTPd 3.0.3)
Name (172.28.48.112:admin): admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> status
Connected to 172.28.48.112.
No proxy connection.
Connecting using address family: any.
Mode: stream; Type: binary; Form: non-print; Structure: file
Verbose: on; Bell: off; Prompting: on; Globbing: on
Store unique: off; Receive unique: off
Case: off; CR stripping: on
Quote control characters: on
Ntrans: off
Nmap: off
Hash mark printing: off; Use of PORT cmds: on
Tick counter printing: off
ftp>
```

1 SNMP Commands

Command	Function
config snmp	Enable or disable the SNMP service.
config snmp community	Add, delete, or modify the SNMP community.
config snmp contact	Add, delete, or modify the SNMP contact.
config snmp location	Add, delete, or modify the SNMP location.
config snmp user	Add or delete the SNMP user for SNMPv3.
config snmp view	Add, delete, or modify the SNMP view.
config snmpagentaddress add	Add the SNMP agent IP address on which the SNMP agent is expected to listen. When SNMP agent is expected to work as part of management VRF, users should specify the optional vrf_name parameter as "mgmt". This configuration goes into snmpd.conf that is used by SNMP agent. SNMP service is restarted to make this configuration effective in SNMP agent.
config snmpagentaddress del	Delete the SNMP agent IP address on which the SNMP agent is expected to listen. When users had added the agent IP as part of "mgmt" VRF, users should specify the optional vrf_name parameter as "mgmt" while deleting as well. This configuration is removed from snmpd.conf that is used by SNMP agent. SNMP service is restarted to make this configuration effective in SNMP agent.
config snmptrap del	Delete the SNMP Trap server IP address to which SNMP agent is expected to send TRAPs. When users had added the trap server IP as part of "mgmt" VRF, users should specify the optional vrf_name parameter as "mgmt" while deleting as well. This configuration is removed from snmpd.conf that is used by SNMP agent. SNMP service is restarted to make this configuration effective in SNMP agent.

config snmptrap modify	Modify the SNMP trap server IP address to which the SNMP agent is expected to send the traps. Users can configure one server IP addrss for each SNMP version to send the traps. When SNMP agent is expected to send traps as part of management VRF, users should specify the optional vrf_name parameter as "mgmt". This configuration goes into snmpd.conf that is used by SNMP agent. SNMP service is restarted to make this configuration effective in SNMP agent.
show runningconfiguration snmp	Display the global SNMP configuration that includes the location, contact, community, and user settings.
show runningconfiguration snmp community	Display the SNMP community settings.
show runningconfiguration snmp contact	Display the SNMP contact setting.
show runningconfiguration snmp location	Display the SNMP location setting.
show runningconfiguration snmp view	Display the SNMP view setting.
show runningconfiguration snmp user	Display the SNMP user settings.
show snmpagentaddress	Display the configured SNMP agent IP addresses.
show snmptrap	Display the configured SNMP Trap server IP addresses.

1.1 config snmp

Function

Run the **config snmp** command to enable or disable the SNMP service.

Syntax

config snmp { **enable** | **disable** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config snmp enable
Restarting SNMP service...
```

1.2 config snmp community

Function

Run the **config snmp community** command to add, delete, or modify the SNMP community.

Syntax

config snmp community add *community* { **RO** | **RW** } [**-s** | **--source**] [**-v** | **--view**]

config snmp community del [*community*]

config snmp community modify [*community*] [**RO** | **RW**] [**-s** | **--source**] [**-v** | **--view**]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config snmp community add testcomm ro -s 172.31.240.48 -v testview1
SNMP community testcomm added to configuration
Restarting SNMP service...
```

```
admin@sonic:~$ sudo config snmp community del testcomm
```

```
SNMP community testcomm removed from configuration
Restarting SNMP service...
```

```
admin@sonic:~$ sudo config snmp community modify testcomm rw -s 172.31.240.48 -v testview2
Restarting SNMP service...
```

1.3 config snmp contact

Function

Run the **config snmp contact** command to add, delete, or modify the SNMP contact.

Syntax

config snmp contact add *contact contact_email*

config snmp contact del *contact*

config snmp contact modify *contact contact_email*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config snmp contact add joe joe@contoso.com
Contact name joe and contact email joe@contoso.com have been added to configuration
Restarting SNMP service...
```

```
admin@sonic:~$ sudo config snmp contact del joe
SNMP contact joe removed from configuration
Restarting SNMP service...
```

```
admin@sonic:~$ sudo config snmp contact modify test test@contoso.com
SNMP contact test and contact email test@contoso.com updated
Restarting SNMP service...
```

1.4 config snmp location

Function

Run the **config snmp location** command to add, delete, or modify the SNMP location.

Syntax

config snmp location{ **add** | **del** | **modify** } **location**

Parameter Description

N/A

Usage Guidelines

N/A

Examples

Add new SNMP location "Emerald City" if it does not already exist

```
admin@sonic:~$ sudo config snmp location add Emerald City
SNMP Location Emerald City has been added to configuration
Restarting SNMP service...
```

Delete SNMP location "Emerald City" if it already exists

```
admin@sonic:~$ sudo config snmp location del Emerald City
SNMP Location Emerald City removed from configuration
Restarting SNMP service...
```

Modify SNMP location "Emerald City" to "Redmond"

```
admin@sonic:~$ sudo config snmp location modify Redmond
SNMP location Redmond modified in configuration
Restarting SNMP service...
```

1.5 config snmp user

Function

Run the **config snmp user** command to add or delete the SNMP user for SNMPv3.

Syntax

config snmp user add *user* { **noAuthNoPriv** | **AuthNoPriv** | **Priv** } { **RO** | **RW** } [[[**MD5** | **SHA**] [*auth-password*]] [[**DES** | **AES**] [*encrypt-password*]]] [**-v** | **--view**]

config snmp user del *user*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config snmp user add testuser1 noauthnopriv ro
SNMP user testuser1 added to configuration
Restarting SNMP service...
```

```
admin@sonic:~$ sudo config snmp user add testuser2 authnopriv ro sha testuser2_auth_pass
SNMP user testuser2 added to configuration
Restarting SNMP service...
```

```
admin@sonic:~$ sudo config snmp user add testuser3 priv rw md5 testuser3_auth_pass aes
testuser3_encrypt_pass -v testview1
SNMP user testuser3 added to configuration
Restarting SNMP service...
```

```
admin@sonic:~$ sudo config snmp user del testuser1
SNMP user testuser1 removed from configuration
Restarting SNMP service...
```

1.6 config snmp view

Function

Run the **config snmp view** command to add, delete, or modify the SNMP view.

Syntax

config snmp view add *viewname viewtype viewoid*

config snmp view del *viewname viewtype viewoid*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config snmp view add testview1 include 1.3.6.1.2.1
Restarting SNMP service...
```

```
admin@sonic:~$ sudo config snmp view del testview1 include 1.3.6.1.2.1
Restarting SNMP service...
```

1.7 config snmpagentaddress add

Function

Run the **config snmpagentaddress add** command to add the SNMP agent IP address on which the SNMP agent is expected to listen. When SNMP agent is expected to work as part of management VRF, users should specify the optional vrf_name parameter as "mgmt". This configuration goes into snmpd.conf that is used by SNMP agent. SNMP service is restarted to make this configuration effective in SNMP agent.

Syntax

config snmpagentaddress add [**-p** *port-num*] [**-v** *vrf-name*] *agentip*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config snmpagentaddress add -v mgmt -p 123 21.22.13.14

Note: For this example, configuration goes into /etc/snmp/snmpd.conf inside snmp docker as follows. When "-v" parameter is not used, the additional "%" in the following line will not be present.

 agentAddress 21.22.13.14:123%mgmt
```

1.8 config snmpagentaddress del

Function

Run the **config snmpagentaddress del** command to delete the SNMP agent IP address on which the SNMP agent is expected to listen. When users had added the agent IP as part of "mgmt" VRF, users should specify the optional vrf_name parameter as "mgmt" while deleting as well. This configuration is removed from snmpd.conf that is used by SNMP agent. SNMP service is restarted to make this configuration effective in SNMP agent.

Syntax

config snmpagentaddress del [**-p** *port-num*] [**-v** *vrf-name*] *agentip*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config snmpagentaddress del -v mgmt -p 123 21.22.13.14
```

1.9 config snmptrap del

Function

Run the **config snmptrap del** command to delete the SNMP Trap server IP address to which SNMP agent is expected to send TRAPs. When users had added the trap server IP as part of "mgmt" VRF, users should specify the optional vrf_name parameter as "mgmt" while deleting as well. This configuration is removed from snmpd.conf that is used by SNMP agent. SNMP service is restarted to make this configuration effective in SNMP agent.

Syntax

config snmptrap del [**-p** *port-num*] [**-v** *vrf-name*] [**-c** *community*] *trapserverip*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config snmptrap del -v mgmt -p 123 21.22.13.14
```

1.10 config snmptrap modify

Function

Run the **config snmptrap modify** command to modify the SNMP trap server IP address to which the SNMP agent is expected to send the traps. Users can configure one server IP addrss for each SNMP version to send the traps. When SNMP agent is expected to send traps as part of management VRF, users should specify the optional vrf_name parameter as "mgmt". This configuration goes into snmpd.conf that is used by SNMP agent. SNMP service is restarted to make this configuration effective in SNMP agent.

Syntax

config snmptrap modify [*snmp-version*] [**-p** *port-num*] [**-v** *vrf-name*] [**-c** *community*] *trapserverip*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config snmptrap modify 2 -p 456 -v mgmt 21.21.21.21

For this example, configuration goes into /etc/snmp/snmpd.conf inside snmp docker as
follows. When "-v" parameter is not used, the additional "%" in the following line will not be
present. In case of SNMPv1, "trapsink" will be updated, in case of v2, "trap2sink" will be
updated and in case of v3, "informsink" will be updated.

trap2sink 31.31.31.31:456%mgmt public
```

1.11 show runningconfiguration snmp

Function

Run the **show runningconfiguration snmp** command to display the global SNMP configuration that includes the location, contact, community, and user settings.

Syntax

show runningconfiguration snmp

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration snmp
Status
--------
enable



Location
------------
Emerald City

SNMP_CONTACT      SNMP_CONTACT_EMAIL
--------------   --------------------
joe                  joe@contoso.com


View         Type       OID
------      ------    -----
testview   include   1.3.6.1.2.1
```

```
Community String          Community Type          Source             View
------------------       ----------------       --------          ------
Jack                          RW                       172.31.240.48     testview1


User      Permission Type      Type      Auth Type      Auth Password      Encryption Type      Encryption
Password      View
------  -----------------  ------  -----------  ---------------  -----------------  ---------
------------  ------
Travis    RO                      Priv      SHA             TravisAuthPass     AES
TravisEncryptPass         testview1

```

1.12 show runningconfiguration snmp community

Function

Run the **show runningconfiguration snmp community** command to display the SNMP community settings.

Syntax

show runningconfiguration snmp community

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration snmp community
Community String          Community Type          Source             View
------------------       ----------------       --------          ------
testcom1                      RO
testcom2                      RO                       172.31.240.48 testview1
```

1.13 show runningconfiguration snmp contact

Function

Run the **show runningconfiguration snmp contact** command to display the SNMP contact setting.

Syntax

show runningconfiguration snmp contact

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration snmp contact
Contact      Contact Email
---------  ---------------
joe          joe@contoso.com
```

1.14 show runningconfiguration snmp location

Function

Run the **show runningconfiguration snmp location** command to display the SNMP location setting.

Syntax

show runningconfiguration snmp location

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration snmp location
Location
------------
Emerald City
```

1.15 show runningconfiguration snmp view

Function

Run the **show runningconfiguration snmp view** command to display the SNMP view setting.

Syntax

show runningconfiguration snmp view

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration snmp view
View         Type         OID
------       ------       -----
testview1 included    1.3.6.1.2.1
```

1.16 show runningconfiguration snmp user

Function

Run the **show runningconfiguration snmp user** command to display the SNMP user settings.

Syntax

show runningconfiguration snmp user

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show runningconfiguration snmp user
User      Permission Type      Type      Auth Type      Auth Password      Encryption Type      Encryption
Password      View
------   -----------------   ------   -----------   ---------------   -----------------   ---------
------------   ------
Travis    RO                      Priv      SHA              TravisAuthPass     AES
TravisEncryptPass
Joe        RO                      Priv      SHA              TravisAuthPass     AES
TravisEncryptPass         testview1

```
```
```

1.17 show snmpagentaddress

Function

Run the **show snmpagentaddress** command to display the configured SNMP agent IP addresses.

Syntax

show snmpagentaddress

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show snmpagentaddress
ListenIP        ListenPort   ListenVrf
----------   ------------   -----------
1.2.3.4                787   mgmt
```

1.18 show snmptrap

Function

Run the **show snmptrap** command to display the configured SNMP Trap server IP addresses.

Syntax

show snmptrap

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show snmptrap
  Version   TrapReceiverIP        Port   VRF     Community
---------   ----------------   ------   -----   -----------
        2   31.31.31.31            456      mgmt    public
```

1 RESTCONF Commands

Command	Function
config rest-server default certs	Configure X509 certificates for the REST server.
config rest-server default client-auth	Configure the authentication type of the REST server.
config rest-server default log-level	Configure the log output level for the REST server.
config rest-server default port	Configure the port of the REST server.
config rest-server default reset port	Configure the REST port of the REST server.
config rest-server default status	Enable or disable the REST server.
show rest-server default	Display the REST server configuration.

1.1 config rest-server default certs

Function

Run the **config rest-server default certs** command to configure X509 certificates for the REST server.

Syntax

config rest-server default certs *server-crt server-key ca-crt*

Parameter Description

server-crt: Config the x509 crt file path for server.

server-key: Config the x509 key file path for server.

ca-crt: Config the x509 ca file path for server.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config rest-server default certs /etc/sonic/certs/target.crt
/etc/sonic/certs/target.key /etc/sonic/certs/ca.crt
Restarting mgmt-framework service...
```

1.2 config rest-server default client-auth

Function

Run the **config rest-server default client-auth** command to configure the authentication type of the REST server.

Syntax

config rest-server default client-auth { **cert** | **none** | **user** }

Parameter Description

cert: Authentication With X.509 Certificates.

none: Without authentication.

user: Authentication With account.

Usage Guidelines

If client-auth is user, the port number of ssh server must be 22(default).

Examples

```
admin@sonic:~$ sudo config rest-server default client-auth cert
```

```
Restarting mgmt-framework service...
```

1.3 config rest-server default log-level

Function

Run the **config rest-server default log-level** command to configure the log output level for the REST server.

Syntax

config rest-server default log-level *log-level*

Parameter Description

log_level: The output log level, the value range is from 1 to 7.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config rest-server default log-level 5
Restarting mgmt-framework service...
```

1.4 config rest-server default port

Function

Run the **config rest-server default port** command to configure the port of the REST server.

Syntax

config rest-server default port *port-num*

Parameter Description

port-num: The port of rest server, the value range is from 1025 to 65535.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config rest-server default port 11443
Restarting mgmt-framework service...
```

1.5 config rest-server default reset port

Function

Run the **config rest-server default reset port** command to configure the REST port of the REST server.

Syntax

config rest-server default reset port

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config rest-server default reset port
Restarting mgmt-framework service...
```

1.6 config rest-server default status

Function

Run the **config rest-server default status** command to enable or disable the REST server.

Syntax

config rest-server default status { **enable** | **disable** }

Parameter Description

enable: Enable the rest server(default).

disable: Disable the rest server.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config rest-server default status enable
Restarting mgmt-framework service...
```

1.7 show rest-server default

Function

Run the **show rest-server default** command to display the REST server configuration.

Syntax

show rest-server default

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show rest-server default
status          enable
port            443
auth_type       none
log_level       2
server_crt      /etc/sonic/certs/target.crt
server_key      /etc/sonic/certs/target.key
ca_crt          /etc/sonic/certs/ca.crt
```

1 Telemetry Commands

Command	Function
config telemetry certs	Configure X509 certificates for telemetry.
config telemetry gnmi auth-type	Set the authentication type for the gNMI server.
config telemetry gnmi log-level	Set the log output level for the gNMI server.
config telemetry gnmi port-num	Set the port of the gNMI server.
config telemetry gnmi status	Enable or disable telemetry.
show telemetry certs	Display the telemetry certificate configuration.
show telemetry gnmi	Display the gNMI server configuration.

1.1 config telemetry certs

Function

Run the **config telemetry certs** command to configure X509 certificates for telemetry.

Syntax

config telemetry telemetry certs *server-crt server-key ca-crt*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config telemetry certs /etc/sonic/certs/target.crt /etc/sonic/certs/target.key
/etc/sonic/certs/ca.crt
Restarting telemetry service...
```

1.2 config telemetry gnmi auth-type

Note
If auth-type is password, the port number of ssh server must be 22(default).

Function

Run the **config telemetry gnmi auth-type** command to set the authentication type for the gNMI server.

Syntax

config telemetry gnmi auth-type { **cert** | **none** | **password** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config telemetry gnmi auth-type cert
Restarting telemetry service...
```

1.3 config telemetry gnmi log-level

Function

Run the **config telemetry gnmi log-level** command to set the log output level for the gNMI server.

Syntax

config telemetry gnmi log-level *log-level*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config telemetry gnmi log-level 5
Restarting telemetry service...
```

1.4 config telemetry gnmi port-num

Function

Run the **config telemetry gnmi port-num** command to set the port of the gNMI server.

Syntax

config telemetry gnmi port-num *port-num*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config telemetry gnmi port-num 8090
Restarting telemetry service...
```

1.5 config telemetry gnmi status

Function

Run the **config telemetry gnmi status** command to enable or disable telemetry.

Syntax

config telemetry gnmi status { **enable** | **disable** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config telemetry gnmi status enable
Restarting telemetry service...
```

1.6 show telemetry certs

Function

Run the **show telemetry certs** command to display the telemetry certificate configuration.

Syntax

show telemetry certs

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show telemetry certs
server_crt      /etc/sonic/certs/target.crt
server_key      /etc/sonic/certs/target.key
ca_crt              /etc/sonic/certs/ca.crt
```

1.7 show telemetry gnmi

Function

Run the **show telemetry gnmi** command to display the gNMI server configuration.

Syntax

show telemetry gnmi

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show telemetry gnmi
    status              enable
    port                  8090
    auth_type      none
    log_level      2      Location
```

1 VXLAN Commands

Command	Function
config vxlan	Add a VXLAN instance.
config vxlan evpn_nvo	Configure EVPN.
config vxlan mac capacity	Configure the dynamic MAC address table capacity of the VNI.
config vxlan mac filter	Configure the filter MAC address of the VNI.
config vxlan map	Configure VLAN-VNI mapping.
config vxlan remote-neigh-learn	Configure the remote learning ability.
config vxlan storm-control	Configure storm control for the VNI.
show vxlan interface	Display VXLAN VTEP information.
show vxlan mac-capacity	Display the dynamic MAC address table capacity of the VNI.
show vxlan mac-filter	Display the filter MAC address of the VNI.
show vxlan name	Display vxlan name configuration.
show vxlan storm-control	Display the storm control entries of the VNI.
show vxlan tunnel	Display brief information about all the vxlans configured in the device.
show vxlan tunnelcounters	Display VXLAN tunnel counters.
show vxlan remotevtep	Display VRF VNI mapping information.
show vxlan remotemac	Display the MAC addresses pointing to the remote VTEP.
show vxlan remotevni	Isplay the VLANs extended to the remote VTEP.
show vxlan vlanvnimap	Display VLAN VNI mapping information.
show vxlan vnicounters	Display VXLAN VNI counters.
show vxlan vrfvnimap	Display VRF VNI mapping information.

1.1 config vxlan

Function

Run the **config vxlan** command to add a VXLAN instance.

Syntax

config vxlan { **add** | **del** }[*OPTIONS*] *vxlan-name src-ip*

Parameter Description

vxlan_name: VTEP name.

src_ip: Sourece IP address of the VTEP.

Usage Guidelines

NOTE: VTEP must be created to use VXLAN, and a device can only have one VTEP. In the VXLAN+MCLAG scenario, when the actual physical port members of the tunnel mapping change, the tunnel needs to be deleted first, and the tunnel needs to be established after the port changes are completed.

Examples

```
admin@sonic:~$ sudo config vxlan add vtep1 1.0.0.1
admin@sonic:~$ sudo config vxlan del vtep1
```

1.2 config vxlan evpn_nvo

Function

Run the **config vxlan evpn_nvo** command to configure EVPN.

Syntax

config vxlan evpn_nvo [*OPTIONS*] { add | del } *nvo-name vxlan-name*

Parameter Description

vtep_name: VTEP name.

nvo_name: NVO name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config vxlan evpn_nvo add nvo vtep1
admin@sonic:~$ sudo config vxlan evpn_nvo del nvo
```

1.3 config vxlan mac capacity

Function

Run the **config vxlan mac capacity** command to configure the dynamic MAC address table capacity of the VNI.

Syntax

config vxlan mac capacity [*OPTIONS*] { add |del } *vni capacity-number*

Parameter Description

add: Add mac capacity

del: Del mac capacity

capacity_number: Total number of MAC addresses

vni: VXLAN ID

Usage Guidelines

NOTE: If you have learned an over-capacity MAC and then configure a MAC capacity limit, you can only wait for natural aging. If packets continue to hit the MAC, you need to clear the MAC table entry before the capacity limit can take effect.

Examples

```
admin@sonic:~$ sudo config vxlan mac capacity add 100011 100
admin@sonic:~$ sudo config vxlan mac capacity del 100011 100
```

1.4 config vxlan mac filter

Function

Run the **config vxlan mac filter** command to configure the filter MAC address of the VNI.

Syntax

config vxlan mac filter [*OPTIONS*] { add |del } *vni mac-address*

Parameter Description

add: Add mac filter.

del: Del mac filter.

mac_address: MAC address.

vni: VXLAN ID.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config vxlan mac filter add 100011 00:00:00:10:10:10
admin@sonic:~$ sudo config vxlan mac filter del 100011 00:00:00:10:10:10
```

1.5 config vxlan map

Function

Run the **config vxlan map** command to configure VLAN-VNI mapping.

Syntax

config vxlan map [*OPTIONS*] { **add** | **del** } *vtep-name vlan-id vni*

Parameter Description

add: Add VLAN-VNI map entry.

del: Del VLAN-VNI map entry.

vxlan_name: VTEP name.

vlan_id: VLAN ID.

vni: VXLAN ID.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config vxlan map add vtep1 11 100011
admin@sonic:~$ sudo config vxlan map del vtep1 11 100011
```

1.6 config vxlan remote-neigh-learn

Function

Run the **config vxlan remote-neigh-learn** command to configure the remote learning ability.

Syntax

config vxlan remote-neigh-learn *vtep-name* { **enable** | **disable** }

Parameter Description

vxlan_name: VTEP name.

enable: Enable remote-neigh-learn.

disable: Disable remote-neigh-learn.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config vxlan remote-neigh-learn enable
admin@sonic:~$ sudo config vxlan remote-neigh-learn disable
```

1.7 config vxlan storm-control

Function

Run the **config vxlan storm-control** command to configure storm control for the VNI.

Syntax

config vxlan storm-control [*OPTIONS*] { add | del } *vni* { **unicast** | **broadcast** | **multicast** } { **pps** *pps-value* | **kbps** *kbps-value* | **level** *level-value* }

Parameter Description

add: Add vxlan storm-control.

del: Del vxlan storm-control.

vni: VXLAN ID.

unicast: Unicast packet.

broadcast: Broadcast packet.

multicast: Multicast packet.

pps: Packets per second.

kbps: Kilobits per second.

level: Ratio of max rates.

pps-value: Value with pps unit.

kbps-value: Value with kbps unit.

level-value: Value with level unit.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config vxlan storm-control add 100011 unicast pps 1000
admin@sonic:~$ sudo config vxlan storm-control del 100011 unicast pps 1000
```

1.8 show vxlan interface

Function

Run the **show vxlan interface** command to display VXLAN VTEP information.

Syntax

show vxlan interface

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vxlan interface
VTEP Information:

        VTEP Name : vtep1, SIP    : 2.0.0.1
        NVO Name    : nvo,    VTEP : vtep1
        Source interface    : Loopback1
        Remote neigh learn: True
        Tunnel counting     : True, Period : 1000
        VNI counting        : True, Period : 1000
```

1.9 show vxlan mac-capacity

Function

Run the **show vxlan mac-capacity** command to display the dynamic MAC address table capacity of the VNI.

Syntax

show vxlan mac-capacity

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vxlan mac-capacity
+--------+----------------+
| VNI        | mac-capacity     |
+======+=============+
| 100011     |   100                |
+--------+----------------+
Total count : 1
```

1.10 show vxlan mac-filter

Function

Run the **show vxlan mac-filter** command to display the filter MAC address of the VNI.

Syntax

show vxlan mac-filter

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vxlan mac-filter
+---------+--------------------+
| VNI     | filter-mac         |
+=======+==================+
| 100011  | 00:00:00:00:00:22:22  |
+---------+--------------------+
Total count : 1
```

1.11 show vxlan name

Function

Run the **show vxlan name** command to display vxlan name configuration.

Syntax

show vxlan name *vxlan-name*

Parameter Description

vxlan_name: vxlan vtep name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vxlan name vtep1
vxlan tunnel name      source ip      destination ip      tunnel map name      tunnel map mapping(vni
-> vlan)
-------------------  -----------  ----------------  -----------------  ------------
```

```
vtep1                                   1.0.0.1
map_10_Vlan10                   10 -> Vlan10
```

1.12 show vxlan storm-control

Function

Run the **show vxlan storm-control** command to display the storm control entries of the VNI.

Syntax

show vxlan storm-control [*VNID*]

Parameter Description

VNID: VXLAN ID

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vxlan storm-control
VNI      Broadcast Control      Multicast Control      Unicast Control
------   -------------------   -------------------   -----------------
100011           10000   pps             10000   pps            1000   pps
100012              60     %                50     %             10000 kbps
admin@sonic:~$ show vxlan storm-control   100011
VNI      Broadcast Control      Multicast Control      Unicast Control
------   -------------------   -------------------   -----------------
100011           10000   pps             10000   pps            1000   pps
```

1.13 show vxlan tunnel

Function

Run the **show vxlan tunnel** command to display brief information about all the vxlans configured in the device.

It displays the vxlan tunnel name, source IP address, destination IP address (if configured), tunnel map name and mapping.

Syntax

show vxlan tunnel

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vxlan tunnel
vxlan tunnel name      source ip      destination ip      tunnel map name      tunnel map mapping(vni -> vlan)
-----------------      --------       -------------       -----------------    ---------------
vtep1                                 1.0.0.1             2.0.0.2
map_10_Vlan10                         10 -> Vlan10
```

1.14 show vxlan tunnelcounters

Function

Run the **show vxlan tunnelcounters** command to display VXLAN tunnel counters.

Syntax

show vxlan tunnelcounters

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vxlan tunnelcounters
Tunnel          RX_PKTS   RX_BYTES   RX_PPS    RX_BPS   TX_PKTS   TX_BYTES   TX_PPS    TX_BPS
------------  --------  --------  ------  -------  -------  --------  ------  -------
EVPN_2.0.0.1      1234   1512034     10/s    1.1KB/s     2234   2235235     23/s   2.2KB/s
EVPN_3.2.3.2      2344   162034      15/s    1.5KB/s      200     55235      2/s   0.2KB/s
```

1.15 show vxlan remotevtep

Function

Run the **show vxlan remotevtep** command to display VRF VNI mapping information.

Syntax

show vxlan remotevtep

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vxlan remotevtep
+---------+---------+------------------+-------------+
| SIP     | DIP     | Creation Source  | OperStatus  |
+=========+=========+==================+=============+
| 1.0.0.1 | 2.0.0.1 | EVPN             | oper_up     |
+---------+---------+------------------+-------------+
Total count : 1
```

1.16 show vxlan remotemac

Function

Run the **show vxlan remotemac** command to display the MAC addresses pointing to the remote VTEP.

Syntax

show vxlan remotemac [*vtep-ip* | **all**] [**count**]

Parameter Description

vtep-ip: VTEP with the specificed IP address

all: All VTEPs

count: Number of remote MAC addresses

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vxlan remotemac all
+-------+-----------------+-------------+------+---------+
| VLAN  | MAC             | RemoteVTEP  |  VNI | Type    |
+=======+=================+=============+======+=========+
| Vlan11| 00:00:00:12:30:10| 2.0.0.1    | 100011| dynamic |
+-------+-----------------+-------------+------+---------+
Total count : 1

admin@sonic:~$ show vxlan remotemac 2.0.0.1
+--------+---------------+-------------+------+--------+
| VLAN   | MAC           | RemoteVTEP  |  VNI | Type   |
+========+===============+=============+======+========+
```

```
| Vlan11    | 00:00:00:12:30:10      | 2.0.0.1             |   100011 | dynamic |
+--------+-----------------+--------------+------+--------+
Total count : 1
```

1.17 show vxlan remotevni

Function

Run the **show vxlan remotevni** command to isplay the VLANs extended to the remote VTEP.

Syntax

show vxlan remotevni [*vtep-ip* | **all**]

Parameter Description

vtep-ip: VTEP with the specificed IP address.

all: All VTEPs.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vxlan remotevni all
+--------+-------------+-----------+
| VLAN       | RemoteVTEP    |    VNI          |
+======+==============+=====+
| Vlan11     | 2.0.0.1              |     100011    |
+--------+-------------+-----------+
Total count : 1

admin@sonic:~$ show vxlan remotevni 2.0.0.1
+--------+-------------+-----------+
| VLAN       | RemoteVTEP    |    VNI          |
+======+===========+========+
| Vlan11     | 2.0.0.1             |      100011    |
+--------+-------------+-----------+
Total count : 1
```

1.18 show vxlan vlanvnimap

Function

Run the **show vxlan vlanvnimap** command to display VLAN VNI mapping information.

Syntax

show vxlan vlanvnimap

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vxlan vlanvnimap
+--------+--------+
| VLAN    |      VNI |
+========+========+
| Vlan11 | 100011 |
+--------+--------+
| Vlan12 | 100012 |
+--------+--------+
Total count : 2
```

1.19 show vxlan vnicounters

Function

Run the **show vxlan vnicounters** command to display VXLAN VNI counters.

Syntax

show vxlan vnicounters

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vxlan vnicounters
VNI       RX_PKTS   RX_BYTES   RX_PPS    RX_BPS   TX_PKTS   TX_BYTES   TX_PPS    TX_BPS
--------  --------  --------  ------  -------  -------  --------  ------  -------
100010       1234    1512034     10/s    1.1KB/s      2234    2235235     23/s   2.2KB/s
```

1.20 show vxlan vrfvnimap

Function

Run the **show vxlan vrfvnimap** command to display VRF VNI mapping information.

Syntax

show vxlan vrfvnimap

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vxlan vrfvnimap
+-------+---------+
| VRF     |     VNI     |
+=======+==========+
| Vrf1    |    100011 |
+-------+---------+
Total count : 1
```

1 Vnet Commands

Command	Function
show vnet brief	Display brief information about all the vnets configured in the device.
show vnet interfaces	Display vnet interfaces information about all the vnets configured in the device.
show vnet name	Display brief information about vnet name configured in the device.
show vnet neighbors	Display vnet neighbor information about all the vnets configured in the device.
show vnet routes all	Display all routes information about all the vnets configured in the device.
show vnet routes tunnel	Display tunnel routes information about all the vnets configured in the device.

1.1 show vnet brief

Function

Run the **show vnet brief** command to display brief information about all the vnets configured in the device.

It displays the vnet name, vxlan tunnel name, vni and peer list (if configured).

Syntax

show vnet brief

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vnet brief
vnet name      vxlan tunnel        vni   peer list
-----------  --------------  -----  ------------------
Vnet_2000      tunnel1             2000
Vnet_3000      tunnel1             3000   Vnet_2000,Vnet4000E
```

1.2 show vnet interfaces

Function

Run the **show vnet interfaces** command to display vnet interfaces information about all the vnets configured in the device.

Syntax

show vnet interfaces

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vnet interfaces
vnet name      interfaces
```

```
-----------  ------------
Vnet_2000     Ethernet1
Vnet_3000     Vlan2000
```

1.3 show vnet name

Function

Run the **show vnet name** command to display brief information about vnet name configured in the device.

Syntax

show vnet name *vnet-name*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vnet name Vnet_3000
vnet name      vxlan tunnel         vni   peer list
-----------  --------------  -----  ------------------
Vnet_3000      tunnel1             3000   Vnet_2000,Vnet4000
```

1.4 show vnet neighbors

Function

Run the **show vnet neighbors** command to display vnet neighbor information about all the vnets configured in the device.

It displays the vnet name, neighbor IP address, neighbor mac address (if configured) and interface.

Syntax

show vnet neighbors

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vnet neighbors
Vnet_2000      neighbor       mac_address      interfaces
-----------   -----------   -------------   ------------
                    11.11.11.11                          Ethernet1
                    11.11.11.12                          Ethernet1

Vnet_3000      neighbor       mac_address       interfaces
-----------   -----------   -----------------   ------------
                20.20.20.20     aa:bb:cc:dd:ee:ff      Vlan2000
```

1.5 show vnet routes all

Function

Run the **show vnet routes all** command to display all routes information about all the vnets configured in the device.

Syntax

show vnet routes all

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vnet routes all
vnet name      prefix              nexthop      interface
-----------   --------------   ---------   -----------
Vnet_2000      100.100.3.0/24                 Ethernet52
Vnet_3000      100.100.4.0/24                 Vlan2000

vnet name      prefix              endpoint      mac address            vni
-----------   --------------   ----------   -----------------   -----
Vnet_2000      100.100.1.1/32   10.10.10.1
Vnet_3000      100.100.2.1/32   10.10.10.2    00:00:00:00:03:04
```

1.6 show vnet routes tunnel

Function

Run the **show vnet routes tunnel** command to display tunnel routes information about all the vnets configured in the device.

Syntax

show vnet routes tunnel

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show vnet routes tunnel
vnet name      prefix              endpoint      mac address            vni
-----------  --------------  ----------  -----------------  -----
Vnet_2000      100.100.1.1/32   10.10.10.1
Vnet_3000      100.100.2.1/32   10.10.10.2    00:00:00:00:03:04
```

1 RDMA Commands

Command	Function
config buffer pool	Configure a custom pool.
config buffer profile	Configure a lossless buffer profile.
config buffer shared-headroom-pool	Configure the shared headroom pool.
config ecn	Configures the possible fields in a particular WRED profile that is specified using "**-profile** *profile-name*" argument.
config interface buffer priority-group lossless	Configure the priority groups on which lossless traffic runs.
config interface buffer queue	Configure the buffer profiles for queues.
config interface cable_length	Configure the length of the cable connected to a port. The cable_length is in unit of meters and must be suffixed with "m".
config pfcwd action	Configure the PFC-deadlock recovery action.
config pfcwd detect-precision	Configure the PFC-deadlock detection precision.
config pfcwd set	Configure the detection times and recovery time of the PFC watchdog for different priority groups.
show buffer configuration	Display the status of buffer pools and profiles currently configured.
show buffer statistics	Display the status of buffer statictis currently deployed to the ASIC.
show ecn	Display all the WRED profiles that are configured in the device.
show pfc asymmetric	Display the status of asymmetric PFC for all interfaces or a given interface.
show pfc counters	Display the details of Rx & Tx priority-flow-control (pfc) for all ports. This command can be used to clear the counters using -

	c option.
show pfc priority	Display the lossless priorities for all interfaces or a given interface.
show pfcwd config	Shows current PFC Watchdog configuration.
show pfcwd stats	Shows current PFC Watchdog statistics (storms detected, packets dropped, etc).

1.1 config buffer pool

Function

Run the **config buffer pool** command to configure a custom pool.

Syntax

config buffer pool set <pool_name> [-t (ingress | egress)] [-m <mode>] [-x <xoff>] [-s <size>]

config buffer pool remove *pool-name*

Parameter Description

- -t, --type [ingress | egress]:
  buffer pool type [required]
- -m, --mode [static]:
  buffer pool mode
- -x, --xoff INTEGER:
  buffer global headroom pool size
- -s, --size INTEGER:
  buffer shared pool size

Usage Guidelines

Configuring the global headroom size may cause device traffic interruption, with the maximum interruption time being approximately 1.5 seconds.

Examples

```
admin@sonic:~$ sudo config buffer pool set def_ingress_pool -t ingress -x 2560 -s 2560000
admin@sonic:~$ sudo config buffer pool remove def_ingress_pool
```

1.2 config buffer profile

Function

Run the **config buffer profile** command to configure a lossless buffer profile.

Syntax

config buffer profile { **add** | **set** } *profile-name* **--pool** *pool-name* **--mode** { **static** | **dynamic** } [**--xon** *xon-threshold*] [**--xon_offset** *xon-offset_threshold*] [**--xoff** *xoff-threshold*] [**--size** *size*] [**--dynamic_th** *dynamic-th* | **--static_th** *static-th*]

config buffer profile remove *profile-name*

Parameter Description

add: The command is designed for adding a new buffer profile to the system.

set: The command is designed for modifying an existing buffer profile in the system.

For a profile with dynamically calculated headroom information, only **dynamic_th** can be modified.

remove: The command is designed for removing an existing buffer profile from the system. When removing a profile, it shouldn't be referenced by any entry in **CONFIG_DB.BUFFER_PG**.

Usage Guidelines

All the parameters are devided to two groups, one for headroom and one for dynamic_th. For any command at lease one group of parameters should be provided.

For headroom parameters:

xon is madantory.

- If shared headroom pool is disabled:
  - At lease one of **xoff** and **size** should be provided and the other will be optional and conducted via the formula **xon** + **xoff** = **size**.
  - **xon** + **xoff** <= **size**.
- If shared headroom pool is enabled:
  - **xoff** should be provided.
  - **size** = **xoff** if it is not provided.

If only **dynamic_th** parameter is provided, the **headroom_type** will be set as **dynamic** and **xon**, **xoff** and **size** won't be set. This is only used for non default dynamic_th. In this case, the profile won't be deployed to ASIC directly. It can be configured to a lossless PG and then a dynamic profile will be generated based on the port's speed, cable length, and MTU and deployed to the ASIC.

NOTE

- If the buffer configuration fails when applying it to a port priority-group, the reason might be an incorrectly input profile name or applying the exit configuration to the port priority-group.
- Applying a buffer profile to a port priority-group may cause device traffic interruption, with the maximum interruption time being approximately 1.5 seconds.
- Making configuration changes after applying a buffer profile to a port priority-group may cause device traffic interruption, with the maximum interruption time being approximately 1.5 seconds.
- Removing a buffer profile from an applied port priority-group may cause device traffic interruption, with the maximum interruption time being approximately 1.5 seconds.
- MMU cache configuration should not be configured under traffic, as there is a probability of cache deadlock.
- Making configuration changes after applying a buffer profile to a port queue may cause device traffic interruption, with the maximum interruption time being approximately 1.5 seconds.
- Removing a buffer profile from an applied port queue may cause device traffic interruption, with the maximum interruption time being approximately 1.5 seconds.

Examples

```
admin@sonic:~$ sudo config buffer profile add --mode static --size 2560 --xoff 2560 --static_th
25600 --pool ingress_lossy_pool profile11
admin@sonic:~$ sudo config buffer profile remove profile1
```

1.3 config buffer shared-headroom-pool

Function

Run the **config buffer shared-headroom-pool** command to configure the shared headroom pool.

The shared headroom pool can be enabled in the following ways:

- Configure the over subscribe ratio. In this case, the size of shared headroom pool is calculated as the accumulative xoff of all of the lossless PG divided by the over subscribe ratio.
- Configure the size.

In case both of the above parameters have been configured, the **size** will take effect. To disable shared headroom pool, configure both parameters to zero.

Syntax

config buffer shared-headroom-pool { **over-subscribe-ratio** *over-subscribe-ratio* | **size** *size* }

Parameter Description

over-subscribe-ratio: The range of over-subscribe-ratio is from 1 to number of ports inclusive.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config shared-headroom-pool over-subscribe-ratio 2
admin@sonic:~$ sudo config shared-headroom-pool size 1024000
```

1.4 config ecn

Function

Run the **config ecn** command to configures the possible fields in a particular WRED profile that is specified using "**-profile** *profile-name*" argument.

The list of the WRED profile fields that are configurable is listed in the below "Usage".

Syntax

config ecn set -profile *profile-name* **-rmax** *red-threshold-max* **-rmin** *red-threshold-min* **-ymax** *yellow-threshold-max* **-ymin** *yellow-threshold-min* **-gmax** *green-threshold-max* **-gmin** *green-threshold-min* **-rdrop** *red-drop-probability* **-ydrop** *yellow-drop-probability* **-gdrop** *green-drop-probability* **--weight** *sampling-weight*

config ecn enable *profile-name* { **none** | **green** | **yellow** | **red** | **green_yellow** | **green_red** | **yellow_red** | **all** }

config ecn apply -profile *profile-name* **-queue_map** *queue-map* **-port** *interface-name*

Parameter Description

profile-name: Profile name.

Usage Guidelines

N/A

Examples

Configures the "max threshold" for the WRED profile name "wredprofileabcd". It will create the WRED profile if it does not exist.

```
admin@sonic:~$ sudo config ecn set -profile default -rmax 5080 -rmin 2540 -ymax 5080 -ymin 2540
-gmax 5080 -gmin 2540 -rdrop 20 -ydrop 20 -gdrop 20
admin@sonic:~$ sudo config ecn enable default all
admin@sonic:~$ sudo config ecn apply -profile default -queue_map 0-2 -port Ethernet1
```

1.5 config interface buffer priority-group lossless

Function

Run the **config interface buffer priority-group lossless** command to configure the priority groups on which lossless traffic runs.

Syntax

config interface buffer priority-group lossless { { { **add** | **set** } *interface-name pg-map* [*profile*] } | { **remove** *interface-name* [*pg-map*] } }

Parameter Description

pg-map: The parameter represents the map of priorities for lossless traffic. It should be a string and in form of a bit map like 3-4. The - connects the lower bound and upper bound of a range of priorities. It can be in one of the following two forms:

- For a range of priorities, the lower bound and upper bound connected by a dash, like 3-4.
- For a single priority, the number, like 6.

add: The command is designed for adding a new lossless PG on top of current PGs. The new PG range must be disjoint with all existing PGs.

For example, currently the PG range 3-4 exist on port Ethernet4, to add PG range 4-5 will fail because it isn't disjoint with 3-4. To add PG range 5-6 will succeed. After that both range 3-4 and 5-6 will work as lossless PG.

profile: The parameter is optional. When provided, it represents the predefined buffer profile for headroom override.

set: The command is designed for modifying an existing PG from dynamic calculation to headroom override or vice versa. The pg-map must be an existing PG.

remove: The command is designed for removing an existing PG. The option pg-map must be an existing PG. All lossless PGs will be removed in case no pg-map provided.

Usage Guidelines

N/A

Examples

To configure lossless_pg on a port:

```
admin@sonic:~$ sudo config interface buffer priority-group lossless add Ethernet0 3-4
```

To change the profile used for lossless_pg on a port:

```
admin@sonic:~$ sudo config interface buffer priority-group lossless set Ethernet0 3-4 new-profile
```

To remove one lossless priority from a port:

```
admin@sonic:~$ sudo config interface buffer priority-group lossless remove Ethernet0 6
```

To remove all lossless priorities from a port:

```
admin@sonic:~$ sudo config interface buffer priority-group lossless remove Ethernet0
```

1.6 config interface buffer queue

Function

Run the **config interface buffer queue** command to configure the buffer profiles for queues.

Syntax

config interface buffer queue add *interface-name queue-map profile*

config interface buffer queue set *interface-name queue-map profile*

config interface buffer queue remove *interface-name queue-map*

Parameter Description

add: The command is designed for adding a buffer profile for a group of queues. The new queue range must be disjoint with all queues with buffer profile configured.

For example, currently the buffer profile configured on queue 3-4 on port Ethernet4, to configure buffer profile on queue 4-5 will fail because it isn't disjoint with 3-4. To configure it on range 5-6 will succeed.

profile: The parameter represents a predefined egress buffer profile to be configured on the queues.

queue-map: The parameter represents the map of queues. It can be in one of the following two forms:

- For a range of priorities, the lower bound and upper bound connected by a dash, like 3-4.
- For a single priority, the number, like 6.

set: The command is designed for modifying an existing group of queues.

remove: The command is designed for removing buffer profile on an existing group of queues.

Usage Guidelines

N/A

Examples

To configure buffer profiles for queues on a port:

```
admin@sonic:~$ sudo config interface buffer queue add Ethernet0 3-4 egress_lossless_profile
```

To change the profile used for queues on a port:

```
admin@sonic:~$ sudo config interface buffer queue set Ethernet0 3-4 new-profile
```

To remove a group of queues from a port:

```
admin@sonic:~$ sudo config interface buffer queue remove Ethernet0 3-4
```

1.7 config interface cable_length

Function

Run the **config interface cable_length** command to configure the length of the cable connected to a port. The cable_length is in unit of meters and must be suffixed with "m".

Syntax

config interface cable_length *interface-name cable-length*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config interface cable_length Ethernet0 40m
```

1.8 config pfcwd action

Function

Run the **config pfcwd action** command to configure the PFC-deadlock recovery action.

Syntax

config pfcwd action { **drop** | **forward** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config pfcwd action forward
```

1.9 config pfcwd detect-precision

Function

Run the **config pfcwd detect-precision** command to configure the PFC-deadlock detection precision.

Syntax

config pfcwd detect-precision *detect-precision*

Parameter Description

N/A

Usage Guidelines

NOTE:

The PFC watchdog function can be enabled only after the PFC watchdog attributes are configured for a queue.
PFC deadlock does not take effect during hot restart of the syncd container.

Examples

```
admin@sonic:~$ sudo config pfcwd detect-precision 100
```

1.10 config pfcwd set

Function

Run the **config pfcwd set** command to configure the detection times and recovery time of the PFC watchdog for different priority groups.

Syntax

config pfcwd set *priority-group* [**-d** *detection_time*] [**-r** *restoration_time*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config pfcwd set 1 -d 10 -r 100
admin@sonic:~$ sudo config pfcwd start Ethernet1 0-2
```

1.11 show buffer configuration

Function

Run the **show buffer configuration** command to display the status of buffer pools and profiles currently configured.

Syntax

show buffer configuration

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show buffer configuration
  Lossless traffic pattern:
  --------------------  -
  default_dynamic_th     0
  over_subscribe_ratio   0
  --------------------  -


  Pool: ingress_lossless_pool
```

```
----  --------
type  ingress
mode  dynamic
----  --------

Pool: egress_lossless_pool
----  --------
type  egress
mode  dynamic
size  34340822
----  --------

Pool: ingress_lossy_pool
----  --------
type  ingress
mode  dynamic
----  --------

Pool: egress_lossy_pool
----  --------
type  egress
mode  dynamic
----  --------

Profile: q_lossy_profile
----------  ------------------------------
dynamic_th  3
pool        [BUFFER_POOL:egress_lossy_pool]
size        0
----------  ------------------------------

Profile: egress_lossy_profile
----------  ------------------------------
dynamic_th  3
pool        [BUFFER_POOL:egress_lossy_pool]
size        4096
----------  ------------------------------

Profile: egress_lossless_profile
----------  --------------------------------
dynamic_th  7
pool        [BUFFER_POOL:egress_lossless_pool]
size        0
----------  --------------------------------

Profile: ingress_lossless_profile
```

```
----------  ----------------------------------
dynamic_th   0
pool         [BUFFER_POOL:ingress_lossless_pool]
size         0
----------  ----------------------------------

Profile: ingress_lossy_profile
----------  ---------------------------------
dynamic_th   3
pool         [BUFFER_POOL:ingress_lossy_pool]
size         0
----------  ---------------------------------
```

1.12 show buffer statistics

Function

Run the **show buffer statistics** command to display the status of buffer statictis currently deployed to the ASIC.

Syntax

show buffer statistics priority-group [**-p** *port-name*]

show buffer statistics queue [**-p** *port-name*]

Parameter Description

port-name: Port name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show buffer statistics priority-group -p Ethernet2
    Port       Priority Group       Guaranteed Used       Guaranteed Available       Share Used       Share
Available       Headroom Used       Headroom Available
---------  ----------------  ------------------  ----------------------  ------------  -------
----------  ---------------  --------------------
  Ethernet2                    0                  4096                          0             2304
26234624                     0                     0
  Ethernet2                    1                  4096                          0         14324736
11912192                     0                     0
  Ethernet2                    2                  4096                          0             1536
26235392                     0                     0
  Ethernet2                    3                  4096                          0             5376
26231552                     0                     0
```

```
  Ethernet2                4              4096                    0          1024
26235904                   0                 0
  Ethernet2                5              2560                    0       1789440          0
81920                      0
  Ethernet2                6              4096                    0       5313792
20923136                   0                 0
  Ethernet2                7              4096                    0         16896
26220032                   0                 0

admin@sonic:~$ show buffer statistics queue -p Ethernet6
    Port       Queue      Guaranteed Used      Guaranteed Available      Share Used      Share Available
---------  -------  -----------------  ----------------------  ------------  ----------------
-
   Ethernet6        UC0              7424                     0          5376             6157056
   Ethernet6        UC1          14366208                     0      14364160                   0
   Ethernet6        UC2              4352                     0          3328             6159104
   Ethernet6        UC3             11008                     0          9984             6152448
   Ethernet6        UC4              7424                     0          5376             6157056
   Ethernet6        UC5           1873920                     0       1871360             3674828
   Ethernet6        UC6           5289216                     0       5287168              875264
   Ethernet6        UC7             10240                     0          8192             6154240
```

1.13 show ecn

Function

Run the **show ecn** command to display all the WRED profiles that are configured in the device.

Syntax

show ecn { **apply** | **config** | **stat** }

Parameter Description

N/A

Usage Guidelines

NOTE:

- The possible cause for an ECN-WRED profile configuration failure is that the configured attribute value is beyond the configurable range.
- WRED/ECN statistics are collected based on the interface and not queue-specific.
- ECN only supports 32-bit statistics counters. If the limit is exceeded, counters are reset.
- The WRED drop function takes effect only for WRED packets (ECN flag: 00) and does not take effect for ECN packets (ECN flag: 01/10/11). The ECN function takes effect only for ECN packets.
- For the M2-W6930-64QC, the ECN counter collects congestion statistics on the ingress

packets with the ECN field set to 11.

Examples

```
admin@sonic:~$ show ecn config
  Profile      Green Max_th      Green Min_th      Green Drop_pro      Yellow Max_th      Yellow Min_th
Yellow Drop_pro      Red Max_th      Red Min_th      Red Drop_pro      Weight      Ecn Enable
---------  --------------  --------------  ----------------  ---------------  ---------------
-----------------  ------------  ------------  --------------  --------  ------------
  default             5080             2540                20             5080             2540
20            5080            2540               20           0        ecn_none
```

```
admin@sonic:~$ show ecn apply
  Interface      Queue      Ecn Wred Profile
-----------  -------  ------------------
  Ethernet6          5                   wredred
```

1.14 show pfc asymmetric

Function

Run the **show pfc asymmetric** command to display the status of asymmetric PFC for all interfaces or a given interface.

Syntax

show pfc asymmetric [*interface-name*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show pfc asymmetric

  Interface      Asymmetric
  -----------  ------------
  Ethernet0       off
  Ethernet2       off
  Ethernet4       off
  Ethernet6       off
  Ethernet8       off
  Ethernet10     off
  Ethernet12     off
```

```
  Ethernet14     off

admin@sonic:~$ show pfc asymmetric Ethernet0

  Interface      Asymmetric
  -----------   ------------
  Ethernet0      off
```

1.15 show pfc counters

Function

Run the **show pfc counters** command to display the details of Rx & Tx priority-flow-control (pfc) for all ports. This command can be used to clear the counters using -c option.

Syntax

show pfc counters

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show pfc counters
    Port Rx      PFC0     PFC1     PFC2     PFC3     PFC4     PFC5     PFC6     PFC7
    -----------  ------  ------  ------  ------  ------  ------  ------  ------
    Ethernet0         0        0        0        0        0        0        0        0
    Ethernet4         0        0        0        0        0        0        0        0
    Ethernet8         0        0        0        0        0        0        0        0
    Ethernet12        0        0        0        0        0        0        0        0

    Port Tx      PFC0     PFC1     PFC2     PFC3     PFC4     PFC5     PFC6     PFC7
    -----------  ------  ------  ------  ------  ------  ------  ------  ------
    Ethernet0         0        0        0        0        0        0        0        0
    Ethernet4         0        0        0        0        0        0        0        0
    Ethernet8         0        0        0        0        0        0        0        0
Ethernet12        0        0        0        0        0        0        0        0
...
```

Note

PFC counters can be cleared by the user with the following command:

```
admin@sonic:~$ sonic-clear pfccounters
```

1.16 show pfc priority

Function

Run the **show pfc priority** command to display the lossless priorities for all interfaces or a given interface.

Syntax

show pfc priority [*interface-name*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show pfc priority

  Interface       Lossless priorities
  -----------   ---------------------
  Ethernet0       3,4
  Ethernet2       3,4
  Ethernet8       3,4
  Ethernet10      3,4
  Ethernet16      3,4

admin@sonic:~$ show pfc priority Ethernet0

  Interface       Lossless priorities
  -----------   ---------------------
  Ethernet0       3,4
```

1.17 show pfcwd config

Function

Run the **show pfcwd config** command to shows current PFC Watchdog configuration.

Syntax

show pfcwd config

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~/hhh$ show pfcwd config
Detect Precision: 10ms
Recovery Action: forward
  Queue      Detect Time      Recovery Time(ms)
-------  -------------  -------------------
  UC5                15                    150
```

1.18 show pfcwd stats

Function

Run the **show pfcwd stats** command to shows current PFC Watchdog statistics (storms detected, packets dropped, etc).

Syntax

show pfcwd stats

Parameter Description

packet-group: Group to which the protocol belongs.

Usage Guidelines

N/A

Examples

```
admin@sonic:~/hhh$ show pfcwd stats -port Ethernet6
  Interface      QUEUE      Count      Status
  -----------  -------  -------  --------
  Ethernet6        UC0          0
  Ethernet6        UC1          0
  Ethernet6        UC2          0
  Ethernet6        UC3          0
  Ethernet6        UC4          0
  Ethernet6        UC5       2379   DETECTED
  Ethernet6        UC6          0
  Ethernet6        UC7          0
  Ethernet6        UC8          0
  Ethernet6        UC9          0
```

1 Troubleshooting Commands

Command	Function
bgp advertise lowest-priority on-startup	Configure BGP to minimize the priorities of the BGP routes to be advertised upon system restart.

1.1 bgp advertise lowest-priority on-startup

Function

Run the **bgp advertise lowest-priority on-startup** command to configure BGP to minimize the priorities of the BGP routes to be advertised upon system restart.

Syntax

[**no**] **bgp advertise lowest-priority on-startup** [*recover-time*]

Parameter Description

recover-time: The time for restoring the priority of the advertised routes, in seconds. The value ranges from 1 to 65535, and the default value is 600.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "router bgp 100" -c "bgp advertise lowest-priority on-startup"
```

1.2 bgp advertise lowest-priority on-startup

Function

Run the **bgp advertise lowest-priority on-startup** command to configure the configuration of delayed route advertisement upon system restart.

Syntax

[**no**] **bgp initial-advertise-delay** { *delay-time* [*startup-time*] | **prefix-list** *name*}

Parameter Description

delay-time: The delay time for advertising routes after the BGP neighborship is established upon system restart, in seconds. The value ranges from 1 to 600. The default value is 1.

startup-time: The time for system restart (the mechanism of delayed route advertisement is adopted for the neighbor in this period), in seconds. The value range is from 5 to 58400. The default value is 600.

name: The name of the prefix list.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "router bgp 100" -c "bgp initial-advertise-delay 60 500" -c "bgp initial-advertise-delay prefix-list aa"
```

1.3 bgp evpn-vni-list

Function

Run the **bgp evpn-vni-list** command to configure the EVPN VNI list.

Syntax

[**no**] **bgp evpn-vni-list** *list-name vni-list*

Parameter Description

list-name: The name of a VNI list.

vni-list: The VNI ID list. The value ranges from 1 to 16777215. The information of multiple VNIs can be configured at the same time, and all the VNIs are separated using commas.

Usage Guidelines

When the local host goes online, BGP will send the host ARP routing information to its neighbors. However, if the peer end does not want to generate traffic redirection through ARP, you can control the local ARP routes so that local ARP routes are not sent to the peer end. This command combines route map and is used on neighbors.

Examples

```
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "bgp evpn-vni-list v1 100,200"
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "route-map map1 deny 10" -c "match evpn
deny-arp v1 local"
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "route-map map1 permit 20"
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "router bgp 65530" -c "address-family l2vpn
evpn" -c "neighbor 13.1.1.1 activate" -c "neighbor 13.1.1.1 route-map map1 out"
```

1.4 clear bgp advertise lowest-priority on-startup

Function

Run the **clear bgp advertise lowest-priority on-startup** command to restore the priorities of the BGP routes advertised to neighbors.

Syntax

clear bgp advertise lowest-priority on-startup

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo vtysh -c "clear bgp advertise lowest-priority on-startup"
```

1.5 config auto-techsupport global max-core-limit

Function

Run the **config auto-techsupport global max-core-limit** command to configure global max-core-limit.

Syntax

config auto-techsupport global max-core-limit *limit*

Parameter Description

limit: A percentage value should be specified. This signifies maximum size to which /var/core/ directory can be grown until.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config auto-techsupport global max-core-limit 10.15
```

1.6 config auto-techsupport global max-techsupport-limit

Function

Run the **config auto-techsupport global max-techsupport-limit** command to configure global max-techsupport-limit.

Syntax

config auto-techsupport global max-techsupport-limit *limit*

Parameter Description

limit: A percentage value should be specified. This signifies maximum size to which /var/core/ directory can be grown until.

Usage Guidelines

N/A

Examples

```
config auto-techsupport global max-techsupport-limit 10.15
```

1.7 config auto-techsupport global rate-limit-interval

Function

Run the **config auto-techsupport global rate-limit-interval** command to configure global rate-limit-interval.

Syntax

config auto-techsupport global rate-limit-interval *interval*

Parameter Description

interval: Minimum time in seconds to wait after the last techsupport creation time before invoking a new one.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config auto-techsupport global rate-limit-interval 200
```

1.8 config auto-techsupport global since

Function

Run the **config auto-techsupport global since** command to configure the time the logs & core-dumps generated.

Syntax

config auto-techsupport global since *date-string*

Parameter Description

date-string: This limits the auto-invoked techsupport to only collect the logs & core-dumps generated since the time provided. Any valid date string of the formats specified here can be used. (https://www.gnu.org/software/coreutils/manual/html_node/Date-input-formats.html). If this value is not explicitly configured or a non-valid string is provided, a default value of "2 days ago" is used.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config auto-techsupport global since “3 days ago”
```

1.9 config auto-techsupport global state

Function

Run the **config auto-techsupport global state** command to configure global state.

Syntax

config auto-techsupport global state { **enabled** | **disabled** }

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config auto-techsupport global state enabled
```

1.10 config auto-techsupport-feature add

Function

Run the **config auto-techsupport global add** command to add feature.

Syntax

config auto-techsupport-feature add *feature-name* **--state** [**enabled** | **disabled**] **--rate-limit-interval** *rate-limit-interval*

Parameter Description

state: enable/disable the capability for the specific feature/container.

rate-limit-interval: Rate limit interval for the corresponding feature. Configure 0 to explicitly disable. For the techsupport to be generated by auto-techsupport, both the global and feature specific rate-limit-interval has to be passed

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config auto-techsupport-feature add bgp --state enabled --rate-limit-interval 200
```

1.11 config auto-techsupport-feature delete

Function

Run the **config auto-techsupport-feature delete** command to delete feature.

Syntax

config auto-techsupport-feature delete *feature-name*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config auto-techsupport-feature delete swss
```

1.12 config auto-techsupport-feature update

Function

Run the **config auto-techsupport-feature update** command to update feature.

Syntax

- **config auto-techsupport-feature update** *feature-name* **--state** [**enabled** | **disabled**]
- **config auto-techsupport-feature update** *feature-name* **--rate-limit-interval** *rate-limit-interval*

Parameter Description

state: enable/disable the capability for the specific feature/container.

rate-limit-interval: Rate limit interval for the corresponding feature. Configure 0 to explicitly disable. For the techsupport to be generated by auto-techsupport, both the global and feature specific rate-limit-interval has to be passed

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config auto-techsupport-feature update snmp --state enabled
admin@sonic:~$ sudo config auto-techsupport-feature update swss --rate-limit-interval 200
```

1.13 redistribute

Function

Run the **redistribute** command to redistribute the route information of other routing protocols to BGP.

Syntax

[**no**] **redistribute** [**arp-host** | **nd-route**]

Parameter Description

arp-host: Host routes converted from ARP entries.

nd-route: Host routes converted from ND entries.

Usage Guidelines

Redistribution arp-host added to IPv4 unicast address family Redistribution nd route added to IPv6 unicast address family.

Examples

```
admin@sonic:~$ sudo vtysh -c "configure terminal" -c "router bgp 100" -c "address-family ipv4
unicast" -c "redistribute arp-host" -c "address-family ipv6 unicast" -c "redistribute nd-route"
```

1.14 show auto-techsupport global

Function

Run the **show auto-techsupport global** command to display auto-techsupport global status.

Syntax

show auto-techsupport global

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show auto-techsupport global
STATE            RATE LIMIT INTERVAL (sec)        MAX TECHSUPPORT LIMIT (%)        MAX CORE LIMIT (%)
SINCE
-------    --------------------------      -------------------------       ------------------
----------
```

```
enabled                                    180                                    10.0
5.0         2 days ago
```

1.15 show auto-techsupport history

Function

Run the **show auto-techsupport history** command to display auto-techsupport history.

Syntax

show auto-techsupport global

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show auto-techsupport history
TECHSUPPORT DUMP                                    TRIGGERED BY          CORE DUMP
----------------------------------------    --------------    ------------------------------
sonic_dump_r-lionfish-16_20210901_221402     bgp
bgpcfgd.1630534439.55.core.gz
sonic_dump_r-lionfish-16_20210901_203725      snmp
python3.1630528642.23.core.gz
sonic_dump_r-lionfish-16_20210901_222408      teamd
python3.1630535045.34.core.gz
```

1.16 show auto-techsupport-feature

Function

Run the **show auto-techsupport-feature** command to display auto-techsupport feature status.

Syntax

show auto-techsupport-feature

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show auto-techsupport-feature
FEATURE NAME          STATE                RATE LIMIT INTERVAL (sec)
--------------     --------     -------------------------
bgp                      enabled                                      600
database                enabled                                    600
dhcp_relay             enabled                                   600
lldp                      enabled                                     600
swss                      disabled                                    800
```

1.17 show bgp evpn-vni-list

Function

Run the **show bgp evpn-vni-list** command to display the VNI list configuration of EVPN.

Syntax

show bgp evpn-vni-list *list-name*

Parameter Description

list-name: The name of a VNI list.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo vtysh -c "show bgp evpn-vni-list "
bgp evpn-vni-list v1:
10 20
```

1.18 show ip bgp neighbors

Function

Run the **show ip bgp neighbors** command to display all the details of IPv4 & IPv6 BGP neighbors when no optional argument is specified.

Syntax

show ip bgp neighbors [*ipv4-address* [**advertised-routes** | **received-routes** | **routes**]]

Parameter Description

N/A

Usage Guidelines

When the optional argument IPv4_address is specified, it displays the detailed neighbor information about that specific IPv4 neighbor.

Command has got additional optional arguments to display only the advertised routes, or the received routes, or all routes.

In order to get details for an IPv6 neighbor, use "show ipv6 bgp neighbor *ipv6-address*" command.

Examples

```
admin@sonic:~$ show ip bgp neighbors
BGP neighbor is 192.168.1.161, remote AS 65501, local AS 65061, external link
  Description: Router01T0
    BGP version 4, remote router ID 1.2.3.4
    BGP state = Established, up for 08w5d14h
    Last read 00:00:46, hold time is 180, keepalive interval is 60 seconds
    Neighbor capabilities:
        4 Byte AS: advertised and received
        Dynamic: received
        Route refresh: advertised and received(old & new)
        Address family IPv4 Unicast: advertised and received
        Graceful Restart Capabilty: advertised and received
            Remote Restart timer is 120 seconds
            Address families by peer:
                IPv4 Unicast(not preserved)
    Graceful restart informations:
        End-of-RIB send: IPv4 Unicast
        End-of-RIB received: IPv4 Unicast
    Message statistics:
        Inq depth is 0
        Outq depth is 0
                                         Sent               Rcvd
        Opens:                              1                  1
        Notifications:                      0                  0
        Updates:                        14066                  3
        Keepalives:                     88718              88698
        Route Refresh:                      0                  0
        Capability:                         0                  0
        Total:                         102785              88702
    Minimum time between advertisement runs is 30 seconds

  For address family: IPv4 Unicast
    Community attribute sent to this neighbor(both)
    2 accepted prefixes

    Connections established 1; dropped 0
```

```
    Last reset never
Local host: 192.168.1.160, Local port: 32961
Foreign host: 192.168.1.161, Foreign port: 179
Nexthop: 192.168.1.160
Nexthop global: fe80::f60f:1bff:fe89:bc00
Nexthop local: ::
BGP connection: non shared network
Read thread: on      Write thread: off
```

Optionally, you can specify an IP address in order to display only that particular neighbor. In this mode, you can optionally specify whether you want to display all routes advertised to the specified neighbor, all routes received from the specified neighbor or all routes (received and accepted) from the specified neighbor.

Examples:

```
admin@sonic:~$ show ip bgp neighbors 192.168.1.161

admin@sonic:~$ show ip bgp neighbors 192.168.1.161 advertised-routes

admin@sonic:~$ show ip bgp neighbors 192.168.1.161 received-routes

admin@sonic:~$ show ip bgp neighbors 192.168.1.161 routes
```

1.19 show ip bgp summary

Function

Run the **show ip bgp summary** command to display the summary of all IPv4 bgp neighbors that are configured and the corresponding states.

Syntax

show ip bgp summary

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ip bgp summary
BGP router identifier 1.2.3.4, local AS number 65061
RIB entries 6124, using 670 KiB of memory
Peers 2, using 143 KiB of memory

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
```

```
192.168.1.161          4 65501       88698      102781                0          0          0 08w5d14h
2
192.168.1.163          4 65502       88698      102780                0          0          0 08w5d14h
2

Total number of neighbors 2
```

1.20 show ipv6 bgp neighbors

Function

Run the **show ipv6 bgp neighbors** command to all the details of one particular IPv6 Border Gateway Protocol (BGP) neighbor. Option is also available to display only the advertised routes, or the received routes, or all routes.

Syntax

show ipv6 bgp neighbors [*ipv6-address* [**advertised-routes** | **received-routes** | **routes**]]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ipv6 bgp neighbors fc00::72 advertised-routes

admin@sonic:~$ show ipv6 bgp neighbors fc00::72 received-routes

admin@sonic:~$ show ipv6 bgp neighbors fc00::72 routes
```

1.21 show ipv6 bgp summary

Function

Run the **show ipv6 bgp summary** command to display the summary of all IPv6 bgp neighbors that are configured and the corresponding states.

Syntax

show ipv6 bgp summary

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ipv6 bgp summary
BGP router identifier 10.1.0.32, local AS number 65100
RIB entries 12809, using 1401 KiB of memory
Peers 8, using 36 KiB of memory

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
fc00::72        4 64600   12588   12591        0       0       0 06:51:17
6402
fc00::76        4 64600   12587    6190        0       0       0 06:51:28
6402
fc00::7a        4 64600   12587    9391        0       0       0 06:51:23
6402
fc00::7e        4 64600   12589   12592        0       0       0 06:51:25
6402

Total number of neighbors 4
```

1.22 show route-map

Function

Run the **show route-map** command to display the routing policy that takes precedence over the other route processes that are configured.

Syntax

show route-map

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show route-map
ZEBRA:
route-map RM_SET_SRC, permit, sequence 10
    Match clauses:
    Set clauses:
        src 10.12.0.102
    Call clause:
    Action:
        Exit routemap
```

```
ZEBRA:
route-map RM_SET_SRC6, permit, sequence 10
    Match clauses:
    Set clauses:
        src fc00:1::102
    Call clause:
    Action:
        Exit routemap
BGP:
route-map FROM_BGP_SPEAKER_V4, permit, sequence 10
    Match clauses:
    Set clauses:
    Call clause:
    Action:
        Exit routemap
BGP:
route-map TO_BGP_SPEAKER_V4, deny, sequence 10
    Match clauses:
    Set clauses:
    Call clause:
    Action:
        Exit routemap
BGP:
route-map ISOLATE, permit, sequence 10
    Match clauses:
    Set clauses:
        as-path prepend 65000
    Call clause:
    Action:
        Exit routemap
```

1 System State Commands

Command	Function
show mmu	Display virtual address to the physical address translation status of the Memory Management Unit (MMU).
show processes cpu	Display the current CPU usage by process.
show processes memory	Display the current memory usage by processes.
show processes summary	Display the current summary information about all the processes.
show services	Display the state of all the SONiC processes running inside a docker container.
show system-health detail	Display the current status of 'Services' and 'Hardware' under monitoring.
show system-health monitor-list	Display a list of all current 'Services' and 'Hardware' being monitored, their status and type.
show system-health summary	Display the current status of 'Services' and 'Hardware' under monitoring.
show system-memory	Display the system-wide memory utilization information – just a wrapper over linux native “free” command.
show system-storage	Display storage usage of the device.

1.1 show mmu

Function

Run the **show mmu** command to display virtual address to the physical address translation status of the Memory Management Unit (MMU).

Syntax

show services

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show mmu
Pool: ingress_lossless_pool
----    --------
xoff    4194112
type    ingress
mode    dynamic
size    10875072
----    --------

Pool: egress_lossless_pool
----    --------
type    egress
mode    static
size    15982720
----    --------

Pool: egress_lossy_pool
----    -------
type    egress
mode    dynamic
size    9243812
----    -------

Profile: egress_lossy_profile
----------    ------------------------------
dynamic_th    3
pool          [BUFFER_POOL|egress_lossy_pool]
size          1518
```

```
----------    ------------------------------

Profile: pg_lossless_100000_300m_profile
----------    ----------------------------------
xon_offset    2288
dynamic_th    -3
xon           2288
xoff          268736
pool          [BUFFER_POOL|ingress_lossless_pool]
size          1248
----------    ----------------------------------

Profile: egress_lossless_profile
---------    ----------------------------------
static_th    3995680
pool         [BUFFER_POOL|egress_lossless_pool]
size         1518
---------    ----------------------------------

Profile: pg_lossless_100000_40m_profile
----------    ----------------------------------
xon_offset    2288
dynamic_th    -3
xon           2288
xoff          177632
pool          [BUFFER_POOL|ingress_lossless_pool]
size          1248
----------    ----------------------------------

Profile: ingress_lossy_profile
----------    ----------------------------------
dynamic_th    3
pool          [BUFFER_POOL|ingress_lossless_pool]
size          0
----------    ----------------------------------

Profile: pg_lossless_40000_40m_profile
----------    ----------------------------------
xon_offset    2288
dynamic_th    -3
xon           2288
xoff          71552
pool          [BUFFER_POOL|ingress_lossless_pool]
size          1248
----------    ----------------------------------
```

1.2 show processes cpu

Function

Run the **show processes cpu** command to display the current CPU usage by process.

Syntax

show processes cpu

Parameter Description

N/A

Usage Guidelines

This command uses linux's "top -bn 1 -o %CPU" command to display the output.

Users can pipe the output to "head" to display only the "n" number of lines (e.g., show processes cpu | head -n 10).

Advanced users can view individual processes using variations of the ps command (e.g., ps -ax | grep <process name>).

Examples

```
admin@sonic:~$ show processes cpu
top - 23:50:08 up   1:18,   1 user,   load average: 0.25, 0.29, 0.25
Tasks: 161 total,   1 running, 160 sleeping,   0 stopped,   0 zombie
%Cpu(s):   3.8 us,   1.0 sy,   0.0 ni, 95.1 id,   0.1 wa,   0.0 hi,   0.0 si,   0.0 st
KiB Mem:    8181216 total,   1161060 used,   7020156 free,    105656 buffers
KiB Swap:         0 total,         0 used,         0 free.    557560 cached Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+
COMMAND
   2047 root      20   0  683772 109288  39652 S  23.8  1.3   7:44.79 syncd
   1351 root      20   0   43360   5616   2844 S  11.9  0.1   1:41.56 redis-server
10093 root      20   0   21944   2476   2088 R   5.9  0.0   0:00.03 top
      1 root      20   0   28992   5508   3236 S   0.0  0.1   0:06.42 systemd
      2 root      20   0       0      0      0 S   0.0  0.0   0:00.00
kthreadd
      3 root      20   0       0      0      0 S   0.0  0.0   0:00.56
ksoftirqd/0
      5 root       0 -20       0      0      0 S   0.0  0.0   0:00.00
kworker/0:0H
...
```

1.3 show processes memory

Function

Run the **show processes memory** command to display the current memory usage by processes.

Syntax

show processes memory

Parameter Description

N/A

Usage Guidelines

This command uses linux's "top -bn 1 -o %MEM" command to display the output.

NOTE that pipe option can be used using " | head -n" to display only the "n" number of lines.

Examples

```
admin@sonic:~$ show processes memory
top - 23:41:24 up 7 days, 39 min,  2 users,  load average: 1.21, 1.19, 1.18
Tasks: 191 total,   2 running, 189 sleeping,   0 stopped,   0 zombie
%Cpu(s):  2.8 us, 20.7 sy,  0.0 ni, 76.3 id,  0.0 wa,  0.0 hi,  0.2 si,  0.0 st
KiB Mem :  8162264 total,  5720412 free,  945516 used,  1496336 buff/cache
KiB Swap:        0 total,        0 free,        0 used.  6855632 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+
COMMAND
18051 root      20   0  851540 274784   8344 S   0.0  3.4   0:02.77 syncd
17760 root      20   0 1293428 259212  58732 S   5.9  3.2  96:46.22 syncd
    508 root      20   0  725364  76244  38220 S   0.0  0.9   4:54.49 dockerd
30853 root      20   0   96348  56824   7880 S   0.0  0.7   0:00.98 show
17266 root      20   0  509876  49772  30640 S   0.0  0.6   0:06.36 docker
24891 admin     20   0  515864  49560  30644 S   0.0  0.6   0:05.54 docker
17643 admin     20   0  575668  49428  30628 S   0.0  0.6   0:06.29 docker
23885 admin     20   0  369552  49344  30840 S   0.0  0.6   0:05.57 docker
18055 root      20   0  509076  49260  30296 S   0.0  0.6   0:06.36 docker
17268 root      20   0  371120  49052  30372 S   0.0  0.6   0:06.45 docker
  1227 root      20   0  443284  48640  30100 S   0.0  0.6   0:41.91 docker
23785 admin     20   0  443796  48552  30128 S   0.0  0.6   0:05.58 docker
17820 admin     20   0  435088  48144  29480 S   0.0  0.6   0:06.33 docker
    506 root      20   0 1151040  43140  23964 S   0.0  0.5   8:51.08 containerd
18437 root      20   0   84852  26388   7380 S   0.0  0.3  65:59.76 python3.6
```

1.4 show processes summary

Function

Run the **show processes summary** command to display the current summary information about all the processes.

Syntax

show processes summary

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show processes summary
PID     PPID CMD                                          %MEM %CPU
1          0 /sbin/init                                  0.0   0.0
2          0 [kthreadd]                                    0.0   0.0
3          2 [ksoftirqd/0]                               0.0   0.0
5          2 [kworker/0:0H]                              0.0   0.0
...
```

1.5 show services

Function

Run the **show services** command to display the state of all the SONiC processes running inside a docker container.

Syntax

show services

Parameter Description

N/A

Usage Guidelines

This helps to identify the status of SONiC's critical processes.

Examples

```
admin@sonic:~$ show services
dhcp_relay              docker
----------------------------
```

```
UID                PID     PPID     C STIME TTY                  TIME CMD
root                 1        0     0 05:26 ?                00:00:12 /usr/bin/python /usr/bin/supervi
root                24        1     0 05:26 ?                00:00:00 /usr/sbin/rsyslogd -n

nat            docker
----------------------------
USER               PID PPID     C STIME TTY                  TIME CMD
root                 1        0     0 05:26 ?                00:00:12 /usr/bin/python /usr/bin/supervisord
root                18        1     0 05:26 ?                00:00:00 /usr/sbin/rsyslogd -n
root                23        1     0 05:26 ?                00:00:01 /usr/bin/natmgrd
root                34        1     0 05:26 ?                00:00:00 /usr/bin/natsyncd

snmp           docker
----------------------------
UID                PID     PPID     C STIME TTY                  TIME CMD
root                 1        0     0 05:26 ?                00:00:16 /usr/bin/python /usr/bin/supervi
root                24        1     0 05:26 ?                00:00:02 /usr/sbin/rsyslogd -n
Debian-+            29        1     0 05:26 ?                00:00:04 /usr/sbin/snmpd -f -LS4d -u Debi
root                31        1     1 05:26 ?                00:15:10 python3.6 -m sonic_ax_impl

syncd          docker
----------------------------
UID                PID     PPID     C STIME TTY                  TIME CMD
root                 1        0     0 05:26 ?                00:00:13 /usr/bin/python /usr/bin/supervi
root                12        1     0 05:26 ?                00:00:00 /usr/sbin/rsyslogd -n
root                17        1     0 05:26 ?                00:00:00 /usr/bin/dsserve /usr/bin/syncd
root                27       17 22 05:26 ?                04:09:30 /usr/bin/syncd --diag -p /usr/sh
root                51       27     0 05:26 ?                00:00:01 /usr/bin/syncd --diag -p /usr/sh

swss           docker
----------------------------
UID                PID     PPID     C STIME TTY                  TIME CMD
root                 1        0     0 05:26 ?                00:00:29 /usr/bin/python /usr/bin/supervi
root                25        1     0 05:26 ?                00:00:00 /usr/sbin/rsyslogd -n
root                30        1     0 05:26 ?                00:00:13 /usr/bin/orchagent -d /var/log/s
root                42        1     1 05:26 ?                00:12:40 /usr/bin/portsyncd -p /usr/share
root                45        1     0 05:26 ?                00:00:00 /usr/bin/intfsyncd
root                48        1     0 05:26 ?                00:00:03 /usr/bin/neighsyncd
root                59        1     0 05:26 ?                00:00:01 /usr/bin/vlanmgrd
root                92        1     0 05:26 ?                00:00:01 /usr/bin/intfmgrd
root              3606        1     0 23:36 ?                00:00:00 bash -c /usr/bin/arp_update; sle
root              3621     3606     0 23:36 ?                00:00:00 sleep 300

...
```

1.6 show system-health detail

Function

Run the **show system-health detail** command to display the current status of 'Services' and 'Hardware' under monitoring.

Syntax

show system-health detail

Parameter Description

N/A

Usage Guidelines

If any of the elements under each of these two sections is 'Not OK' a proper message will appear under the relevant section. In addition, displays a list of all current 'Services' and 'Hardware' being monitored and a list of ignored elements.

Examples

```
admin@sonic:~$ show system-health detail
System status summary

System status LED      red
Services:
    Status: Not OK
    Not Running: 'telemetry', 'orchagent'
Hardware:
    Status: OK

System services and devices monitor list

Name                       Status         Type
--------------    --------    ----------
telemetry                Not OK         Process
orchagent                 Not OK         Process
neighsyncd              OK                Process
vrfmgrd                   OK                Process
dialout_client     OK                Process
zebra                       OK                Process
rsyslog                   OK                Process
snmpd                       OK                Process
redis_server          OK                Process
intfmgrd                  OK                Process
vxlanmgrd                 OK                Process
lldpd_monitor        OK                Process
portsyncd                 OK                Process
```

```
var-log                 OK              Filesystem
lldpmgrd                OK              Process
syncd                   OK              Process
sonic                   OK              System
buffermgrd              OK              Process
portmgrd                OK              Process
staticd                 OK              Process
bgpd                    OK              Process
lldp_syncd              OK              Process
bgpcfgd                 OK              Process
snmp_subagent           OK              Process
root-overlay            OK              Filesystem
fpmsyncd                OK              Process
sflowmgrd               OK              Process
vlanmgrd                OK              Process
nbrmgrd                 OK              Process
PSU 2                   OK              PSU
psu_1_fan_1             OK              Fan
psu_2_fan_1             OK              Fan
fan11                   OK              Fan
fan10                   OK              Fan
fan12                   OK              Fan
ASIC                    OK              ASIC
fan1                    OK              Fan
PSU 1                   OK              PSU
fan3                    OK              Fan
fan2                    OK              Fan
fan5                    OK              Fan
fan4                    OK              Fan
fan7                    OK              Fan
fan6                    OK              Fan
fan9                    OK              Fan
fan8                    OK              Fan

System services and devices ignore list

Name                Status      Type
------------    --------    ------
psu.voltage     Ignored     Device
```

1.7 show system-health monitor-list

Function

Run the **show system-health monitor-list** command to display a list of all current 'Services' and 'Hardware' being monitored, their status and type.

Syntax

show system-health monitor-list

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show system-health monitor-list
System services and devices monitor list

Name                       Status          Type
--------------     --------     ----------
telemetry                Not OK          Process
orchagent                Not OK          Process
neighsyncd               OK                 Process
vrfmgrd                    OK                 Process
dialout_client     OK                 Process
zebra                      OK                 Process
rsyslog                   OK                 Process
snmpd                      OK                 Process
redis_server          OK                 Process
intfmgrd                  OK                 Process
vxlanmgrd                OK                 Process
lldpd_monitor        OK                 Process
portsyncd                OK                 Process
var-log                    OK                 Filesystem
lldpmgrd                 OK                 Process
syncd                      OK                 Process
sonic                      OK                 System
buffermgrd               OK                 Process
portmgrd                  OK                 Process
staticd                   OK                 Process
bgpd                       OK                 Process
lldp_syncd               OK                 Process
bgpcfgd                    OK                 Process
snmp_subagent        OK                 Process
root-overlay          OK                 Filesystem
fpmsyncd                 OK                 Process
sflowmgrd                OK                 Process
vlanmgrd                  OK                 Process
nbrmgrd                   OK                 Process
PSU 2                      OK                 PSU
```

```
psu_1_fan_1          OK                Fan
psu_2_fan_1          OK                Fan
fan11                OK                Fan
fan10                OK                Fan
fan12                OK                Fan
ASIC                 OK                ASIC
fan1                 OK                Fan
PSU 1                OK                PSU
fan3                 OK                Fan
fan2                 OK                Fan
fan5                 OK                Fan
fan4                 OK                Fan
fan7                 OK                Fan
fan6                 OK                Fan
fan9                 OK                Fan
fan8                 OK                Fan
```

1.8 show system-health summary

Function

Run the **show system-health summary** command to display the current status of 'Services' and 'Hardware' under monitoring.

Syntax

show system-health summary

Parameter Description

N/A

Usage Guidelines

If any of the elements under each of these two sections is 'Not OK' a proper message will appear under the relevant section.

Examples

```
admin@sonic:~$ show system-health summary
System status summary

System status LED      red
Services:
    Status: Not OK
    Not Running: 'telemetry', 'sflowmgrd'
Hardware:
    Status: OK
admin@sonic:~$ show system-health summary
System status summary
```

```
System status LED      green
Services:
    Status: OK
Hardware:
    Status: OK
```

1.9 show system-memory

Function

Run the **show system-memory** command to display the system-wide memory utilization information – just a wrapper over linux native “free” command.

Syntax

show system-memory

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show system-memory
Command: free -m -h
                     total               used               free            shared           buffers
cached
Mem:                 3.9G               2.0G               1.8G                33M               324M
791M
-/+ buffers/cache:                951M               2.9G
Swap:                  0B                 0B                 0B
```

1.10 show system-storage

Function

Run the **show system-storage** command to display storage usage of the device.

Syntax

show system-storage

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show system-storage
Filesystem              Size      Used Avail Use% Mounted on
udev                    3.9G         0  3.9G   0% /dev
tmpfs                   785M        15M  770M   2% /run
root-overlay            32G      6.1G   24G  21% /
/dev/sda3               32G      6.1G   24G  21% /host
/dev/loop1              3.9G     335M  3.4G   9% /var/log
tmpfs                   3.9G         0  3.9G   0% /dev/shm
tmpfs                   5.0M         0  5.0M   0% /run/lock
tmpfs                   4.0M         0  4.0M   0% /sys/fs/cgroup
overlay                 32G      6.1G   24G  21%
/var/lib/docker/overlay2/7286b36addf78df670ebe51207156d4f62c7e948258ec105720de2a962faea47
/merged
...
```

1 Static routing Commands

Command	Function
config route add	Add a static route. Note that prefix /nexthop vrf`s and interface name are optional.
config route del	Remove a static route. Note that prefix /nexthop vrf`s and interface name are optional.
show ip route	Display either all the route entries from the routing table or an ipv4 specific route.

1.1 config route add

Function

Run the **config route add** command to add a static route. Note that prefix /nexthop vrf`s and interface name are optional.

Syntax

config route add prefix [**vrf** *vrf-name*] *A.B.C.D/M* **nexthop** { [**vrf** *vrf-name*] *A.B.C.D* | **dev** *dev-name* }

Parameter Description

vrf *vrf-name*: Name of the VRF bound with a prefix or nexthop.

A.B.C.D/M: IP address with mask.

A.B.C.D: IP address.

dev *dev-name*: Interface name.

Usage Guidelines

Configure a static ARP entry and add a static route that uses the static ARP entry as the next hop. After the static ARP entry is deleted, it disappears from the show arp command output, but the route on the chip does not change. That is, the neighbor entry on the chip still exists. In this case, the static route always takes effect.

The neighbor is deleted from the chip only after all the routes bound to the static ARP are deleted.

Examples

```
admin@sonic:~$ config route add prefix 2.2.3.4/32 nexthop 30.0.0.9
```

It also supports ECMP, and adding a new nexthop to the existing prefix will complement it and not overwrite them.

```
admin@sonic:~$ sudo config route add prefix 2.2.3.4/32 nexthop vrf Vrf-RED 30.0.0.9
admin@sonic:~$ sudo config route add prefix 2.2.3.4/32 nexthop vrf Vrf-BLUE 30.0.0.10
```

1.2 config route del

Function

Run the **config route del** command to remove a static route. Note that prefix /nexthop vrf`s and interface name are optional.

Syntax

config route del prefix [**vrf** *vrf-name*] *A.B.C.D/M* **nexthop** { [**vrf** *vrf name*] *A.B.C.D*] | **dev** *dev-name* }

Parameter Description

vrf *vrf-name*: Name of the VRF bound with a prefix or nexthop.

A.B.C.D/M: IP address with mask.

A.B.C.D: IP address.

dev *dev-name*: Interface name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config route del prefix 2.2.3.4/32 nexthop vrf Vrf-RED 30.0.0.9
admin@sonic:~$ sudo config route del prefix 2.2.3.4/32 nexthop vrf Vrf-BLUE 30.0.0.10
```

1.3 show ip route

Function

Run the **show ip route** command to display either all the route entries from the routing table or an ipv4 specific route.

Syntax

show ip route

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
               O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
               T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
               F - PBR, f - OpenFabric,
               > - selected route, * - FIB route, q - queued, r - rejected, b - backup

S>* 0.0.0.0/0 [200/0] via 192.168.111.3, eth0, weight 1, 3d03h58m
S>      1.2.3.4/32 [1/0] via 30.0.0.7, weight 1, 00:00:06
C>* 10.0.0.18/31 is directly connected, Ethernet36, 3d03h57m
C>* 10.0.0.20/31 is directly connected, Ethernet40, 3d03h57m
```

1 Console Commands

Command	Function
config console add	Add a console port setting.
config console baud	Remove a console port setting.
config console del	Remove a console port setting.
config console disable	Disable SONiC console switch feature.
config console enable	Enable SONiC console switch feature.
config console flow_control	Enable or disable flow control feature for a console port.
config console remote_device	Update the remote device name for a console port.
show line	Display serial port or a virtual network connection status.
connect device	Connect to a remote device via console line with an interactive cli.
connect line	Connect to a remote device via console line with an interactive cli.
sonic-clear line	Remote device via console line with an interactive cli.

1.1 config console add

Function

Run the **config console add** command to add a console port setting.

Syntax

config console add port-name [**--baud** | **-b** *baud-rate*] [**--flowcontrol** | **-f**] [**--devicename** | **-d** *remote-device*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ config console add 1 --baud 9600 --devicename switch1
```

1.2 config console baud

Function

Run the **config console baud** command to remove a console port setting.

Syntax

config console baud *port-name baud-rate*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config console baud 1 9600
```

1.3 config console del

Function

Run the **config console del** command to remove a console port setting.

Syntax

config console add port-name *port-name*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config console del 1
```

1.4 config console disable

Function

Run the **config console disable** command to disable SONiC console switch feature.

Syntax

config console disable

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config console disable
```

1.5 config console enable

Function

Run the **config console enable** command to enable SONiC console switch feature.

Syntax

config console enable

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config console enable
```

1.6 config console flow_control

Function

Run the **config console flow_control** command to enable or disable flow control feature for a console port.

Syntax

config console flow_control { **enable** | **disable** } **port-name**

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config console flow_control enable 1
```

1.7 config console remote_device

Function

Run the **config console remote_device** command to update the remote device name for a console port.

Syntax

config console remote_device *port-name remote-device*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config console remote_device 1 switch1
```

1.8 show line

Function

Run the **show line** command to display serial port or a virtual network connection status.

Syntax

show line [**-b** | **--breif**]

Parameter Description

N/A

Usage Guidelines

Optionally, you can display configured console ports only by specifying the `-b` or `--breif` flag.

Examples

```
admin@sonic:~$ show line
  Line      Baud      Flow Control      PID      Start Time      Device
------  ------  --------------  -----  ------------  --------
     1      9600           Enabled        -               -     switch1
     2         -          Disabled        -               -
     3         -          Disabled        -               -
     4         -          Disabled        -               -
     5         -          Disabled        -               -
```

```
admin@sonic:~$ show line -b
  Line      Baud      Flow Control      PID      Start Time      Device
------  ------  --------------  -----  ------------  --------
     1      9600           Enabled        -               -     switch1
```

1.9 connect device

Function

Run the **connect device** command to connect to a remote device via console line with an interactive cli.

Syntax

connect device *devicename*

Parameter Description

N/A

Usage Guidelines

The command is same with “connect line --devicename <devicename>”.

Examples

```
admin@sonic:~$ connect line 1
Successful connection to line 1
Press ^A ^X to disconnect
```

1.10 connect line

Function

Run the **connect line** command to connect to a remote device via console line with an interactive cli.

Syntax

connect line *target* [**-d** | **--devicename**]

Parameter Description

N/A

Usage Guidelines

By default, the target is “port_name”.

Optionally, you can connect with a remote device name by specifying the `-d` or `--devicename` flag

Examples

```
admin@sonic:~$ connect line 1
Successful connection to line 1
Press ^A ^X to disconnect
```

```
admin@sonic:~$ connect line --devicename switch1
Successful connection to line 1
Press ^A ^X to disconnect
```

1.11 sonic-clear line

Function

Run the **sonic-clear line** command to remote device via console line with an interactive cli.

Syntax

sonc-clear line *target* [**-d** | **--devicename**]

Parameter Description

N/A

Usage Guidelines

By default, the target is “port_name”.

Optionally, you can clear with a remote device name by specifying the `-d` or `--devicename` flag.

Examples

```
admin@sonic:~$ sonic-clear line 1
```

```
admin@sonic:~$ sonic-clear line --devicename switch1
```

1 Drop Counters Commands

Command	Function
config dropcounters add-reasons	Add drop reasons to an already initialized counter.
config dropcounters delete	Delete a drop counter.
config dropcounters install	Initialize a new drop counter. The user must specify a name, type, and initial list of drop reasons.
config dropcounters remove-reasons	Remove drop reasons from an already initialized counter.
show dropcounters capabilities	Show the drop counter capabilities that are available on this device. It displays the total number of drop counters that can be configured on this device as well as the drop reasons that can be configured for the counters.
show dropcounters configuration	Show the current running configuration of the drop counters on this device.
show dropcounters counts	Show the current statistics for the configured drop counters. Standard drop counters are displayed as well for convenience.
sonic-clear dropcounters	Clear drop counters.

1.1 config dropcounters add-reasons

Function

Run the **config dropcounters add-reasons** command to add drop reasons to an already initialized counter.

This command will fail if any of the specified drop reasons are not supported.

Syntax

config dropcounters add-reasons *counter-name reasons-list*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config dropcounters add-reasons DEBUG_2 [SIP_CLASS_E]
```

1.2 config dropcounters delete

Function

Run the **config dropcounters delete** command to delete a drop counter.

Syntax

config dropcounters delete *counter-name*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config dropcounters delete DEBUG_2
```

1.3 config dropcounters install

Function

Run the **config dropcounters install** command to initialize a new drop counter. The user must specify a name, type, and initial list of drop reasons.

Syntax

config dropcounters install *counter-name counter-type reasons-list* [**-d** *description*] [**-g** *group*] [**-a** *alias*]

Parameter Description

N/A

Usage Guidelines

This command will fail if the given name is already in use, if the type of counter is not supported, or if any of the specified drop reasons are not supported. It will also fail if all avaialble counters are already in use on the device.

Examples

```
admin@sonic:~$ sudo config dropcounters install DEBUG_2 PORT_INGRESS_DROPS
[EXCEEDS_L2_MTU,DECAP_ERROR] -d "More port ingress drops" -g BAD -a BAD_DROPS
```

1.4 config dropcounters remove-reasons

Function

Run the **config dropcounters remove-reasons** command to remove drop reasons from an already initialized counter.

Syntax

config dropcounters remove-reasons *counter-name reasons-list*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config dropcounters remove_reasons DEBUG_2 [SIP_CLASS_E]
```

1.5 show dropcounters capabilities

Function

Run the **show dropcounters capabilities** command to show the drop counter capabilities that are available on this device. It displays the total number of drop counters that can be configured on this device as well as the drop reasons that can be configured for the counters.

Syntax

show dropcounters capabilities

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show dropcounters capabilities
Counter Type                 Total
-------------------   -------
PORT_INGRESS_DROPS              3
SWITCH_EGRESS_DROPS             2

PORT_INGRESS_DROPS:
        L2_ANY
        SMAC_MULTICAST
        SMAC_EQUALS_DMAC
        INGRESS_VLAN_FILTER
        EXCEEDS_L2_MTU
        SIP_CLASS_E
        SIP_LINK_LOCAL
        DIP_LINK_LOCAL
        UNRESOLVED_NEXT_HOP
        DECAP_ERROR

SWITCH_EGRESS_DROPS:
        L2_ANY
        L3_ANY
        A_CUSTOM_REASON
```

1.6 show dropcounters configuration

Function

Run the **show dropcounters configuration** command to show the current running configuration of the drop counters on this device.

Syntax

show dropcounters configuration [**-g** *group-name*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show dropcounters configuration
Counter    Alias      Group  Type                  Reasons                Description
--------  --------  -----  ------------------  -------------------  -------------
DEBUG_0    RX_LEGIT   LEGIT  PORT_INGRESS_DROPS    SMAC_EQUALS_DMAC       Legitimate port-
level RX pipeline drops
                                                  INGRESS_VLAN_FILTER
DEBUG_1    TX_LEGIT   None   SWITCH_EGRESS_DROPS  EGRESS_VLAN_FILTER     Legitimate switch-
level TX pipeline drops

admin@sonic:~$ show dropcounters configuration -g LEGIT
Counter    Alias      Group  Type                  Reasons                Description
--------  --------  -----  ------------------  -------------------  -------------
DEBUG_0    RX_LEGIT   LEGIT  PORT_INGRESS_DROPS    SMAC_EQUALS_DMAC       Legitimate port-
level RX pipeline drops
                                                  INGRESS_VLAN_FILTER
```

1.7 show dropcounters counts

Function

Run the **show dropcounters counts** command to show the current statistics for the configured drop counters. Standard drop counters are displayed as well for convenience.

Because clear (see below) is handled on a per-user basis different users may see different drop counts.

Syntax

show dropcounters counts [**-g** *group-name*] [**-t** *counter-type*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show dropcounters counts
    IFACE     STATE     RX_ERR     RX_DROPS     TX_ERR     TX_DROPS    RX_LEGIT
---------  -------  ---------  -----------  ---------  -----------  ----------
Ethernet0         U         10          100          0            0          20
Ethernet4         U          0         1000          0            0         100
Ethernet8         U        100           10          0            0           0
```

```
admin@sonic:~$ show dropcounters counts -g LEGIT
    IFACE     STATE     RX_ERR     RX_DROPS     TX_ERR     TX_DROPS    RX_LEGIT
```

```
---------  -------  --------  ----------  --------  ----------  ---------
Ethernet0        U        10         100         0           0         20
Ethernet4        U         0        1000         0           0        100
Ethernet8        U       100          10         0           0          0
```

```
admin@sonic:~$ show dropcounters counts -t SWITCH_EGRESS_DROPS
DEVICE    TX_LEGIT
------  --------
sonic         1000
```

1.8 sonic-clear dropcounters

Function

Run the **sonic-clear dropcounters** command to clear drop counters.
This is done on a per-user basis.

Syntax

sonic-clear dropcounters

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sonic-clear dropcounters
Cleared drop counters
```

1 Feature Commands

Command	Function
config feature autorestart	Configure the status of auto-restart for a specific feature container.
config feature fallback	Fallback the feature.
config feature owner	Configure the owner for a feature as "local" or "kube".
config feature state	Configure the state for a specific feature.
show feature autorestart	Display the status of auto-restart for feature container.
show feature config	Show the config of given feature or all if no feature is given.
show feature status	Show the status of given feature or all if no feature is given.

1.1 config feature autorestart

Function

Run the **config feature autorestart** command to configure the status of auto-restart for a specific feature container.

Syntax

config feature autorestart *feature-name autorestart*

Parameter Description

N/A

Usage Guidelines

If the existing state or auto-restart value for a feature is "always_enabled" then config commands are don't care and will not update state/auto-restart value.

Examples

```
admin@sonic:~$ sudo config feature autorestart bgp disabled
```

1.2 config feature fallback

Function

Run the **config feature fallback** command to fallback the feature.

Syntax

config feature fallback *feature-name fallback*

Parameter Description

N/A

Usage Guidelines

Features configured for "kube" deployment could be allowed to fallback to using local image, until the point of successful kube deployment. The fallback is allowed by default.

Examples

```
admin@sonic:~$ sudo config feature fallback snmp on
```

1.3 config feature owner

Function

Run the **config feature owner** command to configure the owner for a feature as "local" or "kube".

Syntax

config feature owner *feature-name owner*

Parameter Description

N/A

Usage Guidelines

The "local" implies starting the feature container from local image. The "kube" implies that kubernetes server is made eligible to deploy the feature. The deployment of a feature by kubernetes is conditional based on many factors like, whether the kube server is configured or not, connected-to-kube-server or not and if that master has manifest for this feature for this switch or not and more. At some point in future, the deployment *could* happen and till that point the feature can run from local image, called "fallback". The fallback is allowed by default and it could be toggled to "not allowed". When fallback is not allowed, the feature would run only upon deployment by kubernetes master.

Examples

```
admin@sonic:~$ sudo config feature owner snmp kube
```

1.4 config feature state

Function

Run the **config feature state** command to configure the state for a specific feature.

Syntax

config feature state [**--block**] *feature-name state*

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config feature state bgp disabled
```

1.5 show feature autorestart

Function

Run the **show feature autorestart** command to display the status of auto-restart for feature container.

Syntax

show feature autorestart [*feature-name*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show feature autorestart
Feature        AutoRestart
-----------    --------------
bgp              enabled
database       always_enabled
dhcp_relay     enabled
lldp             enabled
pmon             enabled
radv            enabled
snmp             enabled
swss             enabled
syncd            enabled
teamd            enabled
telemetry       enabled
```

1.6 show feature config

Function

Run the **show feature config** command to show the config of given feature or all if no feature is given.

The "fallback" is shown only if configured. The fallback defaults to "true" when not configured.

Syntax

show feature config [*feature-name*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show feature config
Feature            State       AutoRestart     Owner      fallback
-------------   --------   -------------   -------   ----------
bgp                enabled     enabled          local
database           enabled     disabled         local
dhcp_relay         enabled     enabled          kube
lldp               enabled     enabled          kube       true
mgmt-framework   enabled     enabled      local
nat                disabled    enabled          local
pmon               enabled     enabled          kube
radv               enabled     enabled          kube
sflow              disabled    enabled          local
snmp               enabled     enabled          kube
swss               enabled     enabled          local
syncd              enabled     enabled          local
teamd              enabled     enabled          local
telemetry          enabled     enabled          kube
```

1.7 show feature status

Function

Run the **show feature status** command to show the status of given feature or all if no feature is given.

The "fallback" defaults to "true" when not configured.

The subset of features are configurable for remote management and only those report additional data.

Syntax

show feature status [*feature-name*]

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show feature status
Feature             State       AutoRestart      SystemState      UpdateTime               ContainerId
ContainerVersion      SetOwner      CurrentOwner      RemoteState
--------------  --------  -------------  -------------  -------------------  -------------  -
-----------------  ----------  --------------  -------------
bgp                 enabled     enabled          up
local          local               none
database            enabled     disabled
local
dhcp_relay          enabled     enabled          up                2020-11-15 18:21:09    249e70102f55
20201230.100           kube           local
lldp                enabled     enabled          up                2020-11-15 18:21:09    779c2d55ee12
20201230.100           kube           local
mgmt-framework    enabled     enabled          up
local          local               none
nat                 disabled    enabled
local
pmon                enabled     enabled          up                2020-11-15 18:20:27    a2b9ffa8aba3
20201230.100           kube           local
radv                enabled     enabled          up                2020-11-15 18:21:05    d8ff27dcfe46
20201230.100           kube           local
sflow               disabled    enabled
local
snmp                enabled     enabled          up                2020-11-15 18:25:51    8b7d5529e306
20201230.111           kube           kube             running
swss                enabled     enabled          up
local          local               none
syncd               enabled     enabled          up
local          local               none
teamd               enabled     enabled          up
local          local               none
telemetry           enabled     enabled          down              2020-11-15 18:24:59
20201230.100           kube           none
```

1 Flow Counters Commands

Command	Function
show flowcnt-trap stats	Show the current statistics for the registered host interface traps.
sonic-clear flowcnt-trap	Clear the current statistics for the registered host interface traps.

1.1 show flowcnt-trap stats

Function

Run the **show flowcnt-trap stats** command to show the current statistics for the registered host interface traps.

Syntax

show flowcnt-trap stats

Parameter Description

N/A

Usage Guidelines

Because clear (see below) is handled on a per-user basis different users may see different counts.

Examples

```
admin@sonic:~$ show flowcnt-trap stats
Trap Name          Packets          Bytes              PPS
---------     ---------     -------     -------
           dhcp                  100          2,000     50.25/s

For multi-ASIC:
admin@sonic:~$ show flowcnt-trap stats
ASIC ID          Trap Name          Packets          Bytes              PPS
-------     -----------     ---------     -------     -------
    asic0                    dhcp                 100          2,000     50.25/s
    asic1                    dhcp                 200          3,000     45.25/s
```

1.2 sonic-clear flowcnt-trap

Function

Run the **sonic-clear flowcnt-trap** command to clear the current statistics for the registered host interface traps.

This is done on a per-user basis.

Syntax

sonic-clear flowcnt-trap

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sonic-clear flowcnt-trap
Trap Flow Counters were successfully cleared
```

1 GearBox Commands

Command	Function
show gearbox interfaces status	Display information about the gearbox phy interface lanes, speeds and status.
show gearbox phys status	Display basic information about the gearbox phys configured on the switch.

1.1 show gearbox interfaces status

Function

Run the **show gearbox interfaces status** command to display information about the gearbox phy interface lanes, speeds and status.

Syntax

show gearbox interfaces status

Parameter Description

N/A

Usage Guidelines

Data is displayed for both MAC side and line side of the gearbox phy.

Examples

```
admin@sonic:~$ show gearbox interfaces status
    PHY Id         Interface         MAC Lanes         MAC Lane Speed         PHY Lanes         PHY Lane
Speed         Line Lanes         Line Lane Speed         Oper         Admin
--------    -----------    -----------    -----------------    -----------    ----------------
------------    -----------------    ------    -------
             1         Ethernet0     25,26,27,28                          10G             200,201
20G                       206                              40G             up              up
             1         Ethernet4     29,30,31,32                          10G             202,203
20G                       207                              40G             up              up
             1         Ethernet8     33,34,35,36                          10G             204,205
20G                       208                              40G             up              up
```

1.2 show gearbox phys status

Function

Run the **show gearbox phys status** command to display basic information about the gearbox phys configured on the switch.

Syntax

show gearbox phys status

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show gearbox phys status
    PHY Id            Name          Firmware
--------     -------     ----------
             1     sesto-1                  v0.1
```

1 Kubernetes Commands

Command	Function
show kubernetes server config	Display the kubernetes server configuration, if any, else would report as not configured.
show kubernetes server status	Display the kubernetes server status.

1.1 show kubernetes server config

Function

Run the **show kubernetes server config** command to display the kubernetes server configuration, if any, else would report as not configured.

Syntax

show kubernetes server config

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show kubernetes server config
ip                      port        insecure        disable
----------    ------    ----------    ---------
10.3.157.24    6443        True              False
```

1.2 show kubernetes server status

Function

Run the **show kubernetes server status** command to display the kubernetes server status.

Syntax

show kubernetes server status

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show kubernetes server status
ip                      port        connected        update-time
----------    ------    ----------    -------------------
10.3.157.24    6443        true                2020-11-15 18:25:05
```

1 Linux Kernel Dump Commands

Command	Function
show kdump config	Show the configuration of Linux kernel dump.
show kdump files	Show the Linux kernel core dump files and dmesg files which are generated by kernel dump tool.
show kdump logging	Show the last 10 lines of latest dmesg file.

1.1 show kdump config

Function

Run the **show kdump config** command to show the configuration of Linux kernel dump.

Syntax

show kdump config

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:$ show kdump config
Kdump administrative mode: Disabled
Kdump operational mode: Unready
Kdump memory researvation: 0M-2G:256M,2G-4G:320M,4G-8G:384M,8G-:448M
Maximum number of Kdump files: 3
```

1.2 show kdump files

Function

Run the **show kdump files** command to show the Linux kernel core dump files and dmesg files which are generated by kernel dump tool.

Syntax

show kdump files

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show kdump files
            Kernel core dump files                    Kernel dmesg files
---------------------------------------- ----------------------------------------
/var/crash/202106242344/kdump.202106242344 /var/crash/202106242344/dmesg.202106242344
/var/crash/202106242337/kdump.202106242337 /var/crash/202106242337/dmesg.202106242337
```

1.3 show kdump logging

Function

Run the **show kdump logging** command to show the last 10 lines of latest dmesg file.

Syntax

show kdump logging

Parameter Description

N/A

Usage Guidelines

This command can also accept a specific file name and number of lines as arguments.

Examples

```
admin@sonic:~$ show kdump logging
[ 157.642053] RSP: 002b:00007fff1beee708 EFLAGS: 00000246 ORIG_RAX: 0000000000000001
[ 157.732635] RAX: ffffffffffffffda RBX: 0000000000000002 RCX: 00007fc3887d4504
[ 157.818015] RDX: 0000000000000002 RSI: 000055d388eceb40 RDI: 0000000000000001
[ 157.903401] RBP: 000055d388eceb40 R08: 000000000000000a R09: 00007fc3888255f0
[ 157.988784] R10: 000000000000000a R11: 0000000000000246 R12: 00007fc3888a6760
[ 158.074166] R13: 0000000000000002 R14: 00007fc3888a1760 R15: 0000000000000002
[ 158.159553] Modules linked in: nft_chain_route_ipv6(E) nft_chain_route_ipv4(E) xt_TCPMSS(E)
dummy(E) team_mode_loadbalance(E) team(E) sx_bfd(OE) sx_netdev(OE) psample(E)
sx_core(OE) 8021q(E) garp(E) mrp(E) mst_pciconf(OE) mst_pci(OE) xt_hl(E) xt_tcpudp(E)
ip6_tables(E) nft_compat(E) nft_chain_nat_ipv4(E) nf_nat_ipv4(E) nft_counter(E) xt_conntrack(E)
nf_nat(E) jc42(E) nf_conntrack_netlink(E) nf_conntrack(E) nf_defrag_ipv6(E) nf_defrag_ipv4(E)
libcrc32c(E) xfrm_user(E) xfrm_algo(E) mlxsw_minimal(E) mlxsw_i2c(E) i2c_mux_reg(E) i2c_mux(E)
i2c_mlxcpld(E) leds_mlxreg(E) mlxreg_io(E) mlxreg_hotplug(E) mei_wdt(E) evdev(E) intel_rapl(E)
x86_pkg_temp_thermal(E) intel_powerclamp(E) kvm_intel(E) mlx_platform(E) kvm(E) irqbypass(E)
crct10dif_pclmul(E) crc32_pclmul(E) ghash_clmulni_intel(E) intel_cstate(E) intel_uncore(E)
[ 159.016731] intel_rapl_perf(E) pcspkr(E) sg(E) iTCO_wdt(E) iTCO_vendor_support(E) mei_me(E)
mei(E) bonding(E) pcc_cpufreq(E) video(E) button(E) ebt_vlan(E) ebtable_broute(E) bridge(E)
stp(E) llc(E) ebtable_nat(E) ebtable_filter(E) ebtables(E) nf_tables(E) nfnetlink(E) xdpe12284(E)
at24(E) ledtrig_timer(E) tmp102(E) lm75(E) drm(E) coretemp(E) max1363(E)
industrialio_triggered_buffer(E) kfifo_buf(E) industrialio(E) tps53679(E) fuse(E) pmbus(E)
pmbus_core(E) i2c_dev(E) configfs(E) ip_tables(E) x_tables(E) autofs4(E) loop(E) ext4(E) crc16(E)
mbcache(E) jbd2(E) crc32c_generic(E) fscrypto(E) ecb(E) crypto_simd(E) cryptd(E) glue_helper(E)
aes_x86_64(E) nvme(E) nvme_core(E) nls_utf8(E) nls_cp437(E) nls_ascii(E) vfat(E) fat(E) overlay(E)
squashfs(E) zstd_decompress(E) xxhash(E) sd_mod(E) gpio_ich(E) ahci(E)
[ 159.864532] libahci(E) mlxsw_core(E) devlink(E) ehci_pci(E) ehci_hcd(E) crc32c_intel(E) libata(E)
i2c_i801(E) scsi_mod(E) usbcore(E) usb_common(E) lpc_ich(E) mfd_core(E) e1000e(E) fan(E)
thermal(E)
[ 160.075846] CR2: 0000000000000000
```

You can specify a file name in order to show its last 10 lines.

```
admin@sonic:~$ show kdump logging dmesg.202106242337
[ 654.120195] RSP: 002b:00007ffe697690f8 EFLAGS: 00000246 ORIG_RAX: 0000000000000001
[ 654.210778] RAX: ffffffffffffffda RBX: 0000000000000002 RCX: 00007fcfca27b504
[ 654.296157] RDX: 0000000000000002 RSI: 000055a6e4d1b3f0 RDI: 0000000000000001
[ 654.381543] RBP: 000055a6e4d1b3f0 R08: 000000000000000a R09: 00007fcfca2cc5f0
[ 654.466925] R10: 000000000000000a R11: 0000000000000246 R12: 00007fcfca34d760
[ 654.552310] R13: 0000000000000002 R14: 00007fcfca348760 R15: 0000000000000002
[ 654.637694] Modules linked in: binfmt_misc(E) nft_chain_route_ipv6(E) nft_chain_route_ipv4(E)
xt_TCPMSS(E) dummy(E) team_mode_loadbalance(E) team(E) sx_bfd(OE) sx_netdev(OE)
psample(E) sx_core(OE) 8021q(E) garp(E) mrp(E) mst_pciconf(OE) mst_pci(OE) xt_hl(E)
xt_tcpudp(E) ip6_tables(E) nft_chain_nat_ipv4(E) nf_nat_ipv4(E) nft_compat(E) nft_counter(E)
xt_conntrack(E) nf_nat(E) jc42(E) nf_conntrack_netlink(E) nf_conntrack(E) nf_defrag_ipv6(E)
nf_defrag_ipv4(E) libcrc32c(E) xfrm_user(E) xfrm_algo(E) mlxsw_minimal(E) mlxsw_i2c(E)
i2c_mux_reg(E) i2c_mux(E) mlxreg_hotplug(E) mlxreg_io(E) i2c_mlxcpld(E) leds_mlxreg(E)
mei_wdt(E) evdev(E) intel_rapl(E) x86_pkg_temp_thermal(E) intel_powerclamp(E) kvm_intel(E)
kvm(E) mlx_platform(E) irqbypass(E) crct10dif_pclmul(E) crc32_pclmul(E) ghash_clmulni_intel(E)
intel_cstate(E)
[ 655.493833] intel_uncore(E) intel_rapl_perf(E) pcspkr(E) sg(E) iTCO_wdt(E)
iTCO_vendor_support(E) mei_me(E) mei(E) bonding(E) video(E) button(E) pcc_cpufreq(E)
ebt_vlan(E) ebtable_broute(E) bridge(E) stp(E) llc(E) ebtable_nat(E) ebtable_filter(E) ebtables(E)
nf_tables(E) nfnetlink(E) xdpe12284(E) at24(E) ledtrig_timer(E) tmp102(E) drm(E) lm75(E)
coretemp(E) max1363(E) industrialio_triggered_buffer(E) kfifo_buf(E) industrialio(E) fuse(E)
tps53679(E) pmbus(E) pmbus_core(E) i2c_dev(E) configfs(E) ip_tables(E) x_tables(E) autofs4(E)
loop(E) ext4(E) crc16(E) mbcache(E) jbd2(E) crc32c_generic(E) fscrypto(E) ecb(E) crypto_simd(E)
cryptd(E) glue_helper(E) aes_x86_64(E) nvme(E) nvme_core(E) nls_utf8(E) nls_cp437(E)
nls_ascii(E) vfat(E) fat(E) overlay(E) squashfs(E) zstd_decompress(E) xxhash(E) sd_mod(E)
[ 656.337476] gpio_ich(E) ahci(E) mlxsw_core(E) libahci(E) devlink(E) crc32c_intel(E) libata(E)
i2c_i801(E) scsi_mod(E) lpc_ich(E) mfd_core(E) ehci_pci(E) ehci_hcd(E) usbcore(E) e1000e(E)
usb_common(E) fan(E) thermal(E)
[ 656.569590] CR2: 0000000000000000
```

You can also specify a file name and number of lines in order to show the last number of lines.

```
admin@sonic:~$ show kdump logging dmesg.202106242337 -l 20
[ 653.525427] __handle_sysrq.cold.9+0x45/0xf2
[ 653.576487] write_sysrq_trigger+0x2b/0x30
[ 653.625472] proc_reg_write+0x39/0x60
[ 653.669252] vfs_write+0xa5/0x1a0
[ 653.708881] ksys_write+0x57/0xd0
[ 653.748501] do_syscall_64+0x53/0x110
[ 653.792287] entry_SYSCALL_64_after_hwframe+0x44/0xa9
[ 653.852707] RIP: 0033:0x7fcfca27b504
```

```
[ 653.895452] Code: 00 f7 d8 64 89 02 48 c7 c0 ff ff ff ff eb b3 0f 1f 80 00 00 00 00 48 8d 05 f9 61 0d 00
8b 00 85 c0 75 13 b8 01 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 54 c3 0f 1f 00 41 54 49 89 d4 55 48 89 f5 53
[ 654.120195] RSP: 002b:00007ffe697690f8 EFLAGS: 00000246 ORIG_RAX: 0000000000000001
[ 654.210778] RAX: ffffffffffffffda RBX: 0000000000000002 RCX: 00007fcfca27b504
[ 654.296157] RDX: 0000000000000002 RSI: 000055a6e4d1b3f0 RDI: 0000000000000001
[ 654.381543] RBP: 000055a6e4d1b3f0 R08: 000000000000000a R09: 00007fcfca2cc5f0
[ 654.466925] R10: 000000000000000a R11: 0000000000000246 R12: 00007fcfca34d760
[ 654.552310] R13: 0000000000000002 R14: 00007fcfca348760 R15: 0000000000000002
[ 654.637694] Modules linked in: binfmt_misc(E) nft_chain_route_ipv6(E) nft_chain_route_ipv4(E)
xt_TCPMSS(E) dummy(E) team_mode_loadbalance(E) team(E) sx_bfd(OE) sx_netdev(OE)
psample(E) sx_core(OE) 8021q(E) garp(E) mrp(E) mst_pciconf(OE) mst_pci(OE) xt_hl(E)
xt_tcpudp(E) ip6_tables(E) nft_chain_nat_ipv4(E) nf_nat_ipv4(E) nft_compat(E) nft_counter(E)
xt_conntrack(E) nf_nat(E) jc42(E) nf_conntrack_netlink(E) nf_conntrack(E) nf_defrag_ipv6(E)
nf_defrag_ipv4(E) libcrc32c(E) xfrm_user(E) xfrm_algo(E) mlxsw_minimal(E) mlxsw_i2c(E)
i2c_mux_reg(E) i2c_mux(E) mlxreg_hotplug(E) mlxreg_io(E) i2c_mlxcpld(E) leds_mlxreg(E)
mei_wdt(E) evdev(E) intel_rapl(E) x86_pkg_temp_thermal(E) intel_powerclamp(E) kvm_intel(E)
kvm(E) mlx_platform(E) irqbypass(E) crct10dif_pclmul(E) crc32_pclmul(E) ghash_clmulni_intel(E)
intel_cstate(E)
[ 655.493833] intel_uncore(E) intel_rapl_perf(E) pcspkr(E) sg(E) iTCO_wdt(E)
iTCO_vendor_support(E) mei_me(E) mei(E) bonding(E) video(E) button(E) pcc_cpufreq(E)
ebt_vlan(E) ebtable_broute(E) bridge(E) stp(E) llc(E) ebtable_nat(E) ebtable_filter(E) ebtables(E)
nf_tables(E) nfnetlink(E) xdpe12284(E) at24(E) ledtrig_timer(E) tmp102(E) drm(E) lm75(E)
coretemp(E) max1363(E) industrialio_triggered_buffer(E) kfifo_buf(E) industrialio(E) fuse(E)
tps53679(E) pmbus(E) pmbus_core(E) i2c_dev(E) configfs(E) ip_tables(E) x_tables(E) autofs4(E)
loop(E) ext4(E) crc16(E) mbcache(E) jbd2(E) crc32c_generic(E) fscrypto(E) ecb(E) crypto_simd(E)
cryptd(E) glue_helper(E) aes_x86_64(E) nvme(E) nvme_core(E) nls_utf8(E) nls_cp437(E)
nls_ascii(E) vfat(E) fat(E) overlay(E) squashfs(E) zstd_decompress(E) xxhash(E) sd_mod(E)
[ 656.337476] gpio_ich(E) ahci(E) mlxsw_core(E) libahci(E) devlink(E) crc32c_intel(E) libata(E)
i2c_i801(E) scsi_mod(E) lpc_ich(E) mfd_core(E) ehci_pci(E) ehci_hcd(E) usbcore(E) e1000e(E)
usb_common(E) fan(E) thermal(E)
[ 656.569590] CR2: 0000000000000000
```

1 Loading, Reloading And Saving Configuration Commands

Command	Function
config load	Load the configuration from a JSON file.
config load_mgmt_config	Reconfigure hostname and mgmt interface based on device description file.
config load_minigraph	Load the configuration from /etc/sonic/minigraph.xml.
config reload	Clear current configuration and import new configurationn from the input file or from /etc/sonic/config_db.json.
config save	Save the config DB configuration into the user-specified filename or into the default /etc/sonic/config_db.json.

1.1 config load

Function

Run the **config load** command to load the configuration from a JSON file.

Syntax

config load [**-y** | **--yes**] [*filename*]

Parameter Description

-y | **--yes**: When user specifies the optional argument “-y” or “–yes”, this command forces the loading without prompting the user for confirmation. If the argument is not specified, it prompts the user to confirm whether user really wants to load this configuration file.

filename: Path of configuration file user want to load. If not specified, it will use the default /etc/sonic/config_db.json file as the input file.

Usage Guidelines

This command is used to load the configuration from a JSON file like the file which SONiC saves its configuration to, `/etc/sonic/config_db.json`. This command loads the configuration from the input file (if user specifies this optional filename, it will use that input file. Otherwise, it will use the default `/etc/sonic/config_db.json` file as the input file) into CONFIG_DB. The configuration present in the input file is applied on top of the already running configuration. This command does not flush the config DB before loading the new configuration (i.e., If the configuration present in the input file is same as the current running configuration, nothing happens). If the config present in the input file is not present in running configuration, it will be added. If the config present in the input file differs (when key matches) from that of the running configuration, it will be modified as per the new values for those keys.

When user specifies the optional argument "-y" or "--yes", this command forces the loading without prompting the user for confirmation. If the argument is not specified, it prompts the user to confirm whether user really wants to load this configuration file.

Examples

```
admin@sonic:~$ sudo config load
Load config from the file /etc/sonic/config_db.json? [y/N]: y
Running command: /usr/local/bin/sonic-cfggen -j /etc/sonic/config_db.json --write-to-db
```

1.2 config load_mgmt_config

Function

Run the **config load_mgmt_config** command to reconfigure hostname and mgmt interface based on device description file.

Syntax

config load_mgmt_config [**-y** | **--yes**] [*filename*]

Parameter Description

-y | **--yes**: When user specifies the optional argument "-y" or "–yes", this command forces the loading without prompting the user for confirmation. If the argument is not specified, it prompts the user to confirm whether user really wants to load this configuration file.

Filename: Path of device description file user want to use. If not specified, it looks for the file "/etc/sonic/device_desc.xml" default.

Usage Guidelines

This command either uses the optional file specified as argument or looks for the file "/etc/sonic/device_desc.xml".If the file does not exist or if the file does not have valid fields for "hostname" and "ManagementAddress", it fails.

Examples

```
admin@sonic:~$ sudo config load_mgmt_config
Reload config from minigraph? [y/N]: y
Running command: /usr/local/bin/sonic-cfggen -M /etc/sonic/device_desc.xml --write-to-db
```

1.3 config load_minigraph

Function

Run the **config load_minigraph** command to load the configuration from /etc/sonic/minigraph.xml.

Syntax

config load_minigraph [**-y** | **--yes**] [**-n** | **--no-service-restart**]

Parameter Description

-y | **--yes**: When user specifies the optional argument "-y" or "–yes", this command forces the loading without prompting the user for confirmation. If the argument is not specified, it prompts the user to confirm whether user really wants to load this configuration file.

-n | **--no-service-restart**: When user specifies the optional argument "-n" or "–no-service-restart", this command loads the configuration without restarting dependent services running on the device. One use case for this option is during boot time when config-setup service loads minigraph configuration and there is no services running on the device.

Usage Guidelines

When users do not want to use configuration from config_db.json, they can copy the minigraph.xml configuration file to the device and load it using this command.

This command restarts various services running in the device and it takes some time to complete the command.

Note

- If the user had logged in using SSH, users might get disconnected and some configuration failures might happen which might be hard to recover. Users need to reconnect their SSH sessions after configuring the management IP address. It is recommended to execute this command from console port.
- Management interface IP address and default route (or specific route) may require reconfiguration in case if those parameters are not part of the minigraph.xml.

When user specifies the optional argument "**-y**" or "**--yes**", this command forces the loading without prompting the user for confirmation.If the argument is not specified, it prompts the user to confirm whether user really wants to load this configuration file.

When user specifies the optional argument "**-n**" or "**--no-service-restart**", this command loads the configuration without restarting dependent services

running on the device. One use case for this option is during boot time when config-setup service loads minigraph configuration and there is no services running on the device.

Examples

```
admin@sonic:~$ sudo config load_minigraph
Reload config from minigraph? [y/N]: y
Running command: /usr/local/bin/sonic-cfggen -j /etc/sonic/config_db.json --write-to-db
```

1.4 config reload

Function

Run the **config reload** command to clear current configuration and import new configurationn from the input file or from /etc/sonic/config_db.json.

Syntax

config reload [**-y** | **--yes**] [**-l** | **--load-sysinfo**] [*filename*] [**-n** | **--no-service-restart**] [**-f** | **--force]**

Parameter Description

-y | **--yes**: When user specifies the optional argument “-y” or “–yes”, this command forces the loading without prompting the user for confirmation. If the argument is not specified, it prompts the user to confirm whether user really wants to load this configuration file.

-l | **--load-sysinfo**: Load system default information (mac, portmap etc) first.

filename: Path of configuration file user want to load. If not specified, it will use the default /etc/sonic/config_db.json file as the input file.

-n | **--no-service-restart**: When user specifies the optional argument “-n” or “–no-service-restart”, this command clear and loads the configuration without restarting dependent services running on the device. One use case for this option is during boot time when config-setup service loads existing old configuration and there is no services running on the device.

-f | **--force**: When user specifies the optional argument “-f” or “–force”, this command ignores the system sanity checks. By default a list of sanity checks are performed and if

one of the checks fail, the command will not execute. The sanity checks include ensuring the system status is not starting, all the essential services are up and swss is in ready state.

Usage Guidelines

This command shall stop all services before clearing the configuration and it then restarts those services.

This command restarts various services running in the device and it takes some time to complete the command.

Notes

If the user had logged in using SSH, users **might get disconnected** depending upon the new management IP address. Users need to reconnect their SSH sessions.In general, it is recommended to execute this command from console port after disconnecting all SSH sessions to the device.When users to do “config reload” the newly loaded config may have management IP address, or it may not have management IP address.If mgmtIP is there in the newly loaded config file, that mgmtIP might be same as previously configured value or it might be different.This difference in mgmtIP address values results in following possible behaviours.

- Previously configured mgmtIP is same as newly loaded mgmtIP. The SSH session may not be affected at all, but it’s possible that there will be a brief interruption in the SSH session. But, assuming the client’s timeout value isn’t on the order of a couple of seconds, the session would most likely just resume again as soon as the interface is reconfigured and up with the same IP.
- Previously configured mgmtIP is different from newly loaded mgmtIP. Users will lose their SSH connections.
- Newly loaded config does not have any mgmtIP. Users will lose their SSH connections.

Notes

Management interface IP address and default route (or specific route) may require reconfiguration in case if those parameters are not part of the minigraph.xml.

When using the config reload operation in the SONiC operating system, **you need to ensure that compared with the saved configuration, there are no additional logical ports, such as Loopback ports and PortChannel ports**. The reason is that this operation will not delete the logical port that has been created and configured, if the logical port exists, the system display information and the chip will be out of sync.

When the config reload operation is used in SONiC, ensure that no additional logical ports, such as Loopback and PortChannel, are added compared with the saved configuration. This operation does not delete logical ports that have been created or configured. If logical ports exist, the system displays inconsistent information with the chip.

Examples

```
admin@sonic:~$ sudo config reload
Clear current config and reload config from the file /etc/sonic/config_db.json? [y/N]: y
Running command: systemctl stop dhcp_relay
Running command: systemctl stop swss
Running command: systemctl stop snmp
```

```
Warning: Stopping snmp.service, but it can still be activated by:
  snmp.timer
Running command: systemctl stop lldp
Running command: systemctl stop pmon
Running command: systemctl stop bgp
Running command: systemctl stop teamd
Running command: /usr/local/bin/sonic-cfggen -H -k Force10-Z9100-C32 --write-to-db
Running command: /usr/local/bin/sonic-cfggen -j /etc/sonic/config_db.json --write-to-db
Running command: systemctl restart hostname-config
Running command: systemctl restart interfaces-config
Timeout, server 10.11.162.42 not responding.
```

When some sanity checks fail below error messages can be seen.

```
admin@sonic:~$ sudo config reload -y
System is not up. Retry later or use -f to avoid system checks

admin@sonic:~$ sudo config reload -y
Relevant services are not up. Retry later or use -f to avoid system checks

admin@sonic:~$ sudo config reload -y
SwSS container is not ready. Retry later or use -f to avoid system checks
```

1.5 config save

Function

Run the **config save** command to save the config DB configuration into the user-specified filename or into the default /etc/sonic/config_db.json.

Syntax

config save [**-y** | **--yes**] [*filename*]

Parameter Description

-y | **--yes**: When user specifies the optional argument “-y” or “–yes”, this command forces the loading without prompting the user for confirmation. If the argument is not specified, it prompts the user to confirm whether user really wants to load this configuration file.

filename: Names of configuration file(s) to save, separated by comma with no spaces in between. If not specified, it will save the config DB configuration into the default /etc/sonic/config_db.json.

Usage Guidelines

This saves the configuration into the disk which is available even after reboots.Saved file can be transferred to remote machines for debugging. If users wants to load the configuration from this new file at any point of time, they can use "config load" command

and provide this newly generated file as input. If users wants this newly generated file to be used during reboot, they need to copy this file to /etc/sonic/config_db.json.

Examples

Save configuration to /etc/sonic/config_db.json

```
admin@sonic:~$ sudo config save –y
```

Save configuration to a specified file

```
admin@sonic:~$ sudo config save -y /etc/sonic/config2.json
```

1 MAC Address FDB Commands

Command	Function
config mac	Add a static FDB entry.
config mac aging-time	Set the FDB aging time.
show mac	Display the MAC (FDB) entries either in full or partial as given below.
show mac aging-time	Display the default mac aging time on the switch.
sonic-clear fdb all	Clear the FDB table.

1.1 config mac

Function

Run the **config mac** command to add a static FDB entry.

Syntax

config mac add *vlan-id mac-address port-name*

config mac del *vlan-id mac-address*

Parameter Description

vlan-id: VLAN ID, for example, 100.

mac-address: Mac address as xx:xx:xx:xx:xx:xx.

port-name: Interface name.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config mac add 1 00:11:11:11:11:11 Ethernet55
admin@sonic:~$ sudo config mac del 1 00:11:11:11:11:11
```

1.2 config mac aging-time

Function

Run the **config mac aging-time** command to set the FDB aging time.

Syntax

config mac aging-time *aging-time*

Parameter Description

aging-time: Aging time.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config mac aging-time 300
```

1.3 show mac

Function

Run the **show mac** command to display the MAC (FDB) entries either in full or partial as given below.

Syntax

show mac [**-v** *vlan-id*] [**-p** *port-name*] [**-a** *mac-address*] [**-t** *type*] [**-c**]

Parameter Description

vlan-id: VLAN ID, for example, 100

port-name: Interface name

mac-address: MAC address

type: Static or Dynamic

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show mac
No.     Vlan   MacAddress            Port              Type
-----   ------   -----------------   -----------   -------
  1     1000   E2:8C:56:85:4A:CD   Ethernet192     Dynamic
  2     1000   A0:1B:5E:47:C9:76   Ethernet192     Dynamic
  3     1000   AA:54:EF:2C:EE:30   Ethernet192     Dynamic
  4     1000   A4:3F:F2:17:A3:FC   Ethernet192     Dynamic
  5     1000   0C:FC:01:72:29:91   Ethernet192     Dynamic
  6     1000   48:6D:01:7E:C9:FD   Ethernet192     Dynamic
  7     1000   1C:6B:7E:34:5F:A6   Ethernet192     Dynamic
  8     1000   EE:81:D9:7B:93:A9   Ethernet192     Dynamic
  9     1000   CC:F8:8D:BB:85:E2   Ethernet192     Dynamic
 10     1000   0A:52:B3:9C:FB:6C   Ethernet192     Dynamic
 11     1000   C6:E2:72:02:D1:23   Ethernet192     Dynamic
 12     1000   8A:C9:5C:25:E9:28   Ethernet192     Dynamic
 13     1000   5E:CD:34:E4:94:18   Ethernet192     Dynamic
 14     1000   7E:49:1F:B5:91:B5   Ethernet192     Dynamic
 15     1000   AE:DD:67:F3:09:5A   Ethernet192     Dynamic
 16     1000   DC:2F:D1:08:4B:DE   Ethernet192     Dynamic
 17     1000   50:96:23:AD:F1:65   Ethernet192     Static
 18     1000   C6:C9:5E:AE:24:42   Ethernet192     Static
Total number of entries 18
```

Optionally, you can specify a VLAN ID or interface name or type or mac-address in order to display only that particular entries.

```
admin@sonic:~$ show mac -v 1000
No.      Vlan   MacAddress            Port              Type
-----  ------  -----------------  -----------  -------
  1      1000   E2:8C:56:85:4A:CD   Ethernet192      Dynamic
  2      1000   A0:1B:5E:47:C9:76   Ethernet192      Dynamic
  3      1000   AA:54:EF:2C:EE:30   Ethernet192      Dynamic
  4      1000   A4:3F:F2:17:A3:FC   Ethernet192      Dynamic
  5      1000   0C:FC:01:72:29:91   Ethernet192      Dynamic
  6      1000   48:6D:01:7E:C9:FD   Ethernet192      Dynamic
  7      1000   1C:6B:7E:34:5F:A6   Ethernet192      Dynamic
  8      1000   EE:81:D9:7B:93:A9   Ethernet192      Dynamic
  9      1000   CC:F8:8D:BB:85:E2   Ethernet192      Dynamic
 10      1000   0A:52:B3:9C:FB:6C   Ethernet192      Dynamic
 11      1000   C6:E2:72:02:D1:23   Ethernet192      Dynamic
 12      1000   8A:C9:5C:25:E9:28   Ethernet192      Dynamic
 13      1000   5E:CD:34:E4:94:18   Ethernet192      Dynamic
 14      1000   7E:49:1F:B5:91:B5   Ethernet192      Dynamic
 15      1000   AE:DD:67:F3:09:5A   Ethernet192      Dynamic
 16      1000   DC:2F:D1:08:4B:DE   Ethernet192      Dynamic
 17      1000   50:96:23:AD:F1:65   Ethernet192      Static
 18      1000   C6:C9:5E:AE:24:42   Ethernet192      Static
Total number of entries 18
```

```
admin@sonic:~$ show mac -p Ethernet192
No.      Vlan   MacAddress            Port              Type
-----  ------  -----------------  -----------  -------
  1      1000   E2:8C:56:85:4A:CD   Ethernet192      Dynamic
  2      1000   A0:1B:5E:47:C9:76   Ethernet192      Dynamic
  3      1000   AA:54:EF:2C:EE:30   Ethernet192      Dynamic
  4      1000   A4:3F:F2:17:A3:FC   Ethernet192      Dynamic
  5      1000   0C:FC:01:72:29:91   Ethernet192      Dynamic
  6      1000   48:6D:01:7E:C9:FD   Ethernet192      Dynamic
  7      1000   1C:6B:7E:34:5F:A6   Ethernet192      Dynamic
  8      1000   EE:81:D9:7B:93:A9   Ethernet192      Dynamic
  9      1000   CC:F8:8D:BB:85:E2   Ethernet192      Dynamic
 10      1000   0A:52:B3:9C:FB:6C   Ethernet192      Dynamic
 11      1000   C6:E2:72:02:D1:23   Ethernet192      Dynamic
 12      1000   8A:C9:5C:25:E9:28   Ethernet192      Dynamic
 13      1000   5E:CD:34:E4:94:18   Ethernet192      Dynamic
 14      1000   7E:49:1F:B5:91:B5   Ethernet192      Dynamic
 15      1000   AE:DD:67:F3:09:5A   Ethernet192      Dynamic
 16      1000   DC:2F:D1:08:4B:DE   Ethernet192      Dynamic
 17      1000   50:96:23:AD:F1:65   Ethernet192      Static
 18      1000   C6:C9:5E:AE:24:42   Ethernet192      Static
Total number of entries 18
```

```
admin@sonic:~$ show mac -a E2:8C:56:85:4A:CD
No.      Vlan   MacAddress            Port              Type
-----   ------   -----------------   -----------   -------
  1      1000   E2:8C:56:85:4A:CD   Ethernet192      Dynamic
Total number of entries 1
```

```
admin@sonic:~$ show mac -t Static
No.      Vlan   MacAddress            Port              Type
-----   ------   -----------------   -----------   -------
  2      1000   50:96:23:AD:F1:65   Ethernet192      Static
  2      1000   C6:C9:5E:AE:24:42   Ethernet192      Static
Total number of entries 2
```

```
admin@sonic:~$ show mac -c
Total number of entries 18
```

note

In products M2-W6930-64QC、M2-W6920-32QC2X and M2-W6510 series, there are a few points that need to be paid attention to:

(1) In the following operations, fdb may remain:

- Remove vlan
- Layer 2 interface change to router interface.
- Router interface change to layer 2 interface.
- Interface mode change from trunk to access.

These fdbs can be cleared with fdbclear command, or aged after an aging cycle.

(2) The behavior of packets where the source mac is equal to the destination mac and is all 0s is: the source mac does not learn, but the packet will be flooded and forwarded.

(3) The filtering addresses cannot take effect on packets sent to the CPU. For example, if the Layer 2 source MAC if an ARP packet is a filtered address, the ARP packet will still be sent to the CPU, but it will not be forwarded.

(4) The MAC address table is a HASH table and is indexed using the HASH algorithm. When learning addresses or adding addresses, the full capacity may not be learned or the addition may fail due to HASH conflicts.

1.4 show mac aging-time

Function

Run the **show mac aging-time** command to display the default mac aging time on the switch.

Syntax

show mac aging-time

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show mac aging-time
Aging time for switch is 600 seconds
```

1.5 sonic-clear fdb all

Function

Run the **sonic-clear fdb all** command to clear the FDB table.

Syntax

sonic-clear fdb all

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sonic-clear fdb all
FDB entries are cleared.
```

1 Muxcable Commands

Command	Function
config muxcable loopback	Set the configuration and enable/disable of loopback on a port user provides.
config muxcable mode	Set the configuration of a muxcable Port/all ports to be active or auto.
config muxcable prbs	Set the configuration and enable/diable of prbs on a port user provides.
show muxcable berinfo	Display the ber(Bit error rate) of the port user provides on the target user provides.
show muxcable config	Display all the configurations of either all the ports which are connected to muxcable or any individual port selected by the user.
show muxcable eyeinfo	Display the eye info in mv(milli volts) of the port user provides on the target user provides.
show muxcable status	Display all the status of either all the ports which are connected to muxcable or any individual port selected by the user.

1.1 config muxcable loopback

Function

Run the **config muxcable loopback** command to set the configuration and enable/disable of loopback on a port user provides.

Syntax

config muxcable loopback enable [*options*] *port target lane-map*

config muxcable loopback disable [*options*] *port target*

Parameter Description

port: PORT required - Port number should be a valid port.

target: TARGET required - the actual target to run the loopback on 0 -> local side, 1 -> TOR 1 2 -> TOR 2 3 -> NIC.

lane-map: LANE_MAP required - an integer representing the lane_map to be run loopback on 0bit for lane 0, 1bit for lane1 and so on. for example 3 -> 0b'0011 , means running on lane0 and lane1.

Usage Guidelines

While enabling in addition to port the user also needs to provides the target and lane map on which the user intends to run loopback on. The target reflects where the enable/dsiable will happen.

Examples

```
admin@sonic:~$ sudo config muxcable loopback enable 1 1 3
loopback config sucessful
admin@sonic:~$      sudo config muxcable loopback disable 1 0
loopback disable sucessfull
```

1.2 config muxcable mode

Function

Run the **config muxcable mode** command to set the configuration of a muxcable Port/all ports to be active or auto.

Syntax

config muxcable mode [*options*] *operation-status* [*port-name*]

Parameter Description

options:

- --json: option to display the result in json format. By default output will be in tabular format.

operation-status: operation_state, permitted operation to be configured which can only be auto or active.

port-name: Port name should be a valid port.

Usage Guidelines

The user has to enter a port number or else all to make the muxcable config operation on all the ports. Depending on the status of the muxcable port state the resultant output could be OK or INPROGRESS. OK would imply no change on the state, INPROGRESS would mean the toggle is happening in the background.

Examples

```
admin@sonic:~$ sudo config muxcable     mode active Ethernet0
port                  state
---------     -------
Ethernet0     OK
admin@sonic:~$ sudo config muxcable     mode --json active Ethernet0
      {
              "Ethernet0": "OK"
      }
admin@sonic:~$ sudo config muxcable     mode active all
port                    state
----------     ----------
Ethernet0       OK
Ethernet32     INPROGRESS
admin@sonic:~$ sudo config muxcable     mode active all --json
      {
              "Ethernet32": "INPROGRESS",
              "Ethernet0": "OK"
      }
```

1.3 config muxcable prbs

Function

Run the **config muxcable prbs** command to set the configuration and enable/diable of prbs on a port user provides.

Syntax

config muxcable prbs enable [*options*] *port target mode-value lane-map*

config muxcable prbs disable [*options*] *port target*

Parameter Description

port: PORT required - Port number should be a valid port.

target: TARGET required - the actual target to run the prbs on 0 -> local side, 1 -> TOR 1 2 -> TOR 2 3 -> NIC.

mode-value: MODE_VALUE required - the mode/type for configuring the PRBS mode. 0x00 = PRBS 9, 0x01 = PRBS 15, 0x02 = PRBS 23, 0x03 = PRBS 31.

lane-map: LANE_MAP required - an integer representing the lane_map to be run PRBS on 0bit for lane 0, 1bit for lane1 and so on. for example 3 -> 0b'0011 , means running on lane0 and lane1.

Usage Guidelines

While enabling in addition to port the user also needs to provide the target, prbs mode and lane map on which the user intends to run prbs on. The target reflects where the enable/disable will happen.

Examples

```
admin@sonic:~$ sudo config muxcable prbs enable 1 1 3 3
PRBS config sucessful
admin@sonic:~$      sudo config muxcable prbs disable 1 0
PRBS disable sucessful
```

1.4 show muxcable berinfo

Function

Run the **show muxcable berinfo** command to display the ber(Bit error rate) of the port user provides on the target user provides.

Syntax

show muxcable berinfo [*options*] *port target*

Parameter Description

port: Port number should be a valid port.

target: The actual target to get the ber info of.

Usage Guidelines

The target provided as an integer corresponds to actual target as. 0 -> local 1 -> tor 1 2 -> tor 2 3 -> nic.

Examples

```
admin@sonic:~$ show muxcable berinfo 1 1
Lane1          Lane2
-------     -------
0                0
```

1.5 show muxcable config

Function

Run the **show muxcable config** command to display all the configurations of either all the ports which are connected to muxcable or any individual port selected by the user.

Syntax

show muxcable config [*port*] [*options*]

Parameter Description

port: Port name should be a valid port.

options:

- --json: option to display the result in json format. By default output will be in tabular format.

Usage Guidelines

The resultant table or json output will show the current configurations of muxcable on the port(active/standby) and also the ipv4 and ipv6 address of the port as well as peer TOR ip address with the hostname.

Examples

```
admin@sonic:~$ show muxcable config
SWITCH_NAME          PEER_TOR
-------------     ----------
sonic                    10.1.1.1
port               state         ipv4              ipv6
---------     -------     --------     --------
Ethernet0     active     10.1.1.1     fc00::75
admin@sonic:~$ show muxcable config --json
{
        "MUX_CABLE": {
                "PEER_TOR": "10.1.1.1",
                "PORTS": {
                        "Ethernet0": {
                                "STATE": "active",
                                "SERVER": {
                                        "IPv4": "10.1.1.1",
                                        "IPv6": "fc00::75"
                                }
                        }
                }
        }
}
admin@sonic:~$ show muxcable config Ethernet0
```

```
SWITCH_NAME          PEER_TOR
-------------     ----------
sonic                    10.1.1.1
port              state         ipv4             ipv6
---------     -------     --------     --------
Ethernet0     active     10.1.1.1     fc00::75
admin@sonic:~$ show muxcable config Ethernet0 --json
{
        "MUX_CABLE": {
                "PORTS": {
                        "Ethernet0": {
                                "STATE": "active",
                                "SERVER": {
                                        "IPv4": "10.1.1.1",
                                        "IPv6": "fc00::75"
                                }
                        }
                }
        }
}
```

1.6 show muxcable eyeinfo

Function

Run the **show muxcable eyeinfo** command to display the eye info in mv(milli volts) of the port user provides on the target user provides.

Syntax

show muxcable eyeinfo [*options*] *port target*

Parameter Description

port: Port number should be a valid port.

target: The actual target to get the eye info of.

Usage Guidelines

The target provided as an integer corresponds to actual target as. 0 -> local 1 -> tor 1 2 -> tor 2 3 -> nic.

Examples

```
admin@sonic:~$ show muxcable eyeinfo 1 1
Lane1          Lane2
-------     -------
632              622
```

1.7 show muxcable status

Function

Run the **show muxcable status** command to display all the status of either all the ports which are connected to muxcable or any individual port selected by the user.

Syntax

show muxcable status [*port*] [*options*]

Parameter Description

port: Port name should be a valid port.

options:

- --json: option to display the result in json format. By default output will be in tabular format.

Usage Guidelines

The resultant table or json output will show the current status of muxcable on the port (auto/active) and also the health of the muxcable.

Examples

```
admin@sonic:~$ show muxcable status
PORT                STATUS          HEALTH
----------     --------     --------
Ethernet32      active          HEALTHY
Ethernet0        auto              HEALTHY
admin@sonic:~$ show muxcable status --json
          {
                   "MUX_CABLE": {
                                "Ethernet32": {
                                          "STATUS": "active",
                                          "HEALTH": "HEALTHY"
                                },
                                "Ethernet0": {
                                             "STATUS": "auto",
                                             "HEALTH": "HEALTHY"
                                  }
                    }
          }

admin@sonic:~$ show muxcable status Ethernet0
PORT                STATUS          HEALTH
---------     --------     --------
Ethernet0      auto              HEALTHY
admin@sonic:~$ show muxcable status Ethernet0 --json
```

```
    {
        "MUX_CABLE": {
            "Ethernet0": {
                "STATUS": "auto",
                "HEALTH": "HEALTHY"
            }
        }
}
```

1 NDP Commands

Command	Function
show ndp	Display either all the IPv6 neighbor mac addresses, or for a particular IPv6 neighbor, or for all IPv6 neighbors reachable via a specific interface.

1.1 show ndp

Function

Run the **show ndp** command to display either all the IPv6 neighbor mac addresses, or for a particular IPv6 neighbor, or for all IPv6 neighbors reachable via a specific interface.

Syntax

show ndp [**-if** | **--iface** [*interface-name*]] [*ipv6-address*]

Parameter Description

interface-name: interface name.

ipv6-address: ipv6 address.

Usage Guidelines

N/A

Examples

Show all IPv6 neighbors.

```
admin@sonic:~$ show ndp
Address                                 MacAddress              Iface         Vlan        Status
--------------------------    -----------------    -------    ------    ---------
fe80::20c:29ff:feb8:b11e      00:0c:29:b8:b1:1e      eth0           -             REACHABLE
fe80::20c:29ff:feb8:cff0      00:0c:29:b8:cf:f0      eth0           -             REACHABLE
fe80::20c:29ff:fef9:324        00:0c:29:f9:03:24      eth0           -              REACHABLE
Total number of entries 3
```

Show specific IPv6 neighbor.

```
admin@sonic:~$ show ndp fe80::20c:29ff:feb8:b11e
Address                                 MacAddress              Iface         Vlan        Status
--------------------------    -----------------    -------    ------    ---------
fe80::20c:29ff:feb8:b11e      00:0c:29:b8:b1:1e      eth0           -             REACHABLE
Total number of entries 1
show IPv6 neighbors learned on a specific interface
admin@sonic:~$ show ndp -if eth0
Address                                 MacAddress              Iface         Vlan        Status
--------------------------    -----------------    -------    ------    ---------
fe80::20c:29ff:feb8:b11e      00:0c:29:b8:b1:1e      eth0           -             REACHABLE
fe80::20c:29ff:feb8:cff0      00:0c:29:b8:cf:f0      eth0           -             REACHABLE
fe80::20c:29ff:fef9:324        00:0c:29:f9:03:24      eth0           -              REACHABLE
Total number of entries 3
```

1 PBH Commands

Command	Function
config pbh hash	Manage PBH hash objects.
config pbh hash-field	Manage PBH hash field objects.
config pbh rule	Manage PBH rule objects.
config pbh table	Manage PBH table objects.
show pbh hash	Display PBH hash configuration.
show pbh hash-field	Display PBH hash field configuration.
show pbh rule	Display PBH rule configuration.
show pbh statistics	Display PBH statistics.
show pbh table	Display PBH table configuration.

1.1 config pbh hash

Function

Run the **config pbh hash** command to manage PBH hash objects.

It supports add/update/remove operations.

Syntax

config pbh hash add *hash-name* **--hash-field-list** <*hash-field-list*>

config pbh hash update *hash-name* [**--hash-field-list** <*hash-field-list*>]

config pbh hash delete *hash-name*

Parameter Description

hash-name: the name of the PBH hash

hash-field-list: list of hash-field objects to apply with the PBH hash

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config pbh hash add 'inner_v6_hash' --hash-field-list
'inner_ip_proto,inner_l4_dst_port,inner_l4_src_port,inner_dst_ipv6,inner_src_i
admin@sonic:~$ sudo config pbh hash update 'inner_v6_hash' --hash-field-list 'inner_ip_proto'
admin@sonic:~$ sudo config pbh hash delete 'inner_v6_hash'
```

1.2 config pbh hash-field

Function

Run the **config pbh hash-field** command to manage PBH hash field objects.

It supports add/update/remove operations.

Syntax

config pbh hash-field add *hash-field-name* **--hash-field** *hash-field* [**--ip-mask** *ip-mask*] **--sequence-id** *sequence-id*

config pbh hash-field update *hash-field-name* [**--hash-field** *hash-field*] [**--ip-mask** *ip-mask*] [**--sequence-id** *sequence-id*]

config pbh hash-field delete *hash-field-name*

Parameter Description

hash-field-name: the name of the PBH hash field

hash-field: native hash field for the PBH hash field Valid values:

- INNER_IP_PROTOCOL
- INNER_L4_DST_PORT
- INNER_L4_SRC_PORT
- INNER_DST_IPV4
- INNER_SRC_IPV4
- INNER_DST_IPV6
- INNER_SRC_IPV6

ip-mask: IPv4/IPv6 address mask for the PBH hash field Valid only: *hash_field* is:

- INNER_DST_IPV4
- INNER_SRC_IPV4
- INNER_DST_IPV6
- INNER_SRC_IPV6

sequence-id: the order in which fields are hashed

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config pbh hash-field add 'inner_dst_ipv6' --hash-field 'INNER_DST_IPV6' --ip-mask 'ffff::' --sequence-id '4'
admin@sonic:~$ sudo config pbh hash-field update 'inner_dst_ipv6' --ip-mask 'ffff:ffff::'
admin@sonic:~$ sudo config pbh hash-field delete 'inner_dst_ipv6'
```

1.3 config pbh rule

Function

Run the **config pbh rule** command to manage PBH rule objects.

It supports add/update/remove operations.

Syntax

config pbh rule add *table-name rule-name* **--priority** *priority* [**--gre-key** *gre-key*] [**--ether-type** *ether-type*] [**--ip-protocol** *ip-protocol*] [**--ipv6-next-header** *ipv6-next-header*] [**--l4-dst-port** *l4-dst-port*] [**--inner-ether-type** *inner-ether-type* **--hash** *hash* [**--packet-action** *packet-action*] [**--flow-counter** *flow-counter*]

config pbh rule update *table-name rule-name* [**--priority** *priority*] [**--gre-key** *gre-key*] [**--ether-type** *ether-type*] [**--ip-protocol** *ip-protocol*] [**--ipv6-next-header** *ipv6-next-header*] [**--l4-dst-port** *l4-dst-port*] [**--inner-ether-type** *inner-ether-type* [**--hash** *hash*] [**--packet-action** *packet-action*] [**--flow-counter** *flow-counter*]

config pbh rule delete *table-name rule-name*

Parameter Description

table-name: the name of the PBH table

rule-name: the name of the PBH rule

priority: the priority of the PBH rule

gre-key: packet match for the PBH rule: GRE key (value/mask)

ether-type: packet match for the PBH rule: EtherType (IANA Ethertypes)

ip-protocol: packet match for the PBH rule: IP protocol (IANA Protocol Numbers)

ipv6-next-header: packet match for the PBH rule: IPv6 Next header (IANA Protocol Numbers)

l4-dst-port: packet match for the PBH rule: L4 destination port

inner-ether-type: packet match for the PBH rule: inner EtherType (IANA Ethertypes)

hash: *hash* object to apply with the PBH rule

packet-action: packet action for the PBH rule Valid values:

- SET_ECMP_HASH
- SET_LAG_HASH

Default: SET_ECMP_HASH

flow-counter: packet/byte counter for the PBH rule Valid values:

- DISABLED
- ENABLED

Default:DISABLED

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config pbh rule add 'pbh_table' 'nvgre' --priority '2' --ether-type '0x0800' --ip-protocol '0x2f' --gre-key '0x2500/0xffffff00' --inner-ether-type '0x86dd' --hash 'inner_v6_hash' --packet-action 'SET_ECMP_HASH' --flow-counter 'DISABLED'
admin@sonic:~$ sudo config pbh rule update 'pbh_table' 'nvgre' --flow-counter 'ENABLED'
admin@sonic:~$ sudo config pbh rule delete 'pbh_table' 'nvgre'
```

1.4 config pbh table

Function

Run the **config pbh table** command to manage PBH table objects.

It supports add/update/remove operations.

Syntax

config pbh table add *table-name* **--interface-list** *interface-list* **--description** *description*

config pbh table update *table-name* [**--interface-list** *interface-list*] [**--description** *description*]

config pbh table delete *table-name*

Parameter Description

table-name: the name of the PBH table

interface-list: interfaces to which PBH table is applied

description: the description of the PBH table

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config pbh table add 'pbh_table' --interface-list
'Ethernet0,Ethernet4,PortChannel0001,PortChannel0002' --description 'NVGRE and VxLAN'
admin@sonic:~$ sudo config pbh table update 'pbh_table' --interface-list 'Ethernet0'
admin@sonic:~$ sudo config pbh table delete 'pbh_table'
```

1.5 show pbh hash

Function

Run the **show pbh hash** command to display PBH hash configuration.

Syntax

show pbh hash

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show pbh hash
NAME                          HASH FIELD
-------------      -----------------
inner_v4_hash      inner_ip_proto
                              inner_l4_dst_port
                              inner_l4_src_port
                              inner_dst_ipv4
```

```
                              inner_src_ipv4
inner_v6_hash     inner_ip_proto
                              inner_l4_dst_port
                              inner_l4_src_port
                              inner_dst_ipv6
                              inner_src_ipv6
```

1.6 show pbh hash-field

Function

Run the **show pbh hash-field** command to display PBH hash field configuration.

Syntax

show pbh hash-field

Parameter Description

N/A

Usage Guidelines

SYMMETRIC is an artificial column and is only used to indicate fields symmetry.

Examples

```
admin@sonic:~$ show pbh hash-field
NAME                            FIELD                           MASK            SEQUENCE
SYMMETRIC
------------------    ------------------    ---------    ----------    -----------
inner_ip_proto           INNER_IP_PROTOCOL     N/A              1                  No
inner_l4_dst_port     INNER_L4_DST_PORT     N/A              2                  Yes
inner_l4_src_port     INNER_L4_SRC_PORT     N/A              2                  Yes
inner_dst_ipv4           INNER_DST_IPV4          255.0.0.0     3                  Yes
inner_src_ipv4           INNER_SRC_IPV4          0.0.0.255     3                  Yes
inner_dst_ipv6           INNER_DST_IPV6          ffff::        4                  Yes
inner_src_ipv6           INNER_SRC_IPV6          ::ffff        4                  Yes
```

1.7 show pbh rule

Function

Run the **show pbh rule** command to display PBH rule configuration.

Syntax

show pbh rule

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show pbh rule
TABLE             RULE         PRIORITY         MATCH
HASH                        ACTION                    COUNTER
---------    ------    ----------    ------------------------------------    -------------    --
----------    ---------
pbh_table    nvgre       2                    ether_type:                  0x0800
inner_v6_hash    SET_ECMP_HASH    DISABLED
                                                    ip_protocol:                0x2f
                                                    gre_key:                        0x2500/0xffffff00
                                                    inner_ether_type:    0x86dd
pbh_table    vxlan       1                    ether_type:                  0x0800
inner_v4_hash    SET_LAG_HASH      ENABLED
                                                    ip_protocol:                0x11
                                                    l4_dst_port:                0x12b5
                                                    inner_ether_type:    0x0800
```

1.8 show pbh statistics

Function

Run the **show pbh statistics** command to display PBH statistics.

Syntax

show pbh statistics

Parameter Description

N/A

Usage Guidelines

RX PACKETS COUNT and RX BYTES COUNT can be cleared by user.

Examples

```
admin@sonic:~$ show pbh statistics
TABLE             RULE         RX PACKETS COUNT         RX BYTES COUNT
---------    ------    ------------------    ----------------
pbh_table    nvgre       0                                0
pbh_table    vxlan       0                                0
```

1.9 show pbh table

Function

Run the **show pbh table** command to display PBH table configuration.

Syntax

show pbh table

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show pbh table
NAME                INTERFACE                   DESCRIPTION
---------     ---------------     ---------------
pbh_table      Ethernet0                   NVGRE and VxLAN
                        Ethernet4
                        PortChannel0001
                        PortChannel0002
```

1 Routing Stack Commands

SONiC software is agnostic of the routing software that is being used in the device. For example, users can use either Quagga or FRR routing stack as per their requirement. A separate shell (vtysh) is provided to configure such routing stacks. Once if users go to "vtysh", they can use the routing stack specific commands as given in the following example.

Notes

Refer the routing stack [Quagga Command Reference] (https://www.nongnu.org/quagga/docs/quagga.pdf) or [FRR Command Reference] (https://docs.frrouting.org/en/latest/) to know more about the routing stack configuration.

```
admin@sonic:~$ vtysh

Hello, this is FRRouting (version 9.1)
Copyright 1996-2005 Kunihiro Ishiguro, et al.

sonic# show route-map
ZEBRA:
route-map RM_SET_SRC, permit, sequence 10
  Match clauses:
  Set clauses:
    src 10.12.0.102
  Call clause:
  Action:
    Exit routemap
```

1 Watermark Commands

Command	Function
config watermark telemetry interval	Configure the interval for telemetry.
show watermark telemetry interval	Display the configured interval for the telemetry.

1.1 config watermark telemetry interval

Function

Run the **config watermark telemetry interval** command to configure the interval for telemetry.

Syntax

config watermark telemetry interval *value*

Parameter Description

value: There is no regulation on the valid range of values; it leverages linux timer. The default interval is 120 seconds.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config watermark telemetry interval 999
```

1.2 show watermark telemetry interval

Function

Run the **show watermark telemetry interval** command to display the configured interval for the telemetry.

Syntax

show watermark telemetry interval

Parameter Description

N/A

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ show watermark telemetry interval

Telemetry interval 120 second(s)
```

1 Rollback Commands

Command	Function
config apply-patch	Apply patches to update the system configuration.
config checkpoint	Create a checkpoint, which is the starting configuration for database entries recovery.
config delete-checkpoint	Delete the created checkpoint.
config list-checkpoint	View the created checkpoints.
config replace	Replace the current device config db configuration.
config rollback	Rollback the system configuration to the checkpoint.

1.1 config apply-patch

Function

Run the **config apply-patch** command to apply patches to update the system configuration.

Syntax

config apply-patch *patch-file-path* [**-d** | **-n** | **-I | -v** | **-f** { **CONFIGDB** | **SONICYANG** }]

Parameter Description

-patch-file-path: Patch file path.

-f: format of config of the patch is either ConfigDb(ABNF) or SonicYang.

-d: test out the command without affecting config state.

-n: ignore validation for tables without YANG models(hidden in the user interface).

-i: ignore validation for config specified by given path which is a JsonPointer(hidden in the user interface).

-v: print additional details of what the operation is doing.

Usage Guidelines

N/A

Examples

```
mirror-changes.json-patch:
[
  {
    "op": "remove",
    "path": "/MIRROR_SESSION/1/direction"
  },
  {
    "op": "remove",
    "path": "/MIRROR_SESSION/1/dst_port"
  },
  {
    "op": "remove",
    "path": "/MIRROR_SESSION/1/src_port"
  },
  {
    "op": "remove",
    "path": "/MIRROR_SESSION/1/type"
  },
  {
```

```
    "op": "remove",
    "path": "/MIRROR_SESSION/1"
  }
]

admin@sonic:~$ show mirror_session
ERSPAN Sessions
Name       Status       SRC IP       DST IP       GRE       DSCP       TTL       Queue       Policer       Monitor Port
SRC Port       Direction
------  --------  --------  --------  -----  ------  -----  -------  ---------  -------------
-  ----------  -----------

SPAN Sessions
Name   Status       DST Port       SRC Port       Direction       Queue       Policer
------  --------  ----------  ----------  -----------  -------  ---------
  1   active       Ethernet15    Ethernet12    both
  2   active       Ethernet36    Ethernet49    both

admin@sonic:~$ sudo config apply-patch mirror-changes.json-patch
Patch Applier: Patch application starting.
Patch Applier: Patch: [{"op": "remove", "path": "/MIRROR_SESSION/1/direction"}, {"op": "remove", "path":
"/MIRROR_SESSION/1/dst_port"}, {"op": "remove", "path": "/MIRROR_SESSION/1/src_port"}, {"op": "remove",
"path": "/MIRROR_SESSION/1/type"}, {"op": "remove", "path": "/MIRROR_SESSION/1"}]
Patch Applier: Getting current config db.
Patch Applier: Simulating the target full config after applying the patch.
Patch Applier: Validating target config does not have empty tables, since they do not show up in
ConfigDb.
Patch Applier: Sorting patch updates.
Patch Applier: The patch was sorted into 5 changes:
Patch Applier:     * [{"op": "remove", "path": "/MIRROR_SESSION/1/direction"}]
Patch Applier:     * [{"op": "remove", "path": "/MIRROR_SESSION/1/dst_port"}]
Patch Applier:     * [{"op": "remove", "path": "/MIRROR_SESSION/1/src_port"}]
Patch Applier:     * [{"op": "remove", "path": "/MIRROR_SESSION/1/type"}]
Patch Applier:     * [{"op": "remove", "path": "/MIRROR_SESSION/1"}]
Patch Applier: Applying 5 changes in order:
Patch Applier:     * [{"op": "remove", "path": "/MIRROR_SESSION/1/direction"}]
Patch Applier:     * [{"op": "remove", "path": "/MIRROR_SESSION/1/dst_port"}]
Patch Applier:     * [{"op": "remove", "path": "/MIRROR_SESSION/1/src_port"}]
Patch Applier:     * [{"op": "remove", "path": "/MIRROR_SESSION/1/type"}]
Patch Applier:     * [{"op": "remove", "path": "/MIRROR_SESSION/1"}]
Patch Applier: Verifying patch updates are reflected on ConfigDB.
Patch Applier: Patch application completed.
Patch applied successfully.

admin@sonic:~$ show mirror_session
ERSPAN Sessions
```

```
Name      Status      SRC IP      DST IP      GRE      DSCP      TTL      Queue      Policer      Monitor Port
SRC Port      Direction
------  --------  --------  --------  -----  ------  -----  -------  ---------  -------------
-  ----------  -----------

SPAN Sessions
Name   Status      DST Port      SRC Port      Direction      Queue      Policer
------  --------  ----------  ----------  -----------  -------  ---------
  2   active      Ethernet36   Ethernet49   both
```

1.2 config checkpoint

Function

Run the **config checkpoint** command to create a checkpoint, which is the starting configuration for database entries recovery.

Syntax

config checkpoint *checkpoint-name* [**-v**]

Parameter Description

checkpoint-name: the starting position of the database item recovery.

-v: print additional details of what the operation is doing.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config checkpoint mycheckpoint -v
Config Rollbacker: Config checkpoint starting.
Config Rollbacker: Checkpoint name: mycheckpoint.
Config Rollbacker: Getting current config db.
Config Rollbacker: Getting checkpoint full-path.
Config Rollbacker: Ensuring checkpoint directory exist.
Config Rollbacker: Saving config db content to etc/sonic/checkpoints/mycheckpoint.cp.json.
Config Rollbacker: Config checkpoint completed.
Checkpoint created successfully.
```

1.3 config delete-checkpoint

Function

Run the **config delete-checkpoint** command to delete the created checkpoint.

Syntax

config delete-checkpoint *checkpoint-name* [**-v**]

Parameter Description

checkpoint-name: the starting position of the database item recovery.

-v: print additional details of what the operation is doing..

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config delete-checkpoint mycheckpoint -v
Config Rollbacker: Deleting checkpoint starting.
Config Rollbacker: Checkpoint name: mycheckpoint.
Config Rollbacker: Checking checkpoint exists.
Config Rollbacker: Deleting checkpoint.
Config Rollbacker: Deleting checkpoint completed.
Checkpoint deleted successfully.
```

1.4 config list-checkpoint

Function

Run the **config list-checkpoint** command to view the created checkpoints.

Syntax

config list-checkpoint [**-v**]

Parameter Description

-v: print additional details of what the operation is doing.

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config list-checkpoints -v
Config Rollbacker: Listing checkpoints starting.
Config Rollbacker: Verifying checkpoints directory '/etc/sonic/checkpoints' exists.
Config Rollbacker: Getting checkpoints in checkpoints directory.
Config Rollbacker: Found 1 checkpoint:
Config Rollbacker:     * mycheckpoint
Config Rollbacker: Listing checkpoints completed.
[
```

```
    "mycheckpoint"
]
```

1.5 config replace

Function

Run the **config replace** command to replace the current device config db configuration.

Syntax

config replace *target-file-path* [**-d** | **-n** | **-i** | **-v** | **-f** { **CONFIGDB** | **SONICYANG** }]

Parameter Description

target-file-path: Path to the target file on the file-system.

-f: format of config of the patch is either ConfigDb(ABNF) or SonicYang.

-d: test out the command without affecting config state.

-n: ignore validation for tables without YANG models(hidden in the user interface).

-i: ignore validation for config specified by given path which is a JsonPointer(hidden in the user interface).

-v: print additional details of what the operation is doing

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config replace /etc/sonic/config_db.json
Config Replacer: Config replacement starting.
Config Replacer: Target config length: 102832.
Config Replacer: Getting current config db.
Config Replacer: Generating patch between target config and current config db.
Config Replacer: Applying patch using 'Patch Applier'.
Patch Applier: Patch application starting.
Patch Applier: Patch: [{"op": "remove", "path": "/MIRROR_SESSION"}, {"op": "add", "path":
"/PORT/Ethernet36/tagging_mode", "value": "access"}, {"op": "add", "path": "/PORT/Ethernet36/vlan",
"value": "1"}, {"op": "add", "path": "/VLAN/Vlan1/members/1", "value": "Ethernet36"}, {"op": "move", "from":
"/INTERFACE/Ethernet47|10.1.2.3~124", "path": "/INTERFACE/Ethernet12|10.0.0.22~131"}, {"op": "add", "path":
"/INTERFACE/Ethernet15|10.0.0.28~131", "value": {}}, {"op": "add", "path": "/INTERFACE/Ethernet15", "value": {}},
{"op": "add", "path": "/VLAN_MEMBER/Vlan1|Ethernet36", "value": {"tagging_mode": "untagged"}}]
Patch Applier: Getting current config db.
Patch Applier: Simulating the target full config after applying the patch.
Patch Applier: Validating target config does not have empty tables, since they do not show up in
ConfigDb.
```

```
Patch Applier: Sorting patch updates.
Patch Applier: The patch was sorted into 18 changes:
Patch Applier:    * [{"op": "remove", "path": "/INTERFACE/Ethernet47|10.1.2.3~124"}]
Patch Applier:    * [{"op": "add", "path": "/INTERFACE/Ethernet12|10.0.0.22~131", "value": {}}]
Patch Applier:    * [{"op": "add", "path": "/INTERFACE/Ethernet15", "value": {}}]
Patch Applier:    * [{"op": "add", "path": "/INTERFACE/Ethernet15|10.0.0.28~131", "value": {}}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/1/direction"}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/1/dst_port"}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/1/src_port"}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/1/type"}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/1"}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/2/direction"}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/2/dst_port"}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/2/src_port"}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/2/type"}]
Patch Applier:    * [{"op": "add", "path": "/PORT/Ethernet36/tagging_mode", "value": "access"}]
Patch Applier:    * [{"op": "add", "path": "/PORT/Ethernet36/vlan", "value": "1"}]
Patch Applier:    * [{"op": "add", "path": "/VLAN/Vlan1/members/1", "value": "Ethernet36"}]
Patch Applier:    * [{"op": "add", "path": "/VLAN_MEMBER/Vlan1|Ethernet36", "value": {"tagging_mode":
"untagged"}}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION"}]
Patch Applier: Applying 18 changes in order:
Patch Applier:    * [{"op": "remove", "path": "/INTERFACE/Ethernet47|10.1.2.3~124"}]
Patch Applier:    * [{"op": "add", "path": "/INTERFACE/Ethernet12|10.0.0.22~131", "value": {}}]
Patch Applier:    * [{"op": "add", "path": "/INTERFACE/Ethernet15", "value": {}}]
Patch Applier:    * [{"op": "add", "path": "/INTERFACE/Ethernet15|10.0.0.28~131", "value": {}}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/1/direction"}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/1/dst_port"}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/1/src_port"}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/1/type"}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/1"}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/2/direction"}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/2/dst_port"}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/2/src_port"}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION/2/type"}]
Patch Applier:    * [{"op": "add", "path": "/PORT/Ethernet36/tagging_mode", "value": "access"}]
Patch Applier:    * [{"op": "add", "path": "/PORT/Ethernet36/vlan", "value": "1"}]
Patch Applier:    * [{"op": "add", "path": "/VLAN/Vlan1/members/1", "value": "Ethernet36"}]
Patch Applier:    * [{"op": "add", "path": "/VLAN_MEMBER/Vlan1|Ethernet36", "value": {"tagging_mode":
"untagged"}}]
Patch Applier:    * [{"op": "remove", "path": "/MIRROR_SESSION"}]
Patch Applier: Verifying patch updates are reflected on ConfigDB.
Patch Applier: Patch application completed.
Config Replacer: Verifying config replacement is reflected on ConfigDB.
Config Replacer: Config replacement completed.
Config replaced successfully.
```

1.6 config rollback

Function

Run the **config rollback** command to rollback the system configuration to the checkpoint.

Syntax

config rollback *checkpoint-name* [**-d** | **-n** | **-i** | **-v**]

Parameter Description

checkpoint-name: the starting position of the database item recovery.

-d: test out the command without affecting config state.

-n: ignore validation for tables without YANG models.

-i: ignore validation for config specified by given path which is a JsonPointer.

-v: print additional details of what the operation is doing..

Usage Guidelines

N/A

Examples

```
admin@sonic:~$ sudo config rollback mycheckpoint
Config Rollbacker: Deleting checkpoint starting.
Config Rollbacker: Checkpoint name: mycheckpoint.
Config Rollbacker: Checking checkpoint exists.
Config Rollbacker: Deleting checkpoint.
Config Rollbacker: Deleting checkpoint completed.
Checkpoint deleted successfully.

admin@sonic:~$ sudo config interface ip add Ethernet1 10.2.2.3/24
admin@sonic:~$ show ip interfaces
Interface      Master      IPv4 address/mask      Admin/Oper      BGP Neighbor      Neighbor IP
-----------   --------   -------------------   ------------   ---------------   -------------
Ethernet1                  10.2.2.3/24              up/down          N/A                 N/A
...     ...

admin@sonic:~$ sudo config rollback mycheckpoint
Config Rollbacker: Config rollbacking starting.
Config Rollbacker: Checkpoint name: mycheckpoint.
Config Rollbacker: Verifying 'mycheckpoint' exists.
Config Rollbacker: Loading checkpoint into memory.
Config Rollbacker: Replacing config using 'Config Replacer'.
Config Replacer: Config replacement starting.
```

```
Config Replacer: Target config length: 102862.
Config Replacer: Getting current config db.
Config Replacer: Generating patch between target config and current config db.
Config Replacer: Applying patch using 'Patch Applier'.
Patch Applier: Patch application starting.
Patch Applier: Patch: [{"op": "add", "path": "/VLAN/Vlan1/members/0", "value": "Ethernet1"}, {"op": "
add", "path": "/PORT/Ethernet1/tagging_mode", "value": "access"}, {"op": "add", "path": "/PORT/Ethern
et1/vlan", "value": "1"}, {"op": "remove", "path": "/INTERFACE/Ethernet1|10.2.2.3~124"}, {"op": "remo
ve", "path": "/INTERFACE/Ethernet1"}, {"op": "add", "path": "/VLAN_MEMBER/Vlan1|Ethernet1", "value":
{"tagging_mode": "untagged"}}]
Patch Applier: Getting current config db.
Patch Applier: Simulating the target full config after applying the patch.
Patch Applier: Validating target config does not have empty tables, since they do not show up in Conf
igDb.
Patch Applier: Sorting patch updates.
Patch Applier: The patch was sorted into 6 changes:
Patch Applier:    * [{"op": "remove", "path": "/INTERFACE/Ethernet1|10.2.2.3~124"}]
Patch Applier:    * [{"op": "remove", "path": "/INTERFACE/Ethernet1"}]
Patch Applier:    * [{"op": "add", "path": "/PORT/Ethernet1/tagging_mode", "value": "access"}]
Patch Applier:    * [{"op": "add", "path": "/PORT/Ethernet1/vlan", "value": "1"}]
Patch Applier:    * [{"op": "add", "path": "/VLAN/Vlan1/members/0", "value": "Ethernet1"}]
Patch Applier:    * [{"op": "add", "path": "/VLAN_MEMBER/Vlan1|Ethernet1", "value": {"tagging_mode": "
untagged"}}]
Patch Applier: Applying 6 changes in order:
Patch Applier:    * [{"op": "remove", "path": "/INTERFACE/Ethernet1|10.2.2.3~124"}]
Patch Applier:    * [{"op": "remove", "path": "/INTERFACE/Ethernet1"}]
Patch Applier:    * [{"op": "add", "path": "/PORT/Ethernet1/tagging_mode", "value": "access"}]
Patch Applier:    * [{"op": "add", "path": "/PORT/Ethernet1/vlan", "value": "1"}]
Patch Applier:    * [{"op": "add", "path": "/VLAN/Vlan1/members/0", "value": "Ethernet1"}]
Patch Applier:    * [{"op": "add", "path": "/VLAN_MEMBER/Vlan1|Ethernet1", "value": {"tagging_mode":
"untagged"}}]
Patch Applier: Verifying patch updates are reflected on ConfigDB.
Patch Applier: Patch application completed.
Config Replacer: Verifying config replacement is reflected on ConfigDB.
Config Replacer: Config replacement completed.
Config Rollbacker: Config rollbacking completed.
Config rolled back successfully.
```