Naddod N9200-64DC and N9500-64OC Switch

SONiC CLI Guide

NADDOD Pte.Ltd.

Preface

Intended Audience

This document is intended for:

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

Technical Support

- Naddod Networks website: https://www.naddod.com
- Online support center: https://www.naddod.com/support
- Community: https://www.naddod.com/ai-insights
- Email support: support@naddod.com
- Live chat: https://www.naddod.com/about-us/contact-us
- Documentation feedback: info@naddod.com

Notes

The manual provides configuration information, including models, port types, and command line interfaces, for reference purposes only. In the event of any discrepancy or inconsistency between the manual and the actual version, the actual version shall take precedence.

Contents

1 Introduction

SONiC is an open source network operating system based on Linux that runs on switches from multiple vendors and ASICs. SONiC offers a full-suite of network functionality, like BGP and RDMA, that has been production-hardened in the data centers of some of the largest cloud-service providers. It offers teams the flexibility to create the network solutions they need while leveraging the collective strength of a large ecosystem and community.

SONiC software shall be loaded in these supported devices and this CLI guide shall be used to configure the devices as well as to display the configuration, state and status.

Follow the Quick Start Guide to boot the device in ONIE mode, install the SONiC software using the steps specified in the document and login to the device using the default username and password.

After logging into the device, SONiC software can be configured in following three methods.

1. Command Line Interface (CLI)
2. config_db.json
3. minigraph.xml

This document explains the first method and gives the complete list of commands that are supported in SONiC 201904 version (build#19). All the configuration commands need root privileges to execute them. Note that show commands can be executed by all users without the root privileges. Root privileges can be obtained either by using "sudo" keyword in front of all config commands, or by going to root prompt using "sudo -i". Note that all commands are case sensitive.

Example
admin@sonic:~$ sudo config aaa authentication login tacacs+ OR admin@sonic:~$ sudo -i root@sonic:~# config aaa authentication login tacacs+

Note that the command list given in this document is just a subset of all possible configurations in SONiC. Please

follow config_db.json based configuration for the complete list of configuration options.

2 Scope of this Document

It is assumed that all configuration commands start with the keyword "config" as prefix. Any other scripts/utilities/commands that need user configuration control are wrapped as sub-commands under the "config" command. The direct scripts/utilities/commands (examples given below) that are not wrapped under the "config" command are not in the scope of this document.

> acl_loader – This script is already wrapped inside "config acl" command; i.e. any ACL configuration that user is allowed to do is already part of "config acl" command; users are not expected to use the acl_loader script directly and hence this document need not explain the "acl_loader" script.

3 Not Supported Commands in this Document

In this document, some CLI commands or parameters of specific features are marked as "Not support". It may caused by varies reasons. These non-supported commands and parameters are still listed in this document to notify the user these commands, although existed in the Sonic CLI command Line, but it is not recommended to use these commands or parameters. Errors or unexpected results may occur if these commands or parameters are issued.

These commands existed in Community Sonic version, however, these commands/parameters are not working well due to the following reasons.

- The corresponding operations are not supported in the hardware platform.
- The corresponding operations are not fully implemented in Sonic platform or SAI driver.

- The corresponding operations are obsoleted compared with current Sonic implementation but the command is still kept.
- The corresponding operations has defects and under fixing.

4 Content Index of Articles

5 Getting Started with SONiC

This section covers the basic configurations related to the following:

- SSH Login
- Configuring the Management Interface

5.1 SSH Login

All SONiC devices support both serial console-based login and SSH-based login by default. The default credentials (if not modified at image build time) for login is admin/YourPaSsWoRd. In the case of SSH login, users can log in to the management interface (eth0) IP address after configuring the same using the serial console. Refer to the following section for configuring the IP address for the management interface.

Example
At Console: Debian GNU/Linux 9 sonic ttyS1 sonic login: admin Password: YourPaSsWoRd SSH from any remote server to sonic can be done by connecting to SONiC IP user@debug:~$ ssh admin@sonic_ip_address(or SONIC DNS Name) admin@sonic's password:

By default, login takes the user to the default prompt from which all the show commands can be executed.

5.2 Configuring the Management Interface

The management interface (eth0) in SONiC is configured (by default) to use DHCP client to get an IP address from a DHCP server.

Connect the management interface to the same network in which your DHCP server is connected and get the IP address from DHCP server. The IP address received from the DHCP server can be verified using the /sbin/ifconfig eth0 Linux command.

SONiC provides a CLI to configure a static IP for the management interface. There are a few ways by which a static IP address can be configured for the management interface.

Use the config interface ip add eth0 command.

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

Use config_db.json and configure the MGMT_INTERFACE key with the appropriate values. Refer to this page.

Use minigraph.xml and configure "Management IP Interfaces" tag inside "DpgDesc" tag, as given on this page.

Once the IP address is configured, it can be verified using either the show management_interface address command or the /sbin /ifconfig eth0 Linux command. Users can use SSH to log in to this management interface IP address from their management network.

Example
admin@sonic:~$ /sbin/ifconfig eth0 eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 10.11.11.13 netmask 255.255.255.0 broadcast 10.11.12.255

5.3 Getting Help

Help for Config Commands

All commands have in-built help that aids the user in understanding the command as well as the possible sub-commands and options. "-- help" can be used at any level of the command; i.e. it can be used at the command level, or sub-command level or at argument level.

The in-built help will display the available possibilities corresponding to that particular command/sub-command.

config –help

This command lists all the possible configuration commands at the top level.

Usage
config (-?|-h|--help)

Example
admin@sonic:~$ config --help Usage: config [OPTIONS] COMMAND [ARGS]... SONiC command line - 'config' command Options: -?, -h, --help Show this message and exit. Commands: aaa AAA command line acl ACL-related configuration tasks bgp BGP-related configuration tasks container Modify configuration of containers dropcounters Drop counter related configuration tasks ecn ECN-related configuration tasks feature Configure status of feature hostname Change device hostname without impacting the... interface Interface-related configuration tasks interface_naming_mode Modify interface naming mode for interacting with... is-loopback-name-valid Loopback name validation kdump Configure kdump load Import a previous saved config DB dump file. load_mgmt_config Reconfigure hostname and mgmt interface based on... load_minigraph Reconfigure based on minigraph. loopback Loopback-related configuration tasks mclag Multi-Chassis Link Aggregation Group-related... mirror_session nat NAT-related configuration tasks neigh_suppress Neighbour Suppress VLAN-related configuration ntp NTP server configuration tasks

pfcwd	Configure pfc watchdog
platform	Platform-related configuration tasks
portchannel	
pvlan	Private VLAN-related configuration tasks
qos	QoS-related configuration tasks
reload	Clear current configuration and import a previous...
route	route-related configuration tasks
sag	Static Anycast Gateway
save	Export current config DB to a file on disk.
sflow	sFlow-related configuration tasks
snmpagentaddress	SNMP agent listening IP address, port, vrf...
snmptrap	SNMP Trap server configuration to send traps
syslog	Syslog server configuration tasks
tacacs	TACACS+ server configuration
vlan	VLAN-related configuration tasks
vrf	VRF-related configuration tasks
vxlan	
warm_restart	warm_restart-related configuration tasks
watermark	Configure watermark
ztp	Configure Zero Touch Provisioning

Help for Show Commands

show --help

This command displays the full list of show commands available in the software; the output of each of those show commands can be used to analyze, debug or troubleshoot the network node.

Usage
show (-?|-h|--help)

Example

```
admin@sonic:~$ show --help
Usage: show [OPTIONS] COMMAND [ARGS]...
  SONiC command line - 'show' command
Options:
  -?, -h, --help  Show this message and exit.
Commands:
  aaa                 Show AAA configuration
  acl                 Show ACL related information
  arp                 Show IP ARP table
  boot                Show boot configuration
  buffer_pool         Show details of the buffer pools
  clock               Show date and time
  container           Show container
  dropcounters        Show drop counter related information
  ecn                 Show ECN configuration
  environment         Show environmentals (voltages, fans, temps)
  features            Show status of optional features
  interfaces          Show details of the network interfaces
  ip                  Show IP (IPv4) commands
  ipv6                Show IPv6 commands
  kdump               Show kdump configuration, status and information
  line                Show all /dev/ttyUSB lines and their info
  lldp                LLDP (Link Layer Discovery Protocol) information
  logging             Show system log
  mac                 Show MAC (FDB) entries
  management_interface  Show management interface parameters
  mclag               Show MCLAG related information
  mgmt-vrf            Show management VRF attributes
  mirror_session      Show existing everflow sessions
  mmu                 Show mmu configuration
  nat                 Show details of the nat
  ndp                 Show IPv6 Neighbour table
```

```
neigh-suppress       show neigh_suppress
ntp                  Show NTP information
pfc                  Show details of the priority-flow-control (pfc)
pfcwd                Show details of the pfc watchdog
pim                  Show details of the pims
platform             Show platform-specific hardware info
policer              Show existing policers
priority-group       Show details of the PGs
processes            Display process information
pvlan                Show Private VLAN related information
queue                Show details of the queues
reboot-cause         Show cause of most recent reboot
route-map            show route-map
runningconfiguration Show current running configuration information
sag                  show sag information
services             Show all daemon services
sflow                Show sFlow related information
snmpagentaddress     Show SNMP agent listening IP address configuration
snmptrap             Show SNMP agent Trap server configuration
startupconfiguration Show startup configuration information
subinterfaces        Show details of the sub port interfaces
system-memory        Show memory information
tacacs               Show TACACS+ configuration
techsupport          Gather information for troubleshooting
uptime               Show system uptime
users                Show users
version              Show version information
vlan                 Show VLAN information
vnet                 Show vnet related information
vrf                  Show vrf config
vxlan                Show VXLAN information
warm_restart         Show warm restart configuration and state
watermark            Show details of watermark
ztp                  Show Zero Touch Provisioning status
```

The same syntax applies to all subgroups of show which themselves contain subcommands, and subcommands which accept options/arguments.

Example
admin@sonic:~$ show interface -? Usage: show interface [OPTIONS] COMMAND [ARGS]... Show details of the network interfaces Options: -?, -h, --help Show this message and exit. Commands: alias Show Interface Name/Alias Mapping breakout Show Breakout Mode information by interfaces counters Show interface counters description Show interface status, protocol and description naming_mode Show interface naming_mode status neighbor Show neighbor related information portchannel Show PortChannel information status Show Interface status information transceiver Show SFP Transceiver information

5.4 Basic Show Commands

Table of Contents

Display system version

show version

This command displays software component versions of the currently running SONiC image. This includes the SONiC image version as well as Docker image versions. This command displays 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.

Usage

show version

Example
admin@sonic:~$ show version SONiC Software Version: SONiC.2305.1.8_MLNX SONiC OS Version: 11 Distribution: Debian 11.9 Kernel: 5.10.0-23-2-amd64 Build commit: ab82058e7 Build date: Tue Jun 25 03:53:22 UTC 2024 Built by: jenkins@server2 Platform: x86_64-accton_as9746-128d-r0 HwSKU: AS9746-128D ASIC: mellanox ASIC Count: 1 Serial Number: ATO42000011 Model Number: AS9746-128D Hardware Revision: R0B Uptime: 05:38:24 up 5 min, 1 user, load average: 2.03, 1.37, 0.63 Date: Wed 20 Nov 2024 05:38:24

Show System Status

This section explains some command sets that are used to display the status of various parameters pertaining to the physical state of the network node.

show clock

This command displays the current date and time configured on the system.

Usage
show clock

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

show boot

This command displays the current OS image, the image to be loaded on next reboot, and lists all the available images installed on the device.

Usage
show boot

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

show environment

This command displays the platform environmentals, such as voltages, temperatures and fan speeds.

Usage
show environment

Example
Example 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 includes a lot of information; only a sample output is shown 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 above.

show system status

This command displays if the SONiC system has finished booting or not.

You may use this command to inspect the progress state of the SONiC system bring-up. It might show the message in Example 2 (or 3) in the middle of the bring-up. If it is seen after the system is up, there could be some configuration issues in the configuration file.

Usage
show system status

The result of executing this command could be:

SONiC is ready, i.e. port provision is done and services are activated. (refer to Example1)

Port configuration is not fully provisioned (refer to Example2)

Not all SONiC services are ready (Example3, the "teamd" is not in service)

Example1 (SONiC is ready)
admin@sonic:~$ show system status

System is ready

Example2 (port provisioning incomplete)

```
admin@sonic:~$ show system status
System is not ready - Ports are not up
```

Example3 (SONiC system is not ready)

```
admin@sonic:~$ show system status
 System is not ready - core service is down
 Container and Inside Process    Status
 ------------------------------  --------
 database                        Up
 - redis                       Up
 swss                          Up
 - buffermgrd                    Up
 - fdbsyncd                    Up
 - intfmgrd                    Up
 - intfsyncd                   Up
 - nbrmgrd                     Up
 - neighsyncd                    Up
 - orchagent                   Up
 - portmgrd                    Up
 - portsyncd                   Up
 - vlanmgrd                    Up
 - vrfmgrd                     Up
 - vxlanmgrd                     Up
 syncd                         Up
 - syncd                       Up
 bgp                           Up
 - bgpcfgd                     Up
```

```
- bgpd                Up
- fpmsyncd              Up
- staticd             Up
- zebra               Up
mgmt-framework            Up
pmon                 Up
- psud                Up
- xcvrd               Up
teamd                Down
- teammgrd              N/A
- teamsyncd             N/A
lldp                 Up
- lldp-syncd            Up
- lldpd               Up
- lldpmgrd              Up
```

Status:

- Up: container or process (inside the container) is active/running.
- Down: container or process (inside the container) is not active/running.
    - In this example, teamd is the container.
- N/A: daemons (inside of the container) are not available when the container is Down.
    - In this example, teammgrd or teamsyncd is the daemon.

show reboot-cause

This command displays the cause of the previous reboot.

Usage
show reboot-cause

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

show uptime

This command displays the current system uptime.

Usage
show uptime

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

show logging

This command displays 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 using the command sudo cat syslog as this requires root login.

Usage
show logging [(<process_name> [-l|--lines <number_of_lines>]) | (-f|--follow)]

Example
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.

Example
admin@sonic:~$ show logging | more

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

Example
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.

Example
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.

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

show users

This command displays a list of users currently logged in to the device.

Usage
show users

Example
admin@sonic:~$ show users admin pts/9 Mar 25 20:31 (100.127.20.23) admin ttyS1 2019-03-25 20:31

Show Hardware Platform

The information displayed in this set of commands partially overlaps with the one generated by the "show environment" instruction. In this case though, the information is presented in a more succinct fashion. In the future, these two CLI stanzas may end up being combined.

show platform fan

This command displays the fans status and information.

Usage
show platform fan

Example
admin@sonic:~$ show platform fan Drawer LED FAN Speed Direction Presence Status Timestamp

```
-------- ----- ---------- ------- ---------- ---------- -------- -----------------
FanTray1  green      FAN-1F     40%     exhaust    Present       OK  20220527 07:21:02
FanTray1  green      FAN-1R     40%     exhaust    Present       OK  20220527 07:21:02
FanTray2  green      FAN-2F     40%     exhaust    Present       OK  20220527 07:21:02
FanTray2  green      FAN-2R     40%     exhaust    Present       OK  20220527 07:21:02
FanTray3  green      FAN-3F     40%     exhaust    Present       OK  20220527 07:21:02
FanTray3  green      FAN-3R     40%     exhaust    Present       OK  20220527 07:21:02
FanTray4  green      FAN-4F     40%     exhaust    Present       OK  20220527 07:21:02
FanTray4  green      FAN-4R     40%     exhaust    Present       OK  20220527 07:21:02
FanTray5  green      FAN-5F     40%     exhaust    Present       OK  20220527 07:21:02
FanTray5  green      FAN-5R     40%     exhaust    Present       OK  20220527 07:21:02
    N/A  green  PSU-1 FAN-1     12%     exhaust    Present       OK  20220527 07:21:19
    N/A  green  PSU-2 FAN-1     13%     exhaust    Present       OK  20220527 07:21:20
```

show platform firmware status

This command displays the platform components status.

Usage
show platform firmware status

Example

```
admin@sonic:~$ show platform firmware status
Chassis         Module    Component    Version      Description
--------------  --------  -----------  -----------  -------------------------
5835-54X-O-AC-F  N/A       CPLD1        1            CPLD 1
                           CPLD2        1            CPLD 2
                           CPLD3        1            CPLD 3
                           BIOS         v47.01.01.00  Basic Input/Output System
```

show platform firmware update status(not supported)

This command displays the platform components auto_update status.

Usage
show platform firmware update status

Note:

This command do not supported.

show platform firmware updates

This command displays the available updates.

Usage
show platform firmware updates

Example
root@sonic:/home/admin# show platform firmware updates Chassis Module Component Firmware Version (Current/Available) Status --------- -------- ----------- ---------- ---------- ---------- CX9880 N/A OCM_CPLD /etc/naddod/fw/n9500-64oc/components_fw/CX9880_OCM_CPLD_v0A07_Internal.vme 0a.07 / 0a.07 up-to-date BASE_CPLD /etc/naddod/fw/n9500-64oc/components_fw/BASE_Board_CPLD_v0A.0Ah_Internal.vme 0a.0a / 0a.0a up-to-date PORT_CPLD1 /etc/naddod/fw/n9500-64oc/components_fw/PORT1_CPLD_v0A05.vme 0a.05 / 0a.05 up-to-date PORT_CPLD2 /etc/naddod/fw/n9500-64oc/components_fw/PORT2_CPLD_v0A06.vme 0a.06 / 0a.06 up-to-date

FPGA /etc/naddod/fw/n9500-64oc/components_fw/Switch_FPGA_v1A_04h_golden_v0A_04h_primary.bin 0a.04 / 0a.04 up-to-date BIOS /etc/naddod/fw/n9500-64oc/components_fw/cx9880_d1734-bios_v41.0A.00.05-SPS_05.00.04.0100.0.bin v41.0A.00.05 / v41.0A.00.05 up-to-date SDA_SSD /etc/naddod/fw/n9500-64oc/components_fw/F3C1T108_240_480_960.bin TEV35U / F3C1T108 update is required SDB_SSD /etc/naddod/fw/n9500-64oc/components_fw/F3C1T108_240_480_960.bin TEV35U / F3C1T108 update is required

Note:

Not supported on DCS8500-128D, N9200-64D, N9500-128D, CN9500-128D, CN9500-64D, AS9736-64D.

Supported on AS9817-64OC, N9500-64OC.

This function check EEPROM TLV "0x21 Product Name" field, If not match platform/device name, this command will failed.

show platform firmware version

This command displays the utility version.

Usage
show platform firmware version

Example
admin@sonic:~$ show platform firmware version

fwutil version 2.0.0.0

show platform pcieinfo

This command displays the platform pcie information .

Usage
show platform pcieinfo

Example
admin@as5835-54x:~$ show platform pcieinfo Failed to load platform Pcie module. Error : No module named 'sonic_platform.pcie', fallback to load Pcie common utility. ==========Display PCIe Device========== bus:dev.fn 00:00.0 - dev_id=0x1980, Host bridge: Intel Corporation Atom Processor C3000 Series System Agent(rev 11) bus:dev.fn 00:04.0 - dev_id=0x19a1, Host bridge: Intel Corporation Atom Processor C3000 Series ErrorRegisters (rev 11) bus:dev.fn 00:05.0 - dev_id=0x19a2, Generic system peripheral [0807]: Intel Corporation Atom Processor C3000 Series Root Complex Event Collector (rev 11) bus:dev.fn 00:06.0 - dev_id=0x19a3, PCI bridge: Intel Corporation Atom Processor C3000 Series Integrated QATRoot Port (rev 11) bus:dev.fn 00:09.0 - dev_id=0x19a4, PCI bridge: Intel Corporation Atom Processor C3000 Series PCI ExpressRoot Port #0 (rev 11) bus:dev.fn 00:0b.0 - dev_id=0x19a6, PCI bridge: Intel Corporation Atom Processor C3000 Series PCI ExpressRoot Port #2 (rev 11) bus:dev.fn 00:0e.0 - dev_id=0x19a8, PCI bridge: Intel Corporation Atom Processor C3000 Series PCI ExpressRoot Port #4 (rev 11) bus:dev.fn 00:10.0 - dev_id=0x19aa, PCI bridge: Intel Corporation Atom Processor C3000 Series PCI ExpressRoot Port #6 (rev 11)

bus:dev.fn 00:12.0 - dev_id=0x19ac, System peripheral: Intel Corporation Atom Processor C3000 Series SMBus
Contoller - Host (rev 11)
bus:dev.fn 00:13.0 - dev_id=0x19b2, SATA controller: Intel Corporation Atom Processor C3000 Series SATA Controller 0 (rev 11)
bus:dev.fn 00:15.0 - dev_id=0x19d0, USB controller: Intel Corporation Atom Processor C3000 Series USB 3.0 xHCI Controller (rev 11)
bus:dev.fn 00:16.0 - dev_id=0x19d1, PCI bridge: Intel Corporation Atom Processor C3000 Series Integrated LAN Root Port #0 (rev 11)
bus:dev.fn 00:17.0 - dev_id=0x19d2, PCI bridge: Intel Corporation Atom Processor C3000 Series Integrated LAN
Root Port #1 (rev 11)
bus:dev.fn 00:18.0 - dev_id=0x19d3, Communication controller: Intel Corporation Atom Processor C3000 Series
ME HECI 1 (rev 11)
bus:dev.fn 00:1a.0 - dev_id=0x19d8, Serial controller: Intel Corporation Atom Processor C3000 Series HSUART
Controller (rev 11)
bus:dev.fn 00:1a.1 - dev_id=0x19d8, Serial controller: Intel Corporation Atom Processor C3000 Series HSUART
Controller (rev 11)
bus:dev.fn 00:1a.2 - dev_id=0x19d8, Serial controller: Intel Corporation Atom Processor C3000 Series HSUART
Controller (rev 11)
bus:dev.fn 00:1f.0 - dev_id=0x19dc, ISA bridge: Intel Corporation Atom Processor C3000 Series LPC or eSPI (rev 11)
bus:dev.fn 00:1f.1 - dev_id=0x19dd, Memory controller: Intel Corporation Atom Processor C3000 Series Primary
to Side Band (P2SB) Bridge (rev 11)
bus:dev.fn 00:1f.2 - dev_id=0x19de, Memory controller: Intel Corporation Atom Processor C3000 Series Power
Management Controller (rev 11)
bus:dev.fn 00:1f.4 - dev_id=0x19df, SMBus: Intel Corporation Atom Processor C3000 Series SMBus controller
(rev 11)

bus:dev.fn 00:1f.5 - dev_id=0x19e0, Serial bus controller [0c80]: Intel Corporation Atom Processor C3000 Series SPI Controller (rev 11)
bus:dev.fn 01:00.0 - dev_id=0x19e2, Co-processor: Intel Corporation Atom Processor C3000 Series QuickAssist
Technology (rev 11)
bus:dev.fn 02:00.0 - dev_id=0xb771, Ethernet controller: Broadcom Inc. and subsidiaries Device b771 (rev 01)
bus:dev.fn 05:00.0 - dev_id=0x1533, Ethernet controller: Intel Corporation I210 Gigabit Network Connection (rev 03)
bus:dev.fn 06:00.0 - dev_id=0x15c2, Ethernet controller: Intel Corporation Ethernet Connection X553 Backplane (rev 11)
bus:dev.fn 08:00.0 - dev_id=0x15e5, Ethernet controller: Intel Corporation Ethernet Connection X553 1GbE (rev 11)

show platform psustatus

This command displays the status of the device's power supply units.

Usage
show platform psustatus

Example

```
admin@sonic:~$ show platform psustatus
PSU    Model     Serial    HW Rev     Voltage (V)    Current (A)    Power (W)  Status    LED
-----  --------  --------  --------  -------------  -------------  -----------  --------  -----
PSU 1  YM-2651Y  N/A       N/A             12.06          4.62        56.00  OK        green
PSU 2  YM-2651Y  N/A       N/A             12.23          5.82        71.00  OK        green
```

show platform ssdhealth

This command displays health parameters of the device's SSD.

Usage
show platform ssdhealth [--vendor]

Example
admin@as9716-32d-1:~$ show platform ssdhealth Device Model : M.2 (S42) 3ME4 Health : 98.633% Temperature : 40C

Note: This command needs root privilege.

show platform summary

This command displays a summary of the device's hardware platform.

Usage
show platform summary

Example
admin@Sonic:~$ show platform summary Platform: x86_64-accton_as9746_32d-r0 HwSKU: Accton-AS9746-32D-100G ASIC: broadcom

show platform syseeprom

This command displays information stored on the system EEPROM. Note that the output of this command is not the same for all vendor's platforms. A couple of example outputs are given below.

Usage
show platform syseeprom

Example

```
admin@sonic:~$ show platform syseeprom
TlvInfo Header:
  Id String:    TlvInfo
  Version:     1
  Total Length: 117
TLV Name             Code     Len  Value
-------------------  ------  -----  --------------------------
Product Name         0x21       15  5835-54X-O-AC-F
Part Number          0x22       13  FP1ZZ56540B7A
Serial Number        0x23       14  583554X1218123
Base MAC Address     0x24        6  80:A2:35:D2:4C:B5
Platform Name        0x28       27  x86_64-accton_as5835_54x-r0
MAC Addresses        0x2A        2  256
Manufacturer         0x2B        6  Accton
Manufacture Country  0x2C        2  CN
Vendor Name          0x2D        8  Accton
CRC-32               0xFE        4  0xA334B01A
(checksum valid)
```

show platform temperature

The command displays device temperature information.

Usage
show platform temperature

Example

```
admin@sonic:~$ show platform temperature
        Sensor    Temperature    High TH    Low TH    Crit High TH    Crit Low TH    Warning Timestamp
-------------------------------------------------------------------------------------------------------------
PSU-1 temp sensor 1        32         80      N/A          N/A          N/A     False  2022052707:51:05
PSU-2 temp sensor 2        32         80      N/A          N/A          N/A     False  2022052707:51:06
        Temp sensor 1      35.5        80       N/A          N/A          N/A      False  2022052707:51:04
        Temp sensor 2      26.5        80       N/A          N/A          N/A      False  2022052707:51:04
        Temp sensor 3      28.5        80       N/A          N/A          N/A      False  2022052707:51:04
        Temp sensor 4      28         80      N/A          N/A          N/A     False  2022052707:51:04
```

Transceivers

Displays diagnostic monitoring information of the transceivers.

show interfaces transceiver

This command displays transceiver information for all interfaces, or for a specific interface when the option interface_name is specified.

Usage
show interfaces transceiver (eeprom [-d|--dom] | lpmode | presence) [<interface_name>]

Example (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
```

Example (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
```

Example (Display presence of SFP transceiver connected to Ethernet100):

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

Show PIM Status

Displays the status of the PIM cards.

show pim status

This command displays information for all PIM cards.

Example (Display status for all PIM card):

```
admin@sonic:~$ show pim status
Slot Index    Operation Status    Type     HW Status
------------  ------------------  -------  ---------------
slot 2        up                  PIM-16Q  status code: 0b1
slot 3        up                  PIM-16Q  status code: 0b1
```

slot 4	up	PIM-16Q status code: 0b1
slot 5	up	PIM-16Q status code: 0b1
slot 6	up	PIM-16Q status code: 0b1
slot 7	up	PIM-16Q status code: 0b1
slot 8	up	PIM-16Q status code: 0b1
slot 9	up	PIM-16Q status code: 0b0

Note: This command only works for platforms that support PIM hotswap, for example the AS8000.

6 Authentication, Authorization, and Accounting

This section captures the various show and configuration commands that are applicable to the AAA (Authentication, Authorization, and Accounting) module. You can configure the type of authentication (local or remote TACACS based) required for the users and also the authentication failthrough and fallback options.

6.1 AAA

Table of Contents

AAA show commands

This command is used to view the Authentication, Authorization & Accounting settings that are configured in the network node.

show aaa

This command displays the AAA settings currently present in the network node.

Usage
show aaa

Example
admin@sonic:~$ show aaa AAA authentication login local (default) AAA authentication failthrough False (default) AAA authorization login local (default) AAA accounting login disable (default)

AAA config commands

This sub-section explains all the possible CLI based configuration options for the AAA module. The list of commands/sub-commands possible for AAA is given below.

Commands:

aaa authentication sub-commands:

aaa authentication failthrough

aaa authentication fallback

aaa authentication login

aaa authentication failthrough

This command is used to either enable or disable the failthrough option. This command is useful when a user has configured more than one authentication servers or methods. When an authentication request to the first server fails, this configuration allows it to continue the request to the next server or method. When this configuration is enabled, the authentication process continues through all servers or methods configured. When disabled and if the authentication request fails on first server, the authentication process will stop and the login will be disallowed.

Usage
config aaa authentication failthrough (enable | disable | default)

Parameters:

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 "disable".

The below example enables the failthrough option.

Example
admin@sonic:~$ sudo config aaa authentication failthrough enable

aaa authentication fallback

When the servers used in TACACS+ authentication are unreachable, it falls back to local authentication by default.

The fallback function is always enabled in the current design, which means this command takes no effect.

Usage
config aaa authentication fallback (enable | disable | default)

The below example enables the fallback option.

Example
admin@sonic:~$ sudo config aaa authentication fallback enable

aaa authentication login

This command is used to configure the sequence of the authentication methods must be performed.

Usage
config aaa authentication login {radius | tacacs+ | local} [radius | tacacs+ | local]...

Parameters:

radius: Enables remote authentication based on RADIUS.

tacacs+: Enables remote authentication based on TACACS+.

local: Uses local authentication.

default: Resets back to the default value, which is only "local" authentication.

The command below configures AAA to use a remote TACACS+ database for user authentication.

Example
admin@sonic:~$ sudo config aaa authentication login tacacs+ local

aaa authentication login default

This command is used to restore the aaa authentication login configuration.

Usage
config aaa authentication login default

Parameters:

default: Resets back to the default value, which is only "local" authentication.

aaa authorization

This command is used to enable authorization and define the sequence of the authorization methods must be performed.

Usage
config aaa authorization {tacacs+ | local} [local]

Parameters:

tacacs+: Enables TACACS+ authorization.

local: Enables local authorization.

default: Resets back to the default value, which is only "local" authorization.

Example
admin@sonic:~$ sudo config aaa authorization tacacs+

aaa authorization default

This command is used to restore the aaa authorization configuration.

Usage
config aaa authorization default

Parameters:

default: Resets back to the default value, which is only "local" authorization.

aaa accounting

This command is used to enable or disable accounting. If accounting enabled, all the methods will be performed.

Usage
config aaa accounting {tacacs+ | local} [tacacs+ | local]

Parameters:

tacacs+: Enable TACACS+ accounting.

local: Enable local accounting in syslog.

disable: Disable accounting.

Example
admin@sonic:~$ sudo config aaa accounting tacacs+

aaa accounting disable

This command is used to disable accounting.

Usage
config aaa accounting disable

Parameters:

disable: Disable accounting.

6.2 TACACS+

Table of Contents

TACACS+ show commands

show tacacs

This command displays the global configuration fields and the list of all TACACS+ servers and their corresponding configurations.

Usage
show tacacs

The command below shows the TACACS+ configuration.

Example
admin@sonic:~$ show tacacs TACPLUS global auth_type pap (default) TACPLUS global timeout 99 TACPLUS global passkey <EMPTY_STRING> (default) TACPLUS_SERVER address 10.11.12.14 priority 9 tcp_port 50 auth_type mschap timeout 10

passkey testing789 TACPLUS_SERVER address 10.0.0.9 priority 1 tcp_port 49

TACACS+ config commands

config tacacs add

This command is used to add a TACACS+ server to the TACACS server list. Note that more than one TACACS+ server (maximum of eight) can be added to the device. When a user tries to log in, the TACACS client will contact the servers one by one. When any server times

out, the device will try the other servers 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 the /etc/pam.d/common-auth-sonic configuration file that is being used by the TACACS service.

Usage
config tacacs add <ip_address> [-t|--timeout <seconds>] [-k|--key <secret>] [-a|--type <type>] [-o|--port <port>] [-p|--pri <priority>] [-m|--use-mgmt-vrf]

Parameters:

- ip_address : TACACS+ server IP address.
- timeout : transmission timeout interval in seconds. range 1 to 60, default 5
- key : shared secret key for authentication.
- type , "chap" or "pap" or "mschap" or "login".
    - default is "pap". port: TCP
    - "mschap" is not supported now and "pap" is used instead if authtype is configured as "mschap".
- port : port range is 1 to 65535. default 49.

- pri : priority.
    - range 1 to 64, default 1.
- use-mgmt-vrf : indicate that the server is part of the Management VRF.
    - default is "no vrf".

The command below adds a new TACACS+ server with the parameters.

Example
admin@sonic:~$ sudo config tacacs add 10.11.12.13 -t 10 -k testing789 -a pap -o 50 -p 9

config tacacs delete

This command is used to delete the TACACS+ servers configured.

Usage
config tacacs delete <ip_address>

Parameters:

ip_address : TACACS+ server IP address.

The example below deletes a TACACS+ server by IP address.

Example
admin@sonic:~$ sudo config tacacs delete 10.11.12.13

config tacacs authtype

This command is used to specify the global auth-type of TACACS+ servers.

Usage
config tacacs authtype {chap | pap | mschap | login}

Parameters:

chap : Challenge-handshake authentication protocol.

pap: Password authentication protocol.

mschap : Microsoft version (version 2) of the challenge-handshake authentication protocol.

login : Clear text.

Example
sudo config tacacs authtype mschap

config tacacs default authtype

This command is used to restore the global auth-type of TACACS+ servers.

Usage
config tacacs default authtype

Parameters:

none. The default is pap .

Example
sudo config tacacs default authtype

config tacacs passkey

This command is used to specify the global passkey of TACACS+ servers.

Usage
config tacacs passkey <passkey>

Parameters:

passkey: shared secret key (Valid chars: ASCII printable except SPACE, '#', and COMMA).

Example
admin@sonic:~$ sudo config tacacs passkey testing123

config tacacs default passkey

This command is used to restore the global passkey of TACACS+ servers.

Usage
config tacacs default passkey

Parameters:

none.

The default is blank string.

Example
sudo config tacacs default passkey

config tacacs timeout

This command is used to specify the global timeout of TACACS+ servers.

Usage
config tacacs timeout <timeout>

Parameters:

timeout : duration in seconds to wait for before determining that the server has failed to respond. Minimum: 1. Maximum: 60.

Example (Configure non-default case)
sudo config tacacs timeout 60

config tacacs default timeout

This command is used to restore the global timeout of TACACS+ servers.

Usage
config tacacs default timeout

Parameters:

none

The default is 5 seconds.

Example
sudo config tacacs default timeout

config tacacs source ip

This command is used to specify the global source address of TACACS+ servers.

Usage
config tacacs sourceip <source-ip>

Parameters:

source-ip: source IP address (IPv4 or IPv6) for the outgoing TCP/IP dgram.

Example
sudo config tacacs sourceip 192.168.3.45

6.3 RADIUS

Table of Contents

The document shows several commands related to RADIUS service as a RADIUS client (NAS).

RADIUS Show Commands

show radius

This command is used to show RADIUS configuration.

Usage
show radius

Example
admin@sonic:~$ show radius RADIUS global auth_type pap (default) RADIUS global retransmit 3 (default) RADIUS global timeout 5 (default) RADIUS global passkey <EMPTY_STRING> (default) RADIUS_SERVER address 192.168.3.45 auth_port 1812 priority 1

RADIUS Configuration Commands

config radius timeout

This command is used to specify the global timeout of RADIUS servers.

Usage
config radius timeout <timeout>

Parameters:

timeout: duration in seconds to wait for before determining that the server has failed to respond. Minimum: 1. Maximum: 60.

Example
sudo config radius time 5

config radius default timeout

This command is used to restore the global timeout of RADIUS servers.

Usage
config radius default timeout

Parameters:

none

The default is 5 seconds.

Example

sudo config radius default timeout

config radius retransmit

This command is used to specify the global retry attempts of RADIUS servers.

Usage
config radius retransmit <retries>

Parameters:

retries: number of times to re-send a packet, if there is no response. Minimum: 0. Maximum: 10.

Example
config radius retransmit 5

config radius default retransmit

This command is used to restore the global retry attempts of RADIUS servers.

Usage
config radius default retransmit

Parameters:

none

The default is 3 times.

Example

sudo config radius default retransmit

config radius authtype

This command is used to specify the global auth-type of RADIUS servers.

Usage
config radius authtype {chap|pap|mschapv2}

Parameters:

chap : Challenge-handshake authentication protocol.

pap: Password authentication protocol.

mschapv2 : Microsoft version (version 2) of the challenge-handshake authentication protocol.

Example
sudo config radius authtype chap

config radius default authtype

This command is used to restore the global auth-type of RADIUS servers.

Usage
config radius default authtype

Parameters:

none

The default is pap .

Example
sudo config radius default authtype

config radius passkey

This command is used to specify the global passkey of RADIUS servers.

Usage
config radius passkey <passkey>

Parameters:

passkey: shared secret key (Valid chars: ASCII printable except SPACE, '#', and COMMA).

Example
sudo config radius passkey PASSKEY

config radius default passkey

This command is used to restore the global passkey of RADIUS servers.

Usage
config radius default passkey

Parameters:

none

The default is blank string.

Example
sudo config radius default passkey

config radius source ip

This command is used to specify the global source address of RADIUS servers.

Usage
config radius sourceip <source-ip>

Parameters:

source-ip: source IP address (IPv4 or IPv6) used in the IP header of the outgoing UDP/IP dgram.

Example
sudo config radius sourceip 192.168.3.45

config radius default source ip

This command is use to restore the global source address of RADIUS servers.

Usage
config radius default sourceip

Parameters:

none

The default ip address is determined by routing stack.

Example
sudo config radius default sourceip

config radius nasip

This command is used to specify the global NAS-IP address of RADIUS servers.

Usage
config radius nasip <nas-ip>

Parameters:

nas-ip: NAS-IP (IPv4 Address, Type4) or IPV6-Address (Type 95) attribute in the outgoing RADIUS PDU. If the nas-ip is not configured, one of the management IP addresses or the source IP address will be used as NAS-IP.

Example
sudo config radius nasip 192.168.3.45

config radius default nasip

This command is used to remove the global NAS-IP address of RADIUS servers.

Usage
config radius default nasip

Parameters:

none

Example
sudo config radius default nasip

config radius statistics

This command is used to specify the global statistics RADIUS servers.

Usage
config radius statistics {enable|disable|default}

Parameters:

enable: enable statistics collection.

disable: disable statistics collection.

default: reset to disable.

Example
sudo config radius statistics default

config radius add

Usage
config radius add <ip_address_or_domain_name> [--retransmit <retransmit>] [--timeout <timeout>] [--key <key>] [--auth_type {chap | pap | mschapv2}] [--auth-port <auth-port>] [--pri <priority>] [--user-mgmt-vrf]

[--source-interface <source-interface>]

Parameters:

- <ip_address_or_domain_name>: RADIUS server's DNS name, IPv4 or IPv6 address.
- <retransmit>: number of times to re-send a packet if there is no response.
- <timeout>: duration in seconds to wait for before determining that the server has failed to respond. <key>: shared secret key (Valid chars: ASCII printable except SPACE, '#', and COMMA).
- <auth_type>: authentication type. Valid values are:
    - chap : Challenge-handshake authentication protocol.
    - pap: Password authentication protocol.
    - mschapv2 : Microsoft version (version 2) of the challenge-handshake authentication protocol. <auth-port>: authentication port number.
- <priority>: specify RADIUS server's priority.
- --use-mgmt-vrf: use default vrf if not specified.
- <source-interface>: eg: eth0, Loopback0... Use the first IP address retrieved for the interface for the outgoing UDP/IP dgram. The default interface is determined by the routing stack.

Example
sudo config radius add 192.168.3.45 --key test --auth-port 10240

config radius delete

This command is used to delete a RADIUS server.

Usage
config radius delete <ip_address_or_domain_name>

Parameters:

<ip_address_or_domain_name>: IP address or domain name of RADIUS server.

Example
sudo config radius delete 192.168.3.45

6.4 User privilege

User privilege show command

userpri show

This command is used to show the privilege level information of users.

Usage

userpri show
Example
root@sonic:/home/admin# userpri show test 7 local 1 root@sonic:/home/admin#

Notes:

- userpri show can display all users except root and admin.

Different user privilege levels correspond to different access permissions, which are locally authorized. The planning is as follows:

Privilege Level	Type	Group	Permissions
15	Admin	sudo/ docker	Can access all commands.

2-14	Regular User	users	Cannot use **sudo su** or access configuration commands (e.g., **redis-cli**, **sonic-cli**, **vtysh**, **docker**, etc.). Other commands, such as common Linux commands and **show**, are accessible.
1	Guest	users	Can only access **show** commands.

User privilege config command

userpri <username> <privilege>

This command is used to config the privilege level information of users.

Usage
userpri <username> <privilege>

Example
root@sonic:/home/admin# userpri local 1 root@sonic:/home/admin# userpri show test 7 local 1 root@sonic:/home/admin#

Note:

- If the username does not exist, an error will be reported.
- It is not allowed to configure the privilege levels for root and admin.

7 ACL

Table of Contents

This section explains the various show and configuration commands available for users.

ACL Show Commands

show acl table-type

This command is used to display the user-defined ACL table type.

Usage
show acl table-type [<type_name>]

Parameter

- <type_name>: The table type to be displayed.

The following example shows how to display all the ACL table types that are currently defined.

Example
admin@sonic:~$ show acl table-type

```
Name     Bind Point    Match                  Policer
-------  ------------  ---------------------  ---------
L3_DSCP      PORT         Src IPv4 address
                             Dst IPv4 address
                             DSCP
                             IP type
```

show acl table

Displays a specific table or all.

Usage
show acl table [<table_name>]

Parameter

- <table_name>, the table to be displayed.

This command shows the table's name, type, bound interface(s), and applied stage.

Example

```
admin@sonic:~$ show acl table
Name      Type       Binding         Description      Stage    Policer
--------  ---------  --------------  ---------------  -------  ---------
EVERFLOW  MIRROR     Ethernet16      EVERFLOW         ingress
                     Ethernet96
                     Ethernet108
                     Ethernet112
```

```
                PortChannel0001
                PortChannel0002
SNMP_ACL  CTRLPLANE  SNMP          SNMP_ACL       ingress
DT_ACL_T1 L3       Ethernet0      DATA_ACL_TABLE_1 egress
                Ethernet4
                Ethernet112
                Ethernet116
SSH_ONLY  CTRLPLANE  SSH           SSH_ONLY       ingress
```

show acl rule

Displays the rules in a specific ACL table or all tables, or a specific rule in the specified table.

Usage
show acl rule [<table_name> [<rule_name>]]

Parameter

- <table_name>: The name of the ACL table to display the rules for.
- <rule_name>: The name of the rule to display.

Example

```
admin@sonic:~$ show acl rule
Table     Rule         Priority    Action                Match                    Status
--------  -----------  ----------  --------------------  -------------------------- --------
SNMP_ACL  RULE_1       9999        ACCEPT                IP_PROTOCOL: 17          Active
                                                         SRC_IP: 1.1.1.1/32       Active
```

```
SSH_ONLY  RULE_2       9998       ACCEPT                IP_PROTOCOL: 6           Active
                                                SRC_IP: 1.1.1.1/32          Active
EVERFLOW  RULE_3       9997       MIRROR INGRESS: everflow0  SRC_IP: 20.0.0.2/32        Active
EVERFLOW  RULE_4       9996       MIRROR EGRESS : everflow1  L4_SRC_PORT: 4621          Active
DATAACL   RULE_5       9995       REDIRECT: Ethernet8       IP_PROTOCOL: 126           Active
DATAACL   RULE_6       9994       FORWARD               L4_SRC_PORT: 179          Active
DATAACL   RULE_7       9993       FORWARD               L4_DST_PORT: 179          Active
SNMP_ACL  DEFAULT_RULE  1          DROP                  ETHER_TYPE: 2048          Active
SSH_ONLY  DEFAULT_RULE  1          DROP                  ETHER_TYPE: 2048          Active
```

Information in the table(s):

- Table: ACL table name
- Rule: ACL rule name in the table
- Priority: The priority of the rule, where a larger value indicating higher priority. The priority value is automatically assigned based on the sequence-id in the ACL rule configuration file. Please refer to the ACL Rule Configuration File section for more information.
- Action

  action to be executed when a packet matches the rule. One of the following:

- ACCEPT
  - for control plane ACL
- DROP
- FORWARD
- MIRROR INGRESS <mirror section>
- MIRROR EGRESS <mirror section>
- REDIRECT <redirect-object>
  - <redirect-object> One of the following::
    - interface; e.g., physical interface (Ethernet10) or port channel (PortChannel0002)
    - next-hop IP address, e.g., "10.0.0.1"
    - next-hop group of IP address(s), e.g., "10.0.0.1, 10.0.03"

- Match: The matching pattern of the frame header. The rule is executed when the ingress frame matches the pattern. Status: The rule status. Active is the rule be configured in hardware, inactive is not.

aclshow

Using aclshow to display ACL rules and counters.

Usage
aclshow [{-c | --clear}] [{-a | --all}] [{-t | --tables} TABLES] [{-r | --rules} RULES]

Parameters:

- clear, clear ACL counters' statistics.
- all, show all ACL counters.
- rules <RULES>, list of ACL rules. For example: "Rule_1,Rule_2".
- table <TABLES>, list of ACL tables. For example: "Table_1,Table_2".

Notes:

- If the PACKETS COUNT and BYTES COUNT are shown as N/A, either the rule hasn't been successfully written into the hardware or the counter value hasn't be read by the flex-counter. Check the syslog for the specified error message, or use counterpoll command to change the pool interval.

Example
admin@sonic:~$ aclshow -a RULE NAME TABLE NAME PRIO PACKETS COUNT BYTES COUNT ---------- ---------- ------ -------------- ------------ RULE_1 L3_TABLE 9999 0 0 DEFAULT_RULE L3_TABLE 1 0 0

counterpoll show

Show each counter configuration.

Usage
counterpoll show

Example
admin@sonic:~$ counterpoll show Type Interval (in ms) Status ---------- ---------- -------- QUEUE_STAT 1000 enable PORT_STAT default (1000) enable PORT_BUFFER_DROP default (60000) enable RIF_STAT default (1000) enable QUEUE_WATERMARK_STAT 10000 enable PG_WATERMARK_STAT 10000 enable PG_DROP_STAT default (10000) enable BUFFER_POOL_WATERMARK_STAT 10000 enable ACL default (10000) enable

ACL Configuration Commands

This sub-section explains the list of configuration options available for the ACL module.

config acl add table-type

This command is used to create a user-defined ACL table type.

```
config acl add table-type <type_name> [--bind-points <bind_points>]
[--match-vlan-id] [--match-cos]
[--match-src-ip4] [--match-dst-ip4]
[--match-src-ip6] [--match-dst-ip6]
[--match-dscp] [--match-l4-src-port] [--match-l4-dst-port]
[--action-set-policer]
```

Parameters:

- <type_name>: The name of the ACL table type.
- bind-points: A comma-separated list of interface types that can be bound to the ACL table type. Valid values are "PORT" and "PORTCHANNEL". The default value is "PORT".
- match-vlan-id: Specifies that the ACL table type can match the VLAN ID of IP packets.
- match-cos: Specifies that the ACL table type can match the VLAN PCP of IP packets.
- match-src-ip4: Specifies that the ACL table type can match the source IP address of IPv4 packets. This parameter cannot be specified with match-src-ip6 and match-dst-ip6 at the same time.
- match-dst-ip4: Specifies that the ACL table type can match the destination IP address of IPv4 packets. This parameter cannot be specified with match-src-ip6 and match-dst-ip6 at the same time.
- match-src-ip6: Specifies that the ACL table type can match the source IP address of IPv6 packets. This parameter cannot be specified with match-src-ip4 and match-dst-ip4 at the same time.
- match-dst-ip6: Specifies that the ACL table type can match the destination IP address of IPv6 packets. This parameter cannot be specified with match-src-ip4 and match-dst-ip4 at the same time.
- match-dscp: Specifies that the ACL table type can match the DSCP value of IP packets.
- match-l4-src-port: Specifies that the ACL table type can match the source port of TCP/UDP packets.
- match-l4-dst-port: Specifies that the ACL table type can match the destination port of TCP/UDP packets. action-set-policer: Specifies that the ACL table type can be bound to a policer.
- Notes:
    - The ACL table type only is supported to match IP packets (IPv4 or IPv6).
    - AS9736-64D switches, match-vlan-id and match-cos are not supported for the egress stage.

- The following example shows how to create a user-defined ACL table type that can be used to match the source IP address and DSCP for IPv4 packets.

Example
config acl add table-type L3_DSCP --match-src-ip4 --match-dscp

config acl remove table-type

This command is used to remove a user-defined ACL table type.

Usage
config acl remove table-type <type_name>

Parameters:

- <type_name>: The name of the ACL table type.

The following example shows how to remove a user-defined ACL table type.

Example
admin@sonic:~$ sudo config acl remove table-type L3_DSCP

config acl add table

This command applies an ACL to the data plane or control plane. When it's applied to the data plane, the rules are applied to the frame in chip. When it's applied to the control plane, they are applied to the frame trapped to the CPU from the chip.

When applying an ACL to the data plane, you need to use <type> to specify the IP header type or mirroring, the interface, and the stage at which the ACL rules of the table are applied for filtering or forwarding packets.

Usage for data plane
config acl add table <table_name> <type> [{-d | --description} <description>] [{-p | --ports} <interfaces>] [{-s | --stage} {ingress | egress}] [--set-policer]

Parameter

- <table_name>: The name of the ACL table type.
- <type>: One of the following:
    - L3 : Inspect IPv4 header
    - L3V6 : Inspect IPv6 header
    - MIRROR : Inspect IPv4 header for mirroring
    - MIRRORV6 : Inspect IPv6 header for mirroring
    - MIRROR_DSCP: Inspect DSCP for mirroring
    - <table-type> : Specifies a user-defined ACL table type.
- <description>: A description to remind users of the goal. The default is the ACL table name.
- <interfaces>: The interface(s) that are bound to this ACL.
    - The interface(s) can be Ethernet, PortChannel, or VLAN. You may use commas ',' to separate multiple interfaces in the list (for example, "Ethernet01, Ethernet02, PortChannel0001"), but VLANs cannot be mix-configured with Ethernet or PortChannel interfaces.
    - The default option is to apply the ACL to all front ports and PortChannels.
- <stage>: The stage this ACL table will be applied to, either ingress or egress. The default is "ingress". set-policer: Specifies to enable the capability for binding a policer for the ACL rules in this table.

When applying to the control plane, use the keyword CTRLPLANE and list the service protocols to be examined. You cannot use <interface> since it is a management frame and the destination is the CPU.

Usage for control plane
config acl add table <table_name> CTRLPLANE [{-d | --description} <description>] {-v | --services} <services_string>

Parameters:

- <table_name>, the ACL table to be applied to management frames.
- <description>, a description to remind users of the goal. The default is the ACL table name.
- <services_string>, a list of services to be matched, which are separated by commas. Valid values are:
    - "SNMP": SNMP protocol.
    - "NTP": NTP protocol.
    - "SSH": SSH protocol.

Some examples follow:

The ACL table "DATA_L3" is applied to interfaces "Ethernet0, Ethernet4" and inspects the IPv4 header in the ingress direction.

Example
admin@sonic:~$ sudo config acl add table DATA_L3 L3 --description "L3 table" --ports "Ethernet0,Ethernet4" -- stage "ingress"

The ACL table "DATA_L3V6" is applied to interfaces "PortChannel0001, PortChannel0002" and inspects the IPv6 header in the ingressndirection.

Example
admin@sonic:~$ sudo config acl add table DATA_L3V6 L3V6 --description "L3V6 table" --ports "PortChannel0001,PortChannel0002" --stage "ingress"

Note:

- The ACL table may not be provisioned **if** the chip is out of capacity, even when the ACL table exists in the configuration file. You would see "sonic ERR swss#orchagent: :- addAclTable: Failed to create ACL table" in syslog when an ACL table provisioning has failed.

The ACL table "DATA_CTRL" is applied to frames that are trapped to the CPU and whose services are SSH or SNMP.

Example
admin@sonic:~$ sudo config acl add table DATA_CTRL CTRLPLANE --description "CTRLPLANE table" --services "SSH,SNMP"

config acl remove table

This command is used to remove the binding of an ACL table on an interface. That is, the frames going through the interface are not inspected by the rule(s).

Usage
config acl remove table <table_name>

Parameters:

- <table_name>, the ACL table to be removed from binding.

Example
admin@sonic:~$ sudo config acl remove table DATA_L3 admin@sonic:~$ sudo config acl remove table DATA_L3V6

config acl add rule

This command is used to create an ACL rule.

Usage for data plane
config acl add rule <table-name> {permit | deny} [--priority <priority>] [--name <name>]

[--vlan-id <vlan-id] [--cos <cos>]

[--dscp <dscp>]

[--ip-protocol <ip-protocol>]

[--next-header <next-header>]

[--src-ip4 <src-ip>] [--dst-ip4 <dst-ip>]

[--src-ip6 <src-ip>] [--dst-ip6 <dst-ip>]

[--src-l4-port <src-l4-port>] [--dst-l4-port <dst-l4-port>]

[--src-l4-port-range <src-l4-port-range>] [--dst-l4-port-range <dst-l4-port-range>]

[--tcp-flags <tcp-flags>]

[--icmp-type <icmp-type>] [--icmp-code <icmp-code>]

[--icmpv6-type <icmp-type>] [--icmpv6-code <icmp-code>]

[--policer <policer-name>] [--set-dscp <set-dscp>] [--set-tc <set-tc>] [--set-cos <set-cos>]

[--mirror-ingress <mirror-session>]

Parameters:

- <table-name>: The name of the ACL table to add the rule to.
- <packet-action>: Specifies the action to take on packets that match the rule.
    - permit : Forward the packet. Default value.
    - deny : Drop the packet.
- priority: The priority of the rule. This is used to determine the order in which rules are evaluated. Higher numbers have
- higher priority. Minimum: "0". Maximum: "10000". If the value is not specified, a new priority is automatically assigned by adding a delta to the smallest priority such that the new priority is divisible by 10. For example, if the smallest priorityis 11, the value will be 10 (delta is 1).
- name: The name of the rule. If the name is not specified, the name is automatically assigned as priority of the rule. · vlan-id: The VLAN ID of the packet. This is used to match tagged packets. Minimum: "1". Maximum: "4094".
- cos: The VLAN PCP field of the packet. This is used to match tagged packets. Minimum: "0". Maximum: "7".

- dscp: The DSCP value of the packet. This is used to match IP packets. Minimum: "0". Maximum: "63".
- ip-protocol: The IP protocol of the packet. Minimum: "0". Maximum: "255".
- next-header: The IPv6 next header of the packet. Minimum: "0". Maximum: "255".
- src-ip4: The source IPv4 address of the packet.
- dst-ip4: The destination IPv4 address of the packet.
- src-ip6: The source IPv6 address of the packet.
- dst-ip6: The destination IPv6 address of the packet.
- src-l4-port: The source TCP or UDP port of the packet. Minimum: "0". Maximum: "65535".
- dst-l4-port: The destination TCP or UDP port of the packet. Minimum: "0". Maximum: "65535".
- src-l4-port-range: The source TCP or UDP port range of the packet. Format: "<min>-<max>". Minimum: "0". Maximum: "65535".
- dst-l4-port-range: The destination TCP or UDP port range of the packet. Format: "<min>-<max>". Minimum: "0". Maximum: "65535". · tcp-flags: The TCP flags of the packet, support comma-separated lists. The valid value is "fin", "syn", "rst", "psh", "ack",
- "urg", "ece" and "cwr".
- icmp-type: The ICMP type of the packet. Minimum: "0". Maximum: "255".
- icmp-code: The ICMP code of the packet. Minimum: "0". Maximum: "255".
- icmpv6-type: The ICMPv6 type of the packet. Minimum: "0". Maximum: "255".
- icmpv6-code: The ICMPv6 code of the packet. Minimum: "0". Maximum: "255".
- policer: The name of the policer to bind to this rule.
- set-cos: The new VLAN PCP value to set for packets that match this rule.
- set-dscp: The new DSCP value to set for packets that match this rule.
- set-tc: The new Traffic Class (TC) value to set for packets that match this rule.
- mirror-session: The mirror session name. This option is only supported for the ACL table type is MIRROR, MIRRORV6, and MIRROR_DSCP.

Notes:

- This command is not supported to add a rule for the CTRLPLANE ACL table type.
- The priority of actions is: drop (packet_action) > policer's actions > { set_dscp, set_tc, set_cos }. · If no match criteria are specified, all IP packets will be matched.
- If specified the set-cos action, it will override the value configured in TC2COS QoS map.
- If specified the set-dscp action, it will override the value configured in TC2DSCP QoS map.
- The AS9736-64D switch does not support specifying set-cos and policer for the egress stage.

The following example shows how to create a rule that uses to remark the DSCP from 0 to 7.

Example
sudo config acl add table-type L3_DSCP --match-dscp sudo config acl add table L3_DSCP_TABLE L3_DSCP --description "DiffServ table" --ports "Ethernet0,Ethernet4" --stage "ingress" sudo config acl add rule L3_DSCP_TABLE permit --priority 10000 --name DSCP 0 rule --dscp 0 --set-dscp 7

The following example shows how to create a rule that uses to drop the packets with DSCP of 63.

Example
sudo config acl add table-type L3_DSCP --match-dscp sudo config acl add table L3_DSCP_TABLE L3_DSCP --description "DiffServ table" --ports "Ethernet0,Ethernet4" --stage "ingress" sudo config acl add rule diffserv_table deny --priority 10 --dscp 63

config acl remove rule

This command is used to remove an ACL rule.

Usage
config acl remove rule <table_name> {--priority <priority> | --name <name>}

Parameters:

- <table_name>: The ACL table name.
- <priority>: The priority of the rule to delete.
- <name>: The name of the rule to delete.

The following examples show how to delete the rule with priority 10 in ACL table "L3_DSCP_TABLE".

```
sudo config acl remove rule L3_DSCP_TABLE --priority 10
```

config acl update full

This command is used to update the rules in all tables, or one specific table that already exists. That is, this command does not create an ACL table if it has not been created. You can use the show acl rule command to examine the updated ACL rules.

Usage
config acl update full [--table_name <table_name>] [--session_name <session_name>] <acl_configuration_file>

Parameters:

- <table_name>, the name of the ACL table to be loaded from the configuration file. Example: config acl update full "- - table_name DT_ACL_T1 /etc/sonic/acl_table_1.json"
- <session_name>, the mirror session to be loaded from the configuration file. Example: config acl update full "- -session_name mirror_ses1 /etc/sonic/acl_table_1.json"
    - this command fails if the <session_name> does not exist in the the configuration file when it is specified.
- <acl_configuration_file>, a json file that contains the ACL configurations. Refer to section ACL Rule Configuration File for details.

Note :

- The ACL rules may not be provisioned if the chip is out of capacity (even when the rules exist in the configuration file) or the value of some parameters are invalid. You would see "sonic ERR swss#orchagent: :- Failed to create ACL rule. Rule configuration is invalid" in syslog when an ACL rule provisioning has failed.
- Each ACL table contains a default rule that matches everything if none of the higher priority rules are matched. The default rule is used to deny any unmatched traffic.

The following examples show how to 1. replace all ACL tables, 2. replace the ACL table "DATA_L3" only, 3. replace the mirroring session "flow_local_l3" only.

Example
admin@sonic:~$ sudo config acl update full acl_rule_L3_scrip_dstip.json admin@sonic:~$ sudo config acl update full --table_name DATA_L3 acl_rule_L3_scrip_dstip.json admin@sonic:~$ sudo config acl update full --session_name flow_local_l3 acl_rule_L3_mirror_session.json

The configuration file "acl_rule_L3_scrip_dstip.json" has one rule in the "DATA_L3" table: forward (ACCEPT) the IPv4 packet whose destination IP address is "4.4.4.4" and source IP address is "3.3.3.3".

acl_rule_L3_scrip_dstip.json

```
{
        "acl":
        {
        "acl-sets":
        {
                "acl-set":
                {
                        "DATA_L3":
                        {
                        "acl-entries":
                        {
                                "acl-entry":
                                {
                                        "1":
                                        {
                                        "ip":
```

```
                        {
                            "config":
                            {
                                "destination-ip-address": "4.4.4.4/32",
                                "source-ip-address": "3.3.3.3/32"
                            }
                        },
                        "config":
                        {
                            "sequence-id": 1
                        },
                        "actions":
                        {
                            "config":
                            {
                                "forwarding-action": "ACCEPT"
                            }
                        }
                    }
                }
            }
        }
    }
}
```

```
  }
}
```

Note: This command removes all the rules in ACL tables and inserts the rules in the input file, i.e., it replaces the rule(s) with those in the configuration file.

The following example shows how to create a rule to match any packets and forward them.

Example
admin@sonic:~$ sudo config acl update full acl_rule_match_any_forward.json

The configuration file "acl_rule_match_any_forward.json" has one rule in the "DATA_L3" table: forward (ACCEPT) any packets.

acl_rule_match_any_forward.json
cat > acl_rule.json << EEE { "acl": { "acl-sets": { "acl-set": { "DATA_L3": {

```
                "acl-entries":
                {
                        "acl-entry":
                        {
                                "1":
                                {
                                "config":
                                {
                                        "sequence-id": 1
                                },
                                "actions":
                                {
                                        "config":
                                        {
                                                "forwarding-action": "ACCEPT"
                                        }
                                }
                                }
                        }
                }
                }
        }
    }
    }
```

```
}
```

config acl update incremental

Compared to config acl update full, this command performs incremental updates, which checks and modifies the corresponding rule(s), or updates the mirror session if <session name> is specified and configured.

Usage
config acl update incremental [--session_name <session_name>] <acl_json_file>

Parameters

- <session_name>, the mirror session to be loaded from the configuration file. Example: config acl update incremental "- - session_name mirror_ses1 /etc/sonic/acl_table_1.json"
- <acl_json_file>, a json file that contains the ACL configurations. Refer to section ACL Rule Configuration File for details.

Note :

- The ACL rules may not be provisioned if the chip is out of capacity (even when the rules exist in the configuration file) or the value of some parameters are invalid. You would see "sonic ERR swss#orchagent: :- Failed to create ACL rule. Rule configuration is invalid" in syslog when an ACL table provisioning has failed.
- Each ACL table contains a default rule that matches everything if none of the higher priority rules are matched. The default rule is used to deny any unmatched traffic.

Example
admin@sonic:~$ sudo config acl update incremental acl_rule_L3_scrip_dstip.json admin@sonic:~$ sudo config acl update incremental --session_name flow_local_l3 acl_rule_L3_mirror_session.json

counterpoll acl enable

Activate the flex counter to monitor the number and the size (in bytes) of packets that match the ACL rule.

Usage
counterpoll acl enable

Example
admin@sonic:~$ counterpoll acl enable

counterpoll acl disable

Deactivate the flex counter to monitor the number of packets and bytes that match the ACL rule. When the flex counter is disabled, the hardware counter will still increase if the packets match the ACL rule. Once the flex counter is activate again, it will obtainthe latest number of packets matched the ACL rule. To clear the counter, use the aclshow -c command.

Usage
counterpoll acl disable

Example
admin@sonic:~$ counterpoll acl disable

counterpoll acl interval

Set the polling interval of flex counter.

Usage
counterpoll acl interval <poll_interval>

Parameters

- <poll_interval>: the interval in milliseconds to poll the ACL rule matched count. Minimum: 1000. Maximum: 30000.

Configure the polling interval to 2 seconds.

Example
admin@sonic:~$ counterpoll acl interval 2000

8 ARP

config vlan arp_host_route

config vlan proxy_arp

ARP show commands

show arp

This command displays the ARP entries in the device with the following options.

1. Display the entire table.
2. Display the ARP entries learned on a specific interface.
3. Display the ARP of a specific IP address.

Usage
show arp [-if|--iface <interface_name>] [<ip_address>]

Details:

- show arp: Displays all entries.
- show arp -if <interface_name>: Displays the entries that are associated with the specified interface <interface_name>. show arp <ip_address>: Displays the entries that are associated with the specified address <ip_address>.

Example
admin@sonic:~$ show arp Address MacAddress Iface Vlan ---------- ----------------- ------- ------ 192.168.1.183 88:5a:92:fb:bf:41 Ethernet44 - 192.168.1.175 88:5a:92:fc:95:81 Ethernet28 - 192.168.1.181 e4:c7:22:c1:07:7c Ethernet40 - 192.168.1.179 88:5a:92:de:a8:bc Ethernet36 - 192.168.1.118 00:1c:73:3c:de:43 Ethernet64 -

```
192.168.1.11     00:1c:73:3c:e1:38     Ethernet88    -
192.168.1.161    24:e9:b3:71:3a:01     Ethernet0     -
192.168.1.189    24:e9:b3:9d:57:41     Ethernet56    -
192.168.1.187    74:26:ac:8b:8f:c1     Ethernet52    -
192.168.1.165    88:5a:92:de:a0:7c     Ethernet8     -
Total number of entries 10
```

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

Example

```
admin@sonic:~$ show arp -if Ethernet40
Address         MacAddress         Iface       Vlan
-------------   -----------------  ----------  ------
192.168.1.181   e4:c7:22:c1:07:7c  Ethernet40  -
Total number of entries 1
```

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

Example

```
admin@sonic:~$ show arp 192.168.1.181
Address         MacAddress         Iface       Vlan
192.168.1.181   e4:c7:22:c1:07:7c  Ethernet40  -
Total number of entries 1
```

ARP Config Command

config interface arp add/remove

Usage

```
config interface arp add <interface_name> <arp_address> <mac-address>
```

config interface arp remove <interface_name> <arp_address>

Parameter:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- <arp_address>, arp_address can be an IPv4 or IPv6 address（A.B.C.D/X:X::X:X）.
- <mac-address>, mac address as xx:xx:xx:xx:xx:xx.

Example
admin@sonic:~$ sudo config interface arp add Vlan10 10.10.10.10 a8:eb:d3:36:a5:82 admin@sonic:~$ sudo config interface arp remove Vlan10 10.10.10.10

Example
admin@sonic:~$ sudo config interface ip add Ethernet16 2016::6/64 admin@sonic:~$ sudo config interface arp add Ethernet16 2016::80 a8:eb:d3:36:80:80 admin@sonic:~$ sudo config interface arp remove Ethernet16 2016::80

config interface arp aging

Usage
config interface arp aging <interface_name> <interface_arp_aging>

Parameter:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- <interface_arp_aging>: The default ARP aging time is 1800s, and the configuration range is 300~86400

Note:

- If you have already learned ARP, configuring ARP aging time will not take effect immediately. You need to wait for ARP aging before the aging time configuration will take effect.
- Use **show interfaces arp** command, you can view ARP aging configuration information on the interface.

Example
admin@sonic:~$ sudo config interface arp aging Vlan10 10000

config interface arp gratuitous

Usage
config interface arp gratuitous enable config interface arp gratuitous remove

Note:

The default for free ARP is discard, and after enabling free ARP, the received free ARP packets can be added to the ARP cache.

Use **show interfaces arp** command, you can view ARP gratuitous configuration information on the interface.

Example
admin@sonic:~$ sudo config interface arp gratuitous enable Vlan10 admin@sonic:~$ sudo config interface arp gratuitous disable Vlan10

config vlan arp_host_route

Usage
config vlan arp_host_route < vid > { enabled | disable }

Note:

- ARP host routing is disabled by default and can only be configured on VLAN interfaces. ARP to host routing converts ARP to "K" type routing.
- Use **show interfaces arp** command, you can view ARP arp_host_route configuration information on the interface.

Usage
admin@sonic:~$ sudo config vlan proxy_arp 10 enabled admin@sonic:~$ sudo config vlan proxy_arp 10 disabled

config vlan proxy_arp

Usage
config vlan proxy_arp < vid > { enabled | disable }

Note:

ARP proxy is disabled by default and can only be configured on VLAN interfaces.

Use **show vlan brief** to show the configuration.

Usage
admin@sonic:~$ sudo config vlan proxy_arp 10 enabled admin@sonic:~$ sudo config vlan proxy_arp 10 disabled

9 BFD

Table of Contents

Bidirectional Forwarding Detection (BFD) uses the FRR vtysh shell CLI. The following commands are available in the FRR shell. Use the command vtysh to enter FRR mode.

Example
admin@sonic:~$ vtysh Hello, this is FRRouting (version 7.2.1-sonic). Copyright 1996-2005 Kunihiro Ishiguro, et al. sonic#

Refer to FRR BFDd Commands and FRR BGP Commands for more related FRR commands.

BFD Show Commands

This sub-section explains how to display BFD information.

show bfd peers

Shows all configured BFD peer information and the current status. Note: This command is executed within vtysh.

Usage

show bfd [vrf <vrf_name>] peers [json]

Example
sonic# show bfd peers BFD Peers: peer 192.169.3.33 vrf default ID: 1766365608 Remote ID: 455730325 Status: up Uptime: 9 second(s) Diagnostics: ok Remote diagnostics: ok Local timers: Receive interval: 300ms Transmission interval: 300ms Echo transmission interval: 50ms Remote timers: Receive interval: 300ms Transmission interval: 300ms Echo transmission interval: 50ms peer 192.169.1.11 vrf default ID: 1991080464 Remote ID: 3120344281 Status: up Uptime: 2 hour(s), 5 minute(s), 11 second(s) Diagnostics: ok Remote diagnostics: ok Local timers: Receive interval: 300ms Transmission interval: 300ms Echo transmission interval: 50ms Remote timers:

Receive interval: 300ms Transmission interval: 300ms Echo transmission interval: 50ms

Example (json)
sonic# show bfd peers json [{"multihop":false,"peer":"192.169.3.33","vrf":"default","id":1766365608,"remote-id":455730325,"status":"up","uptime":355,"diagnostic":"ok","remote-diagnostic":"ok","receive-interval":300,"transmit-interval":300,"echo-interval":0,"remote-receive-interval":300,"remote-transmit-interval":300,"remote-echo-interval":50},{"multihop":false,"peer":"192.169.1.11","vrf":"default","id":1991080464,"remote-id":3120344281,"status":"up","uptime":7857,"diagnostic":"ok","remote-diagnostic":"ok","receive-interval":300,"transmit-interval":300,"echo-interval":0,"remote-receive-interval":300,"remote-transmit-interval":300,"remote-echo-interval":50}]

show bfd peer

shows specified BFD peer information and the current status. Note: This command is executed within vtysh.

Usage
show bfd [vrf <vrf_name>] peer [ipv4_addr|peer_label|ipv6_addr]

Example
sonic# show bfd vrf default peer 192.169.1.11 BFD Peer: peer 192.169.1.11 vrf default ID: 1991080464 Remote ID: 3120344281 Status: up Uptime: 2 hour(s), 42 minute(s), 25 second(s) Diagnostics: ok Remote diagnostics: ok

```
    Local timers:
        Receive interval: 300ms
        Transmission interval: 300ms
        Echo transmission interval: 50ms
    Remote timers:
        Receive interval: 300ms
        Transmission interval: 300ms
        Echo transmission interval: 50ms
```

Example (json)

```
sonic# show bfd peer 192.169.1.11 json
{"multihop":false,"peer":"192.169.1.11","vrf":"default","id":1991080464,"remote-
id":3120344281,"status":"up","uptime":10273,"diagnostic":"ok","remote-diagnostic":"ok","receive-
interval":300,"transmit-interval":300,"echo-interval":0,"remote-receive-interval":300,"remote-transmit-
interval":300,"remote-echo-interval":50}
```

Please note that this command can be executed on the host interface, as shown in the following example executed outside of vtysh.

Example

```
admin@sonic:~$  show bfd peer 10.0.1.1
Total number of BFD sessions for peer IP 10.0.1.1: 1
Peer Addr    Interface   Vrf     State   Type        Local Addr    TX Interval   RX Interval   Multiplier  Multihop
-----------  ----------  ------- ------- ----------  ------------  ------------  ------------  ----------  ---------
10.0.1.1     default     default  DOWN    async_active  10.0.0.1          300           500           3  true
```

show bfd peer(s) counters

Shows BFD counters for a particular BFD session. Note: This command is executed within vtysh.

Usage

show bfd peer counters show bfd peers counters

Example (all peers)
sonic# show bfd peers counters BFD Peers: peer 192.169.3.33 vrf default Control packet input: 15996 packets Control packet output: 16008 packets Echo packet input: 0 packets Echo packet output: 0 packets Session up events: 1 Session down events: 0 Zebra notifications: 1 peer 192.169.1.11 vrf default Control packet input: 44536 packets Control packet output: 44542 packets Echo packet input: 0 packets Echo packet output: 0 packets Session up events: 1 Session down events: 0 Zebra notifications: 1

Example (specified peer)
sonic# show bfd peer 192.169.3.33 counters BFD Peers: peer 192.169.3.33 vrf default Control packet input: 15996 packets Control packet output: 16008 packets Echo packet input: 0 packets Echo packet output: 0 packets

Session up events: 1 Session down events: 0 Zebra notifications: 1

show peer summary

This command displays the state and key parameters of all BFD sessions.

Note: This command can be executed on the host interface, and the following example shows the result when executed outside of vtysh.

Usage
show bfd summary

Example
admin@sonic:~$ show bfd summary Total number of BFD sessions: 3 Peer Addr Interface Vrf State Type Local Addr TX Interval RX Interval Multiplier Multihop ---------- ---------- ------- ------- ---------- ---------- ---------- ---------- ---------- ---------- 10.0.1.1 default default DOWN async_active 10.0.0.1 300 500 3 true 10.0.2.1 Ethernet12 default UP async_active 10.0.0.1 200 600 3 false 2000::10:1 default default UP async_active 2000::1 100 700 3 false

BFD Peer Specific Commands

This sub-section explains how to configure a BFD peer and its settings.

All commands in this sub-section are entered in BFD mode. Use the bfd command to open the BFD daemon configuration mode.

Example
sonic# config sonic(config)# bfd sonic(config-bfd)#

peer

Creates and configures a new BFD peer to listen and talk to.

Usage
peer <ipv4_addr|ipv6_addr>

Example
sonic(config-bfd)# peer 192.169.1.11 sonic(config-bfd-peer)#

receive-interval

Configures the minimum interval that this system is capable of receiving control packets. The default value is 300 milliseconds.

Usage
receive-interval <value_in_ms>

Example
sonic(config-bfd)# peer 192.169.1.11 sonic(config-bfd-peer)# receive-interval 1000 sonic(config-bfd-peer)# end sonic# show bfd peer 192.169.1.11 BFD Peer: peer 192.169.1.11 vrf default ID: 1991080464 Remote ID: 3120344281 Status: up

```
    Uptime: 4 hour(s), 11 minute(s), 22 second(s)
    Diagnostics: ok
    Remote diagnostics: ok
    Local timers:
        Receive interval: 1000ms
        Transmission interval: 300ms
        Echo transmission interval: 50ms
    Remote timers:
        Receive interval: 300ms
        Transmission interval: 300ms
        Echo transmission interval: 50ms
```

transmit-interval

Configures the minimum transmission interval that this system wants to use to send BFD control packets. The default value is 300 milliseconds.

Usage
transmit-interval <value_in_ms>

Example
sonic(config-bfd)# peer 192.169.1.11 sonic(config-bfd-peer)# transmit-interval 1000 sonic(config-bfd-peer)# end sonic# show bfd peer 192.169.1.11 BFD Peer: peer 192.169.1.11 vrf default ID: 1991080464 Remote ID: 3120344281 Status: up Uptime: 4 hour(s), 13 minute(s), 36 second(s)

```
    Diagnostics: ok
    Remote diagnostics: ok
    Local timers:
        Receive interval: 1000ms
        Transmission interval: 1000ms
        Echo transmission interval: 50ms
    Remote timers:
        Receive interval: 300ms
        Transmission interval: 300ms
        Echo transmission interval: 50ms
```

echo-interval

Configures the minimum echo receive transmission interval. The default value is 50 milliseconds.

Usage
echo-interval <value_in_ms>

Example

```
sonic(config-bfd)# peer 192.169.1.11
sonic(config-bfd-peer)# echo-interval 100
sonic(config-bfd-peer)# end
sonic# show bfd peer 192.169.1.11
BFD Peer:
    peer 192.169.1.11 vrf default
    ID: 1991080464
    Remote ID: 3120344281
    Status: up
    Uptime: 4 hour(s), 29 minute(s), 12 second(s)
    Diagnostics: ok
    Remote diagnostics: ok
    Local timers:
```

```
        Receive interval: 1000ms
        Transmission interval: 1000ms
        Echo transmission interval: 100ms
    Remote timers:
        Receive interval: 300ms
        Transmission interval: 300ms
        Echo transmission interval: 50ms
```

echo-mode

Enables/disables the echo transmission mode. This mode is disabled by default.

It is recommended that the transmission interval of control packets to be increased after enabling echo-mode to reduce bandwidth usage. For example: transmit-interval 2000.

When using multi-hop mode, echo-mode will not work (see RFC 5883 section 3).

Usage
[no] echo-mode

Example
sonic(config-bfd)# peer 192.169.1.11 sonic(config-bfd-peer)# echo-mode sonic(config-bfd-peer)# no echo-mode

BGP BFD Commands

This sub-section explains how to configure or display BFD related settings on BGP neighbors.

The following commands are available in BGP configuration mode.

Usage
router bgp <as_id>

Example
sonic# config sonic(config)# router bgp 65101 sonic(config-router)#

bfd

Enables/disables BFD on BGP neighbors.

Usage
[no] neighbor <ipv4_addr|ipv6_addr|peer_label> bfd

Example
sonic(config-router)# neighbor 192.169.0.2 remote-as 65101 sonic(config-router)# neighbor 192.169.0.2 bfd

ebgp-multihop

Specifying ebgp-multihop allows sessions with eBGP neighbors to establish when they are multiple hops away.

Usage
[no] neighbor <ipv4_addr|neighbor_interface|ipv6_addr> ebgp-multihop

Example
sonic(config-router)# neighbor 192.169.0.2 ebgp-multihop

bfd info on bgp neighbors

When BGP neighbors use BFD to detect if the next hop router is alive, the BFD related information is shown in show bgp neighbors.

Usage
show bgp neighbors [ipv4_addr|neighbor_interface|ipv6_addr]

Example (single hop)
sonic# config sonic(config)# router bgp 65101 sonic(config-router)# neighbor 192.169.0.2 remote-as 65101 sonic(config-router)# neighbor 192.169.0.2 bfd sonic(config-router)# end sonic# show bgp neighbors BGP neighbor is 192.169.0.2, remote AS 65101, local AS 65101, internal link Hostname: sonic BGP version 4, remote router ID 192.169.0.2, local router ID 192.169.0.1 BGP state = Established, up for 00:01:18 Last read 00:00:18, Last write 00:00:18 Hold time is 180, keepalive interval is 60 seconds Neighbor capabilities: 4 Byte AS: advertised and received AddPath: IPv4 Unicast: RX advertised IPv4 Unicast and received Route refresh: advertised and received(old & new) Address Family IPv4 Unicast: advertised and received Hostname Capability: advertised (name: sonic,domain name: n/a) received (name: sonic,domain name: n/a) Graceful Restart Capabilty: advertised and received Remote Restart timer is 120 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:                 1 1
  Notifications:           0 0
  Updates:               1 1
  Keepalives:              2 2
  Route Refresh:           0 0
  Capability:            0 0
  Total:                 4 4
 Minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  Update group 1, subgroup 1
  Packet Queue length 0
  Community attribute sent to this neighbor(all)
  0 accepted prefixes

  Connections established 1; dropped 0
  Last reset 00:01:36, No AFI/SAFI activated for peer
Local host: 192.169.0.1, Local port: 179
Foreign host: 192.169.0.2, Foreign port: 53912
Nexthop: 192.169.0.1
Nexthop global: fe80::6f8:f8ff:fee5:c2ba
Nexthop local: fe80::6f8:f8ff:fee5:c2ba
BGP connection: shared network
BGP Connect Retry Timer in Seconds: 120
Read thread: on Write thread: on FD used: 27

 BFD: Type: single hop
   Detect Multiplier: 3, Min Rx interval: 300, Min Tx interval: 300
   Status: Up, Last update: 0:00:00:05
```

Example (multi hop)

```
sonic# config
sonic(config)# router bgp 65101
sonic(config-router)# neighbor 192.169.2.2 remote-as 65102
sonic(config-router)# neighbor 192.169.2.2 ebgp-multihop
sonic(config-router)# neighbor 192.169.2.2 bfd
sonic# show bgp neighbors
BGP neighbor is 192.169.2.2, remote AS 65102, local AS 65101, external link
Hostname: sonic
 BGP version 4, remote router ID 192.169.2.2, local router ID 192.169.1.1
 BGP state = Established, up for 00:00:02
 Last read 00:00:01, Last write 00:00:01
 Hold time is 180, keepalive interval is 60 seconds
 Neighbor capabilities:
  4 Byte AS: advertised and received
  AddPath:
   IPv4 Unicast: RX advertised IPv4 Unicast and received
  Route refresh: advertised and received(old & new)
  Address Family IPv4 Unicast: advertised and received
  Hostname Capability: advertised (name: sonic,domain name: n/a) received (name: sonic,domain name: n/a)
  Graceful Restart Capabilty: advertised and received
   Remote Restart timer is 120 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 2
  Notifications:      0 0
  Updates:            2 2
```

```
  Keepalives:          5 5
  Route Refresh:       0 0
  Capability:          0 0
  Total:               9 9
Minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast
  Update group 2, subgroup 2
  Packet Queue length 0
  Community attribute sent to this neighbor(all)
  0 accepted prefixes

  Connections established 2; dropped 1
  Last reset 00:01:59, Waiting for NHT
  External BGP neighbor may be up to 255 hops away.
Local host: 192.169.1.1, Local port: 51462
Foreign host: 192.169.2.2, Foreign port: 179
Nexthop: 192.169.1.1
Nexthop global: fe80::6f8:f8ff:fee5:c2ba
Nexthop local: fe80::6f8:f8ff:fee5:c2ba
BGP connection: non shared network
BGP Connect Retry Timer in Seconds: 120
Estimated round trip time: 877 ms
Read thread: on Write thread: on FD used: 27

BFD: Type: multi hop
  Detect Multiplier: 3, Min Rx interval: 300, Min Tx interval: 300
  Status: Up, Last update: 0:00:00:02
```

10 BGP

Table of Contents

This section explains all the BGP show commands and BGP configuration commands in both Quagga" and "FRR" routing software that are supported in SONiC. In 201811 and older versions "Quagga" was enabled by default. In current version "FRR" is enabled by default.

Most of the FRR show commands start with "show bgp" (201904 - 201911) or "show ip bgp" (after 202006). Similar commands in Quagga starts with "show ip bgp". All sub-options supported in all these show commands are common for FRR and Quagga. Detailed show command examples for Quagga are provided at the end of this document. This section covers only the commands supported by FRR.

BGP show commands

show bgp summary (FRR, SONiC versions 201904 - 201911)

This command displays the summary of all IPv4 and IPv6 BGP neighbors that are configured and the corresponding states.

(FRR, SONiC versions >= 201904 and <= 201911)

Usage (FRR, version after 201904 and before 201911)
show bgp summary

Example (FRR, bgp)

```
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
```

show ip bgp summary (Quagga, SONiC versions before 201811 or FRR, SONiC versions after 202006)

This command displays a summary of all IPv4 and IPv6 BGP neighbors that are configured and the corresponding states.

(Quagga, SONiC version <= 201811 or FRR, SONiC version >= 202006)

Usage (Quagga, version before 201811 or FRR, version after 202006)
show ip bgp summary

Example (Quagga/FRR after 202006, ip bgp)

```
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 12770
RIB entries 12807, using 2301 KiB of memory
Peers 4, using 82 KiB of memory
Peer groups 6, using 384 bytes of memory

Neighbor    V      AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd   NeighborName
10.0.0.57   4   64600    3346    4494      0   0    0 00:07:09        6400   ARISTA01T1
```

10.0.0.59	4	64600	3346	4494	0	0	0 00:07:09	6400	ARISTA02T1
10.0.0.61	4	64600	3348	4493	0	0	0 00:07:09	6400	ARISTA03T1
10.0.0.63	4	64600	3347	4493	0	0	0 00:07:09	6400	ARISTA04T1

Total number of neighbors 4

show bgp neighbors (FRR, SONiC version after 201904 and before 201911)

This command displays all the details of IPv4 and 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. The command has additional optional arguments to display only the advertised routes, or the received routes, or all routes. In order to see details for an IPv6 neighbor, use the **show bgp ipv6 neighbor <ipv6_address>** command.

Usage (FRR, after 201904 and before 201911)

```
show bgp neighbors [<ipv4-address> [advertised-routes | received-routes | routes]]
```

Example (FRR, after 201904 and before 201911)

```
admin@sonic:~$ show bgp neighbors
BGP neighbor is 10.0.0.57, remote AS 64600, local AS 65100, external link
Description: ARISTA01T1
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 Capabilty: 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.

Example (FRR, specific neighbor's information)

```
admin@sonic:~$ show bgp neighbors 10.0.0.57
BGP neighbor is 10.0.0.57, remote AS 64600, local AS 65100, external link
 Description: ARISTA01T1
 Member of peer-group PEER_V4 for session parameters
 BGP version 4, remote router ID 100.1.0.29, local router ID 10.1.0.32
 BGP state = Established, up for 00:04:24
Last read 00:00:00, Last write 00:00:01
 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: as7726-32x-1,domain name: n/a) not received
 Graceful Restart Capabilty: 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:             4228    3202
  Keepalives:            89      88
  Route Refresh:          0       0
  Capability:             0       0
  Total:               4321    3291
 Minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  PEER_V4 peer-group member
  Update group 1, subgroup 1
  Packet Queue length 0
  Inbound soft reconfiguration allowed
  Community attribute sent to this neighbor(all)
  Inbound path policy configured
  Outbound path policy configured
  Route map for incoming advertisements is *FROM_BGP_PEER_V4
  Route map for outgoing advertisements is *TO_BGP_PEER_V4
  6400 accepted prefixes

  Connections established 1; dropped 0
  Last reset 00:04:36, No AFI/SAFI activated for peer
Local host: 10.0.0.56, Local port: 179
Foreign host: 10.0.0.57, Foreign port: 57108
Nexthop: 10.0.0.56
Nexthop global: fc00::71
Nexthop local: fe80::82a2:35ff:fe46:999
BGP connection: shared network
BGP Connect Retry Timer in Seconds: 120
Read thread: on Write thread: on FD used: 32
```

```
admin@sonic:~$ show bgp neighbors 10.0.0.57 advertised-routes
BGP table version is 11920, local router ID is 10.1.0.32, vrf id 0
Default local pref 100, local AS 65100
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop      Metric LocPrf Weight Path
*> 0.0.0.0/0        10.0.0.59                0 64600 65534 6666 6667 i
*> 10.1.0.32/32     0.0.0.0          0       32768 i
*> 100.1.0.29/32    10.0.0.57                0 64600 i
*> 100.1.0.30/32    10.0.0.59                0 64600 i
                                    ...
*> 193.11.248.0/25  10.0.0.61                0 64600 65534 64799 65515 i
*> 193.11.248.128/25
                    10.0.0.61                0 64600 65534 64799 65515 i

Total number of prefixes 6405

admin@sonic:~$ show bgp neighbors 10.0.0.57 received-routes
BGP table version is 0, local router ID is 10.1.0.32, vrf id 0
Default local pref 100, local AS 65100
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop Metric LocPrf Weight Path
*> 0.0.0.0/0        10.0.0.57                0 64600 65534 6666 6667 i
*> 100.1.0.29/32    10.0.0.57                0 64600 i
*> 192.168.8.0/25   10.0.0.57                0 64600 65501 i
*> 192.168.8.128/25 10.0.0.57                0 64600 65501 i
*> 192.168.16.0/25  10.0.0.57                0 64600 65502 i
```

```
                                    ...
*> 193.11.248.0/25    10.0.0.57                0 64600 65534 64799 65515 i
*> 193.11.248.128/25
                    10.0.0.57                0 64600 65534 64799 65515 I

Total number of prefixes 6400
admin@sonic:~$ show bgp neighbors 10.0.0.57 routes
BGP table version is 11920, local router ID is 10.1.0.32, vrf id 0
Default local pref 100, local AS 65100
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*= 0.0.0.0/0         10.0.0.57                0 64600 65534 6666 6667 i
*> 100.1.0.29/32     10.0.0.57                0 64600 i
*= 192.168.8.0/25    10.0.0.57                0 64600 65501 i
*= 192.168.8.128/25  10.0.0.57                0 64600 65501 i
*= 192.168.16.0/25   10.0.0.57                0 64600 65502 i
*= 192.168.16.128/25
                    10.0.0.57                0 64600 65502 i
                                    ...
*= 193.11.240.0/25    10.0.0.57                0 64600 65534 64799 65514 i
*= 193.11.240.128/25
                    10.0.0.57                0 64600 65534 64799 65514 i
*= 193.11.248.0/25    10.0.0.57                0 64600 65534 64799 65515 i
*= 193.11.248.128/25
                    10.0.0.57                0 64600 65534 64799 65515 i
Displayed 6400 routes and 25602 total paths
```

show ip bgp neighbors (Quagga, SONiC version before 201811 or FRR, SONiC version after 202006)

This command displays all the details of IPv4 and 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. The command has additional optional arguments to display only the advertised routes, or the received routes, or all routes. In order to see details for an IPv6 neighbor, use the **show bgp ipv6 neighbor <ipv6_address>** command.

Usage (Quagga, before 201811 or FRR, after 202006)
show ip bgp neighbors [[advertised-routes | received-routes | routes]]

For an example of show ip bgp neighbors, you can refer to show bgp neighbors with the same options.

show ip bgp network

This command displays all the details of IPv4 Border Gateway Protocol (BGP) prefixes.

Usage
show ip bgp network [[<ipv4-address>|<ipv4-prefix>] [(bestpath | multipath | longer-prefixes | json)]]

Example
admin@sonic:~$ show ip bgp network BGP table version is 10839, local router ID is 10.1.0.32, vrf id 0 Default local pref 100, local AS 65100 Status codes: s suppressed, d damped, h history, * valid, > best, = multipath, i internal, r RIB-failure, S Stale, R Removed Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path *= 0.0.0.0/0 10.0.0.63 0 64600 65534 6666 6667 i *= 10.0.0.61 0 64600 65534 6666 6667 i *> 10.0.0.57 0 64600 65534 6666 6667 i *= 10.0.0.59 0 64600 65534 6666 6667 i

```
                                    ...
*= 193.11.248.128/25
                10.0.0.63 0 64600 65534 64799 65515 i
*=              10.0.0.61 0 64600 65534 64799 65515 i
*=              10.0.0.59 0 64600 65534 64799 65515 i
*>              10.0.0.57 0 64600 65534 64799 65515 i
Displayed 6405 routes and 25602 total paths
admin@sonic:~$ show ip bgp network 192.168.8.130 bestpath
BGP routing table entry for 192.168.8.128/25
Paths: (4 available, best #3, table default)
 Advertised to non peer-group peers:
 10.0.0.57 10.0.0.59 10.0.0.61 10.0.0.63
 64600 65501
   10.0.0.57 from 10.0.0.57 (100.1.0.29)
     Origin IGP, valid, external, multipath, best (Router ID)
     Last update: Tue Nov 24 07:23:34 2020

admin@sonic:~$ show ip bgp network 192.168.8.130 multipath
BGP routing table entry for 192.168.8.128/25
Paths: (4 available, best #3, table default)
 Advertised to non peer-group peers:
 10.0.0.57 10.0.0.59 10.0.0.61 10.0.0.63
 64600 65501
   10.0.0.63 from 10.0.0.63 (100.1.0.32)
     Origin IGP, valid, external, multipath
     Last update: Tue Nov 24 07:23:34 2020

 64600 65501
   10.0.0.61 from 10.0.0.61 (100.1.0.31)
     Origin IGP, valid, external, multipath
     Last update: Tue Nov 24 07:23:34 2020

 64600 65501
   10.0.0.57 from 10.0.0.57 (100.1.0.29)
```

```
    Origin IGP, valid, external, multipath, best (Router ID)
    Last update: Tue Nov 24 07:23:34 2020

 64600 65501
  10.0.0.59 from 10.0.0.59 (100.1.0.30)
    Origin IGP, valid, external, multipath
    Last update: Tue Nov 24 07:23:34 2020

admin@sonic:~$ show ip bgp network 10.1.0.32 json
{
 "prefix":"10.1.0.32\/32",
 "advertisedTo":{
  "10.0.0.57":{
  },
  "10.0.0.59":{
  },
  "10.0.0.61":{
  },
  "10.0.0.63":{
  }
 },
 "paths":[
  {
   "aspath":{
    "string":"Local",
    "segments":[
    ],
    "length":0
   },
   "origin":"IGP",
   "med":0,
   "metric":0,
   "weight":32768,
   "valid":true,
```

```
    "sourced":true,
    "local":true,
    "bestpath":{
      "overall":true,
      "selectionReason":"First path received"
    },
    "lastUpdate":{
      "epoch":1606202576,
       "string":"Tue Nov 24 07:22:56 2020\n"
    },
    "nexthops":[
      {
        "ip":"0.0.0.0",
        "afi":"ipv4",
        "metric":0,
        "accessible":true,
       "used":true
      }
   ],
   "peer":{
     "peerId":"0.0.0.0",
     "routerId":"10.1.0.32"
    }
   }
 ]
}
admin@sonic:~$ show ip bgp network 10.1.0.32/32 bestpath
BGP routing table entry for 10.1.0.32/32
Paths: (1 available, best #1, table default)
 Advertised to non peer-group peers:
 10.0.0.57 10.0.0.59 10.0.0.61 10.0.0.63
 Local
   0.0.0.0 from 0.0.0.0 (10.1.0.32)
     Origin IGP, metric 0, weight 32768, valid, sourced, local, best (First path received)
```

```
    Last update: Tue Nov 24 07:22:56 2020

admin@sonic:~$ show ip bgp network 10.1.0.32/32 multipath
BGP routing table entry for 10.1.0.32/32
Paths: (1 available, best #1, table default)
 Advertised to non peer-group peers:
 10.0.0.57 10.0.0.59 10.0.0.61 10.0.0.63
 Local
 0.0.0.0 from 0.0.0.0 (10.1.0.32)
 Origin IGP, metric 0, weight 32768, valid, sourced, local, best (First path received)
 Last update: Tue Nov 24 07:22:56 2020
admin@sonic:~$ show ip bgp network 10.1.0.32/32 json
{
  "prefix":"10.1.0.32\/32",
  "advertisedTo":{
    "10.0.0.57":{
    },
    "10.0.0.59":{
    },
    "10.0.0.61":{
    },
    "10.0.0.63":{
    }
  },
  "paths":[
    {
      "aspath":{
        "string":"Local",
        "segments":[
        ],
        "length":0
      },
      "origin":"IGP",
      "med":0,
```

```
    "metric":0,
    "weight":32768,
    "valid":true,
    "sourced":true,
    "local":true,
    "bestpath":{
      "overall":true,
      "selectionReason":"First path received"
    },
   "lastUpdate":{
     "epoch":1606202576,
     "string":"Tue Nov 24 07:22:56 2020\n"
   },
   "nexthops":[
     {
       "ip":"0.0.0.0",
       "afi":"ipv4",
       "metric":0,
       "accessible":true,
      "used":true
     }
  ],
   "peer":{
     "peerId":"0.0.0.0",
     "routerId":"10.1.0.32"
   }
  }
 ]
}
admin@sonic:~$ show ip bgp network 10.1.0.32/32 longer-prefixes
BGP table version is 10839, local router ID is 10.1.0.32, vrf id 0
Default local pref 100, local AS 65100
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
```

```
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete

 Network          Next Hop Metric LocPrf Weight Path
*> 10.1.0.32/32    0.0.0.0      0        32768 i

Displayed 1 routes and 25602 total paths
```

Note: The **longer-prefixes** option is only available when a network prefix with a "/" notation is used

show bgp ipv6 summary (FRR, SONiC versions after 201904 and before 201911)

This command displays the summary of all IPv6 BGP neighbors that are configured and the corresponding states.

Usage (FRR, after 201904 and before 201911)

```
show bgp ipv6 summary
```

Example (FRR, after 201904 and before 201911)

```
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
```

show ipv6 bgp summary (Quagga, SONiC versions before 201811 or FRR, SONiC versions after 202006)

This command displays the summary of all IPv6 BGP neighbors that are configured and the corresponding states.

Usage (Quagga, before 201811 or FRR, after 202006)
show ipv6 bgp summary

Example (Quagga, before 201811 or FRR, after 202006)

```
admin@sonic:~$ show ipv6 bgp summary

IPv6 Unicast Summary:
BGP router identifier 10.1.0.32, local AS number 65100 vrf-id 0
BGP table version 11661
RIB entries 12807, using 2301 KiB of memory
Peers 4, using 82 KiB of memory
Peer groups 6, using 384 bytes of memory

Neighbor   V     AS MsgRcvd MsgSent TblVer  InQ OutQ Up/Down State/PfxRcd NeighborName
fc00::72   4  64600    4341    6224       0    0    0 00:56:55        6400 ARISTA01T1
fc00::76   4  64600    4341    6224       0    0    0 00:56:55        6400 ARISTA02T1
fc00::7a   4  64600    4340    6224       0    0    0 00:56:55        6400 ARISTA03T1
fc00::7e   4  64600    4339    6224       0    0    0 00:56:55        6400 ARISTA04T1

Total number of neighbors 4
```

show bgp ipv6 neighbors (FRR, SONiC versions after 201904 and before 201911)

This command displays all the details of one particular IPv6 Border Gateway Protocol (BGP) neighbor. An option is also available to display only the advertised routes, or the received routes, or all routes.

Usage (FRR, after 201904 and before 201911)
show bgp ipv6 neighbors [<ipv6-address> [(advertised-routes | received-routes | routes)]]

Example (FRR, after 201904 and before 201911)

```
admin@sonic:~$ show bgp ipv6 neighbors
BGP neighbor is fc00::72, remote AS 64600, local AS 65100, external link
 Description: ARISTA01T1
 Member of peer-group PEER_V6 for session parameters
  BGP version 4, remote router ID 100.1.0.29, local router ID 10.1.0.32
  BGP state = Established, up for 01:18:47
   Last read 00:00:02, Last write 00:00:02
  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:
    IPv6 Unicast: RX advertised IPv6 Unicast and received
   Route refresh: advertised and received(new)
   Address Family IPv6 Unicast: advertised and received
   Hostname Capability: advertised (name: as5812-54x,domain name: n/a) not received
   Graceful Restart Capabilty: advertised and received
    Remote Restart timer is 300 seconds
    Address families by peer:
     none
 Graceful restart information:
  End-of-RIB send: IPv6 Unicast
  End-of-RIB received: IPv6 Unicast
 Message statistics:
  Inq depth is 0
  Outq depth is 0
                  Sent    Rcvd
   Opens:              2       1
  Notifications:       2       0
```

```
  Updates:            5081    3202
  Keepalives:         1576    1575
  Route Refresh:         0       0
  Capability:            0       0
  Total:              6661    4778
Minimum time between advertisement runs is 0 seconds

For address family: IPv6 Unicast
  PEER_V6 peer-group member
  Update group 2, subgroup 2
  Packet Queue length 0
  Inbound soft reconfiguration allowed
  Community attribute sent to this neighbor(all)
  Inbound path policy configured
  Outbound path policy configured
  Route map for incoming advertisements is *FROM_BGP_PEER_V6
  Route map for outgoing advertisements is *TO_BGP_PEER_V6
  6400 accepted prefixes

  Connections established 1; dropped 0
  Last reset 01:19:13, No AFI/SAFI activated for peer
Local host: fc00::71, Local port: 179
Foreign host: fc00::72, Foreign port: 43581
Nexthop: 10.0.0.56
Nexthop global: fc00::71
Nexthop local: fe80::3e2c:99ff:fe15:aa60
BGP connection: shared network
BGP Connect Retry Timer in Seconds: 120
Read thread: on Write thread: on FD used: 22
...

admin@sonic:~$ show bgp ipv6 neighbors fc00::72
BGP neighbor is fc00::72, remote AS 64600, local AS 65100, external link
 Description: ARISTA01T1
```

```
Member of peer-group PEER_V6 for session parameters
 BGP version 4, remote router ID 100.1.0.29, local router ID 10.1.0.32
 BGP state = Established, up for 01:18:47
 Last read 00:00:02, Last write 00:00:02
 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:
   IPv6 Unicast: RX advertised IPv6 Unicast and received
  Route refresh: advertised and received(new)
  Address Family IPv6 Unicast: advertised and received
  Hostname Capability: advertised (name: as5812-54x,domain name: n/a) not received
  Graceful Restart Capabilty: advertised and received
   Remote Restart timer is 300 seconds
   Address families by peer:
    none
Graceful restart information:
  End-of-RIB send: IPv6 Unicast
  End-of-RIB received: IPv6 Unicast
Message statistics:
  Inq depth is 0
  Outq depth is 0
                    Sent    Rcvd
  Opens:               2       1
  Notifications:       2       0
  Updates:          5081    3202
  Keepalives:       1576    1575
  Route Refresh:       0       0
  Capability:          0       0
Total:              6661    4778
 Minimum time between advertisement runs is 0 seconds

 For address family: IPv6 Unicast
```

```
  PEER_V6 peer-group member
  Update group 2, subgroup 2
  Packet Queue length 0
  Inbound soft reconfiguration allowed
  Community attribute sent to this neighbor(all)
  Inbound path policy configured
  Outbound path policy configured
  Route map for incoming advertisements is *FROM_BGP_PEER_V6
  Route map for outgoing advertisements is *TO_BGP_PEER_V6
  6400 accepted prefixes

  Connections established 1; dropped 0
  Last reset 01:19:13, No AFI/SAFI activated for peer
Local host: fc00::71, Local port: 179
Foreign host: fc00::72, Foreign port: 43581
Nexthop: 10.0.0.56
Nexthop global: fc00::71
Nexthop local: fe80::3e2c:99ff:fe15:aa60
BGP connection: shared network
BGP Connect Retry Timer in Seconds: 120
Read thread: on Write thread: on FD used: 22

admin@sonic:~$ show bgp ipv6 neighbors fc00::72 advertised-routes
BGP table version is 11661, local router ID is 10.1.0.32, vrf id 0
Default local pref 100, local AS 65100
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> ::/0             fc00::72                 0 64600 65534 6666 6667 i
*> 2064:100::1d/128 fc00::72                 0 64600 i
*> 2064:100::1e/128 fc00::76                 0 64600 i
```

```
*> 2064:100::1f/128 fc00::7a                0 64600 i
*> 2064:100::20/128 fc00::7e                0 64600 i
                                          ...
*> 20c1:bf8::/64    fc00::72                0 64600 65534 64799 65515 i
*> 20c1:bf8:0:80::/64
                    fc00::72                0 64600 65534 64799 65515 i
*> fc00:1::/64      ::                      0 32768 i
*> fc02:1000::/64   ::                      0 32768 i

Total number of prefixes 6405

admin@sonic:~$ show bgp ipv6 neighbors fc00::72 received-routes
BGP table version is 0, local router ID is 10.1.0.32, vrf id 0
Default local pref 100, local AS 65100
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop Metric LocPrf Weight Path
*> ::/0           fc00::72                0 64600 65534 6666 6667 i
*> 2064:100::1d/128 fc00::72               0 64600 i
*> 20c0:a808::/64   fc00::72               0 64600 65501 i
*> 20c0:a808:0:80::/64
                    fc00::72               0 64600 65501 i
                                          ...
*> 20c1:bf8::/64    fc00::72               0 64600 65534 64799 65515 i
*> 20c1:bf8:0:80::/64
                    fc00::72               0 64600 65534 64799 65515 i


Total number of prefixes 6400

admin@sonic:~$ show bgp ipv6 neighbors fc00::72 routes
```

```
BGP table version is 11661, local router ID is 10.1.0.32, vrf id 0
Default local pref 100, local AS 65100
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> ::/0             fc00::72                 0 64600 65534 6666 6667 i
*> 2064:100::1d/128 fc00::72                 0 64600 i
*> 20c0:a808::/64   fc00::72                 0 64600 65501 i
*> 20c0:a808:0:80::/64
                    fc00::72                 0 64600 65501 i
                                                ...
*> 20c1:bf8::/64    fc00::72                 0 64600 65534 64799 65515 i
*> 20c1:bf8:0:80::/64
                    fc00::72                 0 64600 65534 64799 65515 i

Displayed 6400 routes and 25602 total paths
```

show ipv6 bgp neighbors (Quagga, SONiC versions before 201811 or FRR, SONiC versions after 202006)

This command displays all the details of one particular IPv6 Border Gateway Protocol (BGP) neighbor. An option is also available to display only the advertised routes, or the received routes, or all routes.

Usage (Quagga, before 201811 or FRR, after 202006)
show ipv6 bgp neighbors [<ipv6-address> [(advertised-routes | received-routes | routes)]]

For an example of show ipv6 bgp neighbors, you can refer to show bgp ipv6 neighbors with the same options.

show ipv6 bgp network

This command displays all the details of IPv6 Border Gateway Protocol (BGP) prefixes.

Usage (Quagga or FRR after 202006)

```
show ipv6 bgp network [[<ipv6-address>|<ipv6-prefix>] [(bestpath | multipath | longer-prefixes | json)]]
```

Example (Quagga or FRR after 202006)

```
admin@sonic:~$ show ipv6 bgp network
BGP table version is 11661, local router ID is 10.1.0.32, vrf id 0
Default local pref 100, local AS 65100
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
                i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*= ::/0             fc00::7a                 0 64600 65534 6666 6667 i
*=                  fc00::7e                 0 64600 65534 6666 6667 i
*>                  fc00::72                 0 64600 65534 6666 6667 i
*=                  fc00::76                 0 64600 65534 6666 6667 i
*> 2064:100::1d/128 fc00::72                 0 64600 i
*> 2064:100::1e/128 fc00::76                 0 64600 i
*> 2064:100::1f/128 fc00::7a                 0 64600 i
                                            ...
*= 20c1:bf8:0:80::/64
                    fc00::7e                 0 64600 65534 64799 65515 i
*=                  fc00::7a                 0 64600 65534 64799 65515 i
*=                  fc00::76                 0 64600 65534 64799 65515 i
*>                  fc00::72                 0 64600 65534 64799 65515 i
*> fc00:1::/64      ::             0         32768 i
*> fc02:1000::/64   ::             0         32768 i

Displayed 6405 routes and 25602 total paths
```

```
admin@sonic:~$ show ipv6 bgp network 2064:100::1d bestpath
BGP routing table entry for 2064:100::1d/128
Paths: (1 available, best #1, table default)
  Advertised to non peer-group peers:
  fc00::72 fc00::76 fc00::7a fc00::7e
  64600
    fc00::72 from fc00::72 (100.1.0.29)
    (fe80::5054:ff:fe02:b909) (prefer-global)
      Origin IGP, valid, external, best (First path received)
      Last update: Tue Nov 24 08:56:51 2020

admin@sonic:~$ show ipv6 bgp network 20c0:a810::/64 multipath
BGP routing table entry for 20c0:a810::/64
Paths: (4 available, best #4, table default)
  Advertised to non peer-group peers:
  fc00::72 fc00::76 fc00::7a fc00::7e
  64600 65502
    fc00::76 from fc00::76 (100.1.0.30)
    (fe80::5054:ff:fe25:758e) (prefer-global)
      Origin IGP, valid, external, multipath
      Last update: Tue Nov 24 08:56:51 2020

  64600 65502
    fc00::7e from fc00::7e (100.1.0.32)
    (fe80::5054:ff:fe51:5f51) (prefer-global)
      Origin IGP, valid, external, multipath
      Last update: Tue Nov 24 08:56:51 2020

  64600 65502
    fc00::72 from fc00::72 (100.1.0.29)
    (fe80::5054:ff:fe02:b909) (prefer-global)
       Origin IGP, valid, external, multipath
      Last update: Tue Nov 24 08:56:51 2020
```

```
 64600 65502
   fc00::7a from fc00::7a (100.1.0.31)
   (fe80::5054:ff:fef2:88ce) (prefer-global)
     Origin IGP, valid, external, multipath, best (Older Path)
     Last update: Tue Nov 24 08:56:51 2020

admin@sonic:~$ show ipv6 bgp network 2064:100::1d json
{
  "prefix":"2064:100::1d\/128",
  "advertisedTo":{
    "fc00::72":{
    },
    "fc00::76":{
    },
    "fc00::7a":{
    },
    "fc00::7e":{
    }
  },
  "paths":[
   {
     "aspath":{
       "string":"64600",
        "segments":[
          {
            "type":"as-sequence",
            "list":[
              64600
            ]
          }
        ],
       "length":1
     },
```

```
    "origin":"IGP",
    "valid":true,
    "bestpath":{
      "overall":true,
      "selectionReason":"First path received"
    },
    "lastUpdate":{
      "epoch":1606208211,
      "string":"Tue Nov 24 08:56:51 2020\n"
    },
    "nexthops":[
      {
        "ip":"fc00::72",
        "afi":"ipv6",
        "scope":"global",
        "metric":0,
       "accessible":true,
       "used":true
      },
      {
        "ip":"fe80::5054:ff:fe02:b909",
        "afi":"ipv6",
        "scope":"link-local",
        "accessible":true
      }
    ],
    "peer":{
      "peerId":"fc00::72",
      "routerId":"100.1.0.29",
      "type":"external"
    }
  }
 ]
}
```

```
admin@sonic:~$ show ipv6 bgp network 2064:100::1d/128 bestpath
BGP routing table entry for 2064:100::1d/128
Paths: (1 available, best #1, table default)
  Advertised to non peer-group peers:
  fc00::72 fc00::76 fc00::7a fc00::7e
  64600
    fc00::72 from fc00::72 (100.1.0.29)
    (fe80::5054:ff:fe02:b909) (prefer-global)
    Origin IGP, valid, external, best (First path received)
    Last update: Tue Nov 24 08:56:51 2020

admin@sonic:~$ show ipv6 bgp network 20c0:a810::/64 multipath
BGP routing table entry for 20c0:a810::/64
Paths: (4 available, best #4, table default)
  Advertised to non peer-group peers:
  fc00::72 fc00::76 fc00::7a fc00::7e
  64600 65502
    fc00::76 from fc00::76 (100.1.0.30)
    (fe80::5054:ff:fe25:758e) (prefer-global)
      Origin IGP, valid, external, multipath
      Last update: Tue Nov 24 08:56:51 2020

  64600 65502
    fc00::7e from fc00::7e (100.1.0.32)
   (fe80::5054:ff:fe51:5f51) (prefer-global)
     Origin IGP, valid, external, multipath
     Last update: Tue Nov 24 08:56:51 2020

  64600 65502
    fc00::72 from fc00::72 (100.1.0.29)
    (fe80::5054:ff:fe02:b909) (prefer-global)
      Origin IGP, valid, external, multipath
      Last update: Tue Nov 24 08:56:51 2020
```

```
 64600 65502
   fc00::7a from fc00::7a (100.1.0.31)
   (fe80::5054:ff:fef2:88ce) (prefer-global)
     Origin IGP, valid, external, multipath, best (Older Path)
     Last update: Tue Nov 24 08:56:51 2020

admin@sonic:~$ show ipv6 bgp network 2064:100::1d/128 json
{
 "prefix":"2064:100::1d\/128",
 "advertisedTo":{
   "fc00::72":{
   },
   "fc00::76":{
   },
   "fc00::7a":{
   },
   "fc00::7e":{
   }
 },
 "paths":[
   {
     "aspath":{
     "string":"64600",
     "segments":[
       {
        "type":"as-sequence",
        "list":[
          64600
        ]
       }
     ],
     "length":1
     },
```

```
    "origin":"IGP",
    "valid":true,
    "bestpath":{
      "overall":true,
      "selectionReason":"First path received"
    },
    "lastUpdate":{
      "epoch":1606208211,
      "string":"Tue Nov 24 08:56:51 2020\n"
    },
    "nexthops":[
      {
        "ip":"fc00::72",
        "afi":"ipv6",
        "scope":"global",
        "metric":0,
        "accessible":true,
        "used":true
      },
      {
        "ip":"fe80::5054:ff:fe02:b909",
        "afi":"ipv6",
        "scope":"link-local",
        "accessible":true
      }
    ],
    "peer":{
      "peerId":"fc00::72",
      "routerId":"100.1.0.29",
      "type":"external"
    }
  }
 ]
}
```

```
admin@sonic:~$ show ipv6 bgp network 2064:100::1d/128 longer-prefixes
BGP table version is 12770, local router ID is 10.1.0.32, vrf id 0
Default local pref 100, local AS 65100
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop Metric LocPrf Weight Path
*> 2064:100::1d/128 fc00::72                0 64600 i

Displayed 1 routes and 25602 total paths
```

Note: The **longer-prefixes** option is only available when a network prefix with a "/" notation is used.

show route-map

This command displays the routing policy that takes precedence over the other route processes that are configured.

Usage
show route-map

Example
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
```

BGP config commands

This sub-section explains the list of configuration options available for the BGP module, both for IPv4 and IPv6 BGP neighbors.

config bgp shutdown all

This command is used to shutdown all the BGP IPv4 and IPv6 sessions. When a session is shutdown using this command, the BGP state in **show ip bgp summary** is displayed as "Idle (Admin)"

Usage
config bgp shutdown all

Example

```
admin@sonic:~$ sudo config bgp shutdown all
Shutting down BGP session with neighbor 10.0.0.57...
Shutting down BGP session with neighbor 10.0.0.59...
Shutting down BGP session with neighbor 10.0.0.61...
Shutting down BGP session with neighbor 10.0.0.63...
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 21863
RIB entries 3, using 552 bytes of memory
Peers 4, using 82 KiB of memory
Peer groups 6, using 384 bytes of memory

Neighbor    V      AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd NeighborName
10.0.0.57   4   64600    4437    5982      0   0    0 00:06:02 Idle (Admin) ARISTA01T1
10.0.0.59   4   64600    4434    4682      0   0    0 00:06:11 Idle (Admin) ARISTA02T1
10.0.0.61   4   64600    4433    4649      0   0    0 00:06:14 Idle (Admin) ARISTA03T1
10.0.0.63   4   64600    4431    4603      0   0    0 00:06:16 Idle (Admin) ARISTA04T1
```

Total number of neighbors 4

config bgp shutdown neighbor

This command shuts down a BGP session with a neighbor by specifying the IP address or hostname.

Usage
sudo config bgp shutdown neighbor (<ip_address> | <hostname>)

Example
admin@sonic:~$ sudo config bgp shutdown neighbor 10.0.0.57 Shutting down BGP session with neighbor 10.0.0.57... admin@sonic:~$ sudo config bgp shutdown neighbor ARISTA01T1 Shutting down BGP session with neighbor 10.0.0.57... Shutting down BGP session with neighbor fc00::72...

config bgp startup all

This command starts up all the IPv4 and IPv6 BGP neighbors

Usage
config bgp startup all

Example
admin@sonic:~$ sudo config bgp startup all Starting up BGP session with neighbor 10.0.0.57... Starting up BGP session with neighbor 10.0.0.59... Starting up BGP session with neighbor 10.0.0.61... Starting up BGP session with neighbor 10.0.0.63...

config bgp startup neighbor

This command starts up a particular IPv4 or IPv6 BGP neighbor using either the IP address or hostname.

Usage
config bgp startup neighbor (<ip-address> | <hostname>)

Example
admin@sonic:~$ sudo config bgp startup neighbor 10.0.0.57 Starting up BGP session with neighbor 10.0.0.57... admin@sonic:~$ sudo config bgp startup neighbor ARISTA01T1 Starting up BGP session with neighbor 10.0.0.57... Starting up BGP session with neighbor fc00::72...

config bgp remove neighbor

This command removes a particular IPv4 or IPv6 BGP neighbor configuration using either the IP address or hostname.

Usage
config bgp remove neighbor <neighbor_ip_or_hostname>

Example
admin@sonic:~$ sudo config bgp remove neighbor 10.0.0.57 Removed configuration of BGP neighbor 10.0.0.57 admin@sonic:~$ sudo config bgp remove neighbor fc00::72 Removed configuration of BGP neighbor fc00::72 admin@sonic:~$ sudo config bgp remove neighbor ARISTA01T1 Removed configuration of BGP neighbor 10.0.0.57 Removed configuration of BGP neighbor fc00::72

Note:

- These SONiC bgp commands (**shutdown/startup/remove**) will only apply to the neighbor entries included in config_db.json (redis db). Otherwise, it will show error message about it could not locate the neighbor and take no effect.

An example entry in config_db.json

```
 "BGP_NEIGHBOR": {
    "10.0.0.57": {
    "admin_status": "up",
    "asn": "64600",
    "holdtime": "10",
    "keepalive": "3",
    "local_addr": "10.0.0.56",
    "name": "ARISTA01T1",
    "nhopself": "0",
    "rrclient": "0"
 },

admin@sonic:~$ sudo config bgp shutdown neighbor 10.1.1.1
Usage: config bgp shutdown neighbor [OPTIONS] <ipaddr_or_hostname>
Try "config bgp shutdown neighbor -h" for help.

Error: Could not locate neighbor '10.1.1.1'
```

For FRR 'split' mode, please use these commands in FRR VTY shell instead:

Example

```
admin@sonic:~$ vtysh
Hello, this is FRRouting (version 8.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

sonic# config
```

```
sonic(config)# router bgp 65100
sonic(config-router)# neighbor 10.0.0.61 shutdown (shutdown)
sonic(config-router)# no neighbor 10.0.0.61 shutdown (startup)
sonic(config-router)# no neighbor 10.0.0.61 (remove)
sonic(config-router)# bgp shutdown (shutdown all)
sonic(config-router)# no bgp shutdown (startup all)
```

11 Configuration File Management

Table of Contents

This section explains the commands that are used to load the configuration from either ConfigDB or from minigraph.

Loading the Configuration from a JSON File

config load

This command loads the configuration from a JSON file, such as the file to which SONiC saves its configuration, /etc/sonic/config_db . json .

This command loads the configuration from the input file (if an optional filename is specified, that input file is used, otherwise the default /etc/sonic/config_db.json file is used) into CONFIG_DB. The configuration present in the input file is applied on top of the already running configuration.

This command does not flush 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 the 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.

Usage
config load [-y|--yes] [<filename>]

Parameters:

- "-y" or "--yes", forces the loading without prompting the user for confirmation.
    - If this argument is not specified, it prompts the user to confirm whether the user really wants to load this configuration file.
- <filename>, loads the configuration from the input file (<filename>) and stores into CONFIG_DB; otherwise, it uses /etc/sonic /config_db.json as the default input file.

Note

- This command does not flush CONFIG_DB before loading the new configuration. That is, if there is a new configuration in <filename>, it will be added into CONFIG_DB (running configuration); if there is any configuration changed in <filename>, it will update CONFIG_DB with those entries.

Example
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

Loading the Configuration from a Minigraph (XML) File

config load_minigraph

This command is used to load the configuration from /etc/sonic/minigraph.xml, when users do not want to use the configuration in confi g_db.json .

You 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.

Usage
config load_minigraph [-y|--yes] [-n|--no-service-restart]

Parameter:

- "-y" or "--yes", 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" or "--no-service-restart", 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 the minigraph configuration and there are no services running on the device.

Note

- If you are logged in using SSH, you might get disconnected and some configuration failures could happen, from which it might be hard to recover. You need to reconnect the SSH session after configuring the management IP address. It is recommended to execute this command from the console port.
- The management interface IP address and default route (or specific route) may require reconfiguration in case those parameters are not part of minigraph.xml.

Example
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

Reloading the Configuration

config reload

Clears the current configuration and imports a new configuration from an input file, or from

/etc/sonic/config_db.json .

Usage
config reload [-y|--yes] [-l|--load-sysinfo] [<filename>] [-n|--no-service-restart]

Parameters:

- "-y" or "--yes", 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" or "--no-service-restart", clears 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 the existing old configuration and there are no services running on the device.

Notes:

- Stops all services before clearing the configuration and then restarts those services after configuration is reloaded. It takes some time to complete the command since it needs to restart various running services in the device.
- If users are logged in using SSH, they might be disconnected depending upon the new management IP address. Users will need to reconnect their SSH sessions. In general, it is recommended to execute this command from the console port after disconnectingall SSH sessions to the device.
- config reload may change the management IP address in the input file (<filename>), this introduces the following possible scenario:

  1. mgmtIP (management IP address) is not changed. The SSH session may not be affected if the SSH session has not timed out, but it needs to resume the connection after the interface is re-configured and up.
  2. mgmtIP is changed in new configuration file. Users will lose their SSH connections.
  3. There is not any mgmtIP in the new configuration file. Users will lose their SSH connections.

The management interface IP address and default route (or specific route) may require reconfiguration if those parameters are not part of minigraph.xml.

Example
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.

Loading the Management Configuration

config load_mgmt_config

This command is used to reconfigure the hostname and mgmt interface based on the device description file.

Usage
config load_mgmt_config [-y|--yes] [<filename>]

Parameters:

- "-y" or "--yes", 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.

Note

- This command either uses the optional file specified in <filename> or looks for the file /etc/sonic/device_desc.xml . The execution fails If the file does not exist or does not have valid fields for hostname and ManagementAddress .

Example
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

Saving the Configuration to a File for Persistence

config save

This command saves CONFIG_DB (the running configuration) into the user-specified filename or the default /etc/sonic/config_db.json .

Usage
config save [-y|--yes] [<filename>]

Note

- This command retains the configuration in storage after rebooting. The file can be transferred to remote machines for debugging. You can use config load to load the configuration file at any point and generate a new CONFIG_DB (running configuration) or copy to /etc/sonic/config_db.json if you want this newly generated file to be used during reboot.

Example (boot configuration file)
admin@sonic:~$ sudo config save -y

or

Example (specific file)
admin@sonic:~$ sudo config save -y /etc/sonic/config2.json

12 Container Auto-restart

Table of Contents

SONiC includes a feature in which Docker containers can be automatically shut down and restarted if one of the critical processes running in the container exits unexpectedly. Restarting the entire container ensures that the configuration is reloaded and all processes in the container are restarted, thus increasing the likelihood of entering a healthy state.

Container Auto-restart Show Commands

show feature autorestart

This command displays the status of the auto-restart feature for containers.

Usage
show feature autorestart [<feature_name>]

Example
admin@sonic:~$ show feature autorestart Container Name Status -------------- -------- database enabled syncd enabled teamd disabled dhcp_relay enabled lldp enabled pmon enabled bgp enabled swss disabled telemetry enabled sflow enabled snmp enabled radv disabled

Optionally, you can specify a container name in order to display the auto-restart feature status for that container only.

Container Auto-restart Config Command

config feature autorestart <feature_name> <autorestart_status>

This command configures the status of the auto-restart feature for a specific container.

Usage
config feature autorestart <feature_name> (enabled | disabled)

Example
admin@sonic:~$ sudo config feature autorestart database disabled

13 CoPP

CoPP (Control Plane Policing) is a mechanism to manage and limit the protocol packets trapped in a control plane.

Users may modify the configuration to filter out some protocols or limit the number of packets to proceed.

Changing CoPP configuration is system-level tuning. Users should know the impact before applying it.

Note

- The default configuration of CoPP is accurately measured for system operation. For any change or modification, users should know the effect on the system and have the confidence to manage it, the system could be in an unexpected state which is out of service. To recover it, the user may restore the factory default configuration (refer to "sudo config-setup factory" in (202111) New Default Configuration)

CoPP trap(s) is composed of trap ID and trap group which has options - meter, and action to indicate how to handle the protocol packets when the condition is matched. The trap ID is predefined and associated with the protocol packet, for example, STP, LACP, EAPOL, and so on. The meter can be measured by packets or bytes , and the action can be one of trap, copy, or drop . A trap group has more options to specify the matching criteria to trigger the trap, please refer to the Schema section.

Schema

CoPP configuration has two sections, COPP_GROUP and COPP_TRAP. The previous one specifies trapping criteria and actions, and later one associates the trap ID(s) to the trap group to apply the matching criteria and actions for the protocol(s).

Schema
{ "COPP_GROUP": { "<group-name>": { "queue": <CPU queue#>, "trap_action": <trap, copy, or drop>, "trap_priority": <priority>, "meter_type": <packets, bytes>, "mode": <sr_tcm, tr_tcm, storm>, "color": <aware, blind>, "cbs": <commit burst size>, "cir": <commit information rate>, "pbs": <peak burst size>, "pir": <peak information rate>,

```
        "green_action": <action for packets marked as green>,
        "yellow_action": <action for packets marked as yellow>,
        "red_action": <action for packets marked as red>,
        "genetlink_name": <psample for sflow>,
        "genetlink_mcgrp_name": <packets for sflow>
        }
    },
    "COPP_TRAP": {
        "<trap-name>": {
        "trap_ids": <list of trap ID>,
        "trap_group": <group name>
        }
    }
}
```

Parameters:

- <group-name> : group name.
    - queue: Specifies the CPU queue number (0..47)the packets will enqueue into for processing when trap_action is trap or copy .
    - trap_action : Specifies the action for the trap group.
        - trap : trap the packets to the CPU for a process but not forward the packets.
        - copy: trap the packets to CPU for process and forward the packets.
        - drop : drop the packets.
    - trap_priority : Specifies the priority (0..65535) of the trap group. A higher number means higher priority.
    - meter_type : Specifies the meter type.
        - packets
        - bytes
    - mode : Specifies the meter mode.
        - sr_tcm: srTCM (Single Rate Three Color Marker).
        - tr_tcm: trTCM (Triple Rate Three Color Marker).
        - storm: storm control.
    - color : Specifies the color mode.

        - aware: color-aware mode.
        - blind: color-blind mode.
    - cbs : Committed Burst Size. Packets or bytes depending on the meter_type value.
    - cir : Committed Information Rate. Packets or bytes depending on the meter_type value.
    - pbs : Peak Burst Size. Packets or bytes depending on the meter_type value.
    - pir : Peak Information Rate. Packets or bytes depending on the meter_type value.
    - green_action : action applied on the packets which are marked as green by the meter. A valid value is the same as trap_ action .
    - yellow_action : action applied on the packets which are marked as yellow color by the meter. A valid value is the same as trap_action .
    - red_action : action applied on the packets which are marked as red color by the meter. A valid value is the same as tra p_action .
    - genetlink_name: genetlink name. Ignore (Don't add this parameter) if sFlow is disabled. The value only supports "psamp le " which is used for sFlow only.
    - genetlink_mcgrp_name: genetlink multicast group name. Ignore (Don't add this parameter) if sFlow is disabled. The value only supports "packets " which is used for sFlow only.
- <trap-name> : Trap name to identify different trap configurations.
    - trap_ids : Specifies the trap ID in the trap group. It will associate the corresponding packet type with the specified trap group. The supported trap IDs are listed in the below.
    - trap_group: Specifies the trap group to which the specified Trap ID associates with.

Supported trap IDs

- stp
- lacp
- eapol
- lldp
- pvrst
- igmp_query
- sample_packet
- udld
- switch_cust_range
- arp_req

- arp_resp
- dhcp
- ospf
- pim
- dhcpv6
- neigh_discovery
- src_nat_miss
- dest_nat_miss
- isis
- arp_suppression
- nd_suppression
- ip2me
- ssh
- snmp
- bgp
- bgpv6
- bfd
- bfdv6
- l3_mtu_error
- ttl_error
- vxlan_arp

Note:

- The trap ID src_nat_miss and dest_nat_miss are only supported on the following models:
  - AS5835-54X
  - AS7326-56X, AS7726-32X
  - AS7712-32X
- The trap ID arp_suppression , nd_suppression and vxlan_arp are only supported on the Broadcom Trident3, Trident4 switches, including the following models:
  - AS5835-54X
  - AS7326-56X, AS7726-32X
- The trap ID l3_mtu_error is not supported on the following models: AS9736- 64D.

Predefined trap groups and trap IDs in system

The following shows the predefined trap groups and IDs added by default:

Trap Group

	group	queue	trap_action	trap_priority	meter_type	mode	cir	cbs	red_action	genetlink_name	genetlink_mcgrp_name	(referred by)
1	default	0	trap		packets	sr_tcm	600	600	drop			
2	queue4_group1	4	trap	4								bgp, lacp,
3	queue4_group2	4	copy	4	packets	sr_tcm	600	600	drop			arp
4	queue4_group3	4	trap	4								lldp, dhcp, udld
5	queue1_group1	1	trap	1	packets	sr_tcm	6000	6000	drop			ip2me
6	queue1_group2	1	trap	1	packets	sr_tcm	600	600	drop			nat
7	queue2_group1	2	trap	1	packets	sr_tcm	1000	1000	drop	psample	packets	sflow

8	queue4_group4	4	trap	4	packets	sr_tcm	1000	1000	drop			ospf
9	queue4_group5	4	trap	4	packets	sr_tcm	1000	1000	drop			isis
10	queue4_group6	4	trap	5	packets	sr_tcm	600	600	drop			evpn
11	queue4_group7	4	copy	5	packets	sr_tcm	600	600	drop			evpn_vxlan

Trap ID

	trap	trap_ids	trap_group
1	bgp	bgp, bgpv6	queue4_group1
2	lacp	lacp	queue4_group1
3	arp	arp_req, arp_resp, neigh_discovery	queue4_group2
4	lldp	lldp	queue4_group3
5	dhcp	dhcp, dhcpv6	queue4_group3
6	udld	udld	queue4_group3
7	ip2me	ip2me	queue1_group1
8	nat	src_nat_miss, dest_nat_miss	queue1_group2
9	sflow	sample_packet	queue2_group1

10	ospf	ospf	queue4_group4
11	isis	isis	queue4_group4
12	evpn	arp_supression, nd_supression	queue4_group6
13	evpn_vxlan	vxlan_arp	queue4_group7

Note:

- The trap group default is created to trap the IPv4/IPv6 packets whose TTL fields in the IP headers are 0 to CPU.
- The trap group queue4_group7 is only created for AS4630-54PE, AS5835-54X, AS5835-54T, AS7326-56X, and AS7726-32X models.

Example

The following example configures a trap group (queue1_group2) and a trap (nat) which lists two NAT trap IDs (src_nat_miss and dest_nat _miss), and associates the trap list with the trap group (queue1_group2) which defines a meter (packet), criteria (600), and action (drop).

Example of trap group

```
{
   "COPP_GROUP": {
        "queue1_group2": {
        "trap_action":"trap",
        "trap_priority":"1",
        "queue": "1",
        "meter_type":"packets",
        "mode":"sr_tcm",
        "cir":"600",
        "cbs":"600",
        "red_action":"drop"
```

```
        }
    },
    "COPP_TRAP": {
        "nat": {
        "trap_ids": "src_nat_miss,dest_nat_miss",
        "trap_group": "queue1_group2"
        }
    }
}
```

14 Critical Resource Monitoring

Table of Contents

CRM show commands

crm show

Display the usage of show command

Usage
admin@sonic:~$ crm show ? Usage: crm show [OPTIONS] COMMAND [ARGS]... Show CRM related information

```
Options:
  --help  Show this message and exit.
Commands:
  resources   Show CRM resources information
  summary     Show CRM general information
  thresholds  Show CRM thresholds information
```

crm show summary

Display polling interval setting

Example
admin@sonic:~$ crm show summary Polling Interval: 300 second(s)

crm show resources

Display the usage of show resources command

Usage
admin@sonic:~$ crm show resources Usage: crm show resources [OPTIONS] COMMAND [ARGS]... Show CRM resources information Options: --help Show this message and exit.

```
Commands:
  acl                 Show CRM information for acl resource
  all                 Show CRM information for all resources
  dnat                Show CRM information for DNAT resource
  fdb                 Show CRM information for fdb resource
  ipmc                Show CRM information for IPMC resource
  ipv4                CRM resource IPv4 address family
  ipv6                CRM resource IPv6 address family
  mpls                CRM resource MPLS address family
  nexthop             Show CRM information for nexthop resource
  snat                Show CRM information for SNAT resource
  srv6-my-sid-entry   Show CRM information for SRV6 MY_SID entry
  srv6-nexthop        Show CRM information for SRV6 Nexthop
```

crm show resources all

Display all statistic which include used by all components and available resources in the ASIC

Example

```
admin@sonic:~$ crm show resources all
Resource Name          Used Count    Available Count
---------------------  ------------  -----------------
ipv4_route                  66           100286
ipv6_route                  68            39279
ipv4_nexthop                 0            32765
ipv6_nexthop                 0            32765
ipv4_neighbor                0            32765
```

```
ipv6_neighbor                0           4062
nexthop_group_member         0           32767
nexthop_group                0           511
fdb_entry                    0           16384
ipmc_entry                   0           0
snat_entry                   0           45056
dnat_entry                   0           45056
mpls_inseg                   0           0
mpls_nexthop                 0           32765
srv6_nexthop                 0           32765
srv6_my_sid_entry            0           0
Stage    Bind Point    Resource Name     Used Count    Available Count
-------  ------------  ---------------  ------------  -----------------
INGRESS  PORT          acl_group              32            224
INGRESS  PORT          acl_table              3             2
INGRESS  LAG           acl_group              0             224
INGRESS  LAG           acl_table              0             2
INGRESS  VLAN          acl_group              0             224
INGRESS  VLAN          acl_table              0             5
INGRESS  RIF           acl_group              0             224
INGRESS  RIF           acl_table              0             5
INGRESS  SWITCH        acl_group              0             224
INGRESS  SWITCH        acl_table              0             5
EGRESS   PORT          acl_group              0             224
EGRESS   PORT          acl_table              0             2
EGRESS   LAG           acl_group              0             224
EGRESS   LAG           acl_table              0             2
EGRESS   VLAN          acl_group              0             224
EGRESS   VLAN          acl_table              0             2
EGRESS   RIF           acl_group              0             224
EGRESS   RIF           acl_table              0             2
EGRESS   SWITCH        acl_group              0             224
EGRESS   SWITCH        acl_table              0             2
Table ID       Resource Name     Used Count    Available Count
```

```
-------------- -------------- ------------ ----------------
0x7000000000a20  acl_entry                2            6142
0x7000000000a20  acl_counter              2            6142
```

crm show resources acl

Display the usage of ACL resources show command

Usage

```
admin@sonic:~$ crm show resources acl

Usage: crm show resources acl [OPTIONS] COMMAND [ARGS]...

  Show CRM information for acl resource

Options:

  --help  Show this message and exit.

Commands:

  group  Show CRM information for acl group resource

  table  Show CRM information for acl table resource
```

crm show resources acl group

Display ACL group statistic which include used by all components and available resources in the ASIC

Example

```
admin@sonic:~$ crm show resources acl group
Stage    Bind Point    Resource Name      Used Count    Available Count
-------  ------------  ---------------  ------------  -----------------
INGRESS  PORT          acl_group                32             224
```

```
INGRESS  PORT        acl_table              2            3
INGRESS  LAG         acl_group              0          224
INGRESS  LAG         acl_table              0            3
INGRESS  VLAN        acl_group              0          224
INGRESS  VLAN        acl_table              0            6
INGRESS  RIF         acl_group              0          224
INGRESS  RIF         acl_table              0            6
INGRESS  SWITCH      acl_group              0          224
INGRESS  SWITCH      acl_table              0            6
EGRESS   PORT        acl_group              0          224
EGRESS   PORT        acl_table              0            2
EGRESS   LAG         acl_group              0          224
EGRESS   LAG         acl_table              0            2
EGRESS   VLAN        acl_group              0          224
EGRESS   VLAN        acl_table              0            2
EGRESS   RIF         acl_group              0          224
EGRESS   RIF         acl_table              0            2
EGRESS   SWITCH      acl_group              0          224
EGRESS   SWITCH      acl_table              0            2
```

crm show resources acl table

Display ACL table statistic which include used by all components and available resources in the ASIC

Example

```
admin@sonic:~$ crm show resources acl table
Table ID       Resource Name     Used Count    Available Count
-------------- ----------------- ------------ -----------------
0x7000000000a20  acl_entry              2           6142
0x7000000000a20  acl_counter            2           6142
```

crm show resources dnat

(Unsupported in Broadcom platform) Display the usage of DNAT resources show command

Example
admin@sonic:~$ crm show resources dnat Resource Name Used Count Available Count ---------- ---------- ---------- dnat_entry 0 45056

crm show resources fdb

Display FDB statistic which include used by all components and available resources in the ASIC

Example
admin@sonic:~$ crm show resources fdb Resource Name Used Count Available Count ---------- ---------- ---------- fdb_entry 0 32768

crm show resources ipmc

(Unsupported) Display the usage of IPMC resources show command

Example
admin@sonic:~$ crm show resources ipmc Resource Name Used Count Available Count ---------- ---------- ---------- ipmc_entry

crm show resources ipv4

Display the usage of IPv4 resources show command

Usage
admin@sonic:~$ crm show resources ipv4 Usage: crm show resources ipv4 [OPTIONS] COMMAND [ARGS]... CRM resource IPv4 address family Options: --help Show this message and exit. Commands: neighbor Show CRM information for neighbor resource nexthop Show CRM information for nexthop resource route Show CRM information for route resource

crm show resources ipv4 neighbor

Display IPv4 neighbor statistic which include used by all components and available resources in the ASIC

Example
admin@sonic:~$ crm show resources ipv4 Usage: crm show resources ipv4 [OPTIONS] COMMAND [ARGS]... CRM resource IPv4 address family Options: --help Show this message and exit. Commands: neighbor Show CRM information for neighbor resource nexthop Show CRM information for nexthop resource route Show CRM information for route resource

```
admin@as5812-54x:~$ crm show resources ipv4 neighbor
Resource Name      Used Count    Available Count
---------------  ------------  -----------------
ipv4_neighbor            0            8192
```

crm show resources ipv4 nexthop

Display IPv4 nexthop statistic which include used by all components and available resources in the ASIC

Example

```
admin@sonic:~$ crm show resources ipv4 nexthop
Resource Name      Used Count    Available Count
---------------  ------------  -----------------
ipv4_nexthop             0            49118
```

crm show resources ipv4 route

Display IPv4 route statistic which include used by all components and available resources in the ASIC

Example

```
admin@sonic:~$ crm show resources ipv4 route
Resource Name      Used Count    Available Count
---------------  ------------  -----------------
ipv4_route              66            98238
```

crm show resources ipv6

Display the usage of IPv6 resources show command

Usage

```
admin@sonic:~$ crm show resources ipv6

Usage: crm show resources ipv6 [OPTIONS] COMMAND [ARGS]...

  CRM resource IPv6 address family

Options:

  --help  Show this message and exit.

Commands:

  neighbor  Show CRM information for neighbor resource

  nexthop   Show CRM information for nexthop resource

  route     Show CRM information for route resource
```

crm show resources ipv6 neighbor

Display IPv6 neighbor statistic which include used by all components and available resources in the ASIC

Example

```
admin@sonic:~$ crm show resources ipv6 neighbor
Resource Name      Used Count    Available Count
---------------  ------------  -----------------
ipv6_neighbor            33             4096
```

crm show resources ipv6 nexthop

Display IPv6 nexthop statistic which include used by all components and available resources in the ASIC

Example

```
admin@sonic:~$ crm show resources ipv6 nexthop
Resource Name      Used Count    Available Count
---------------  ------------  -----------------
ipv6_nexthop             33            49117
```

crm show resources ipv6 route

Display IPv6 route statistic which include used by all components and available resources in the ASIC

Example

```
admin@sonic:~$ crm show resources ipv6 route
Resource Name      Used Count    Available Count
---------------  ------------  -----------------
ipv6_route               68            16316
```

crm show resources mpls

(Unsupported in Broadcom platform) Display the usage of MPLS resources show command

Example

```
admin@sonic:~$ crm show resources mpls
Usage: crm show resources mpls [OPTIONS] COMMAND [ARGS]...
  CRM resource MPLS address family
Options:
  --help  Show this message and exit.
Commands:
  inseg    Show CRM information for in-segment resource
  nexthop  Show CRM information for nexthop resource
```

crm show resources mpls inseg

(Unsupported in Broadcom platform) Display MPLS inseg statistic which include used by all components and available resources in the ASIC.

Example
admin@sonic:~$ crm show resources mpls inseg Resource Name Used Count Available Count ---------- ---------- ---------- mpls_inseg 0 0

crm show resources mpls nexthop

(Unsupported in Broadcom platform) Display MPLS nexthop statistic which include used by all components and available resources in the ASIC.

Example
admin@sonic:~$ crm show resources mpls nexthop Resource Name Used Count Available Count ---------- ---------- ---------- mpls_nexthop 0 32765

crm show resources nexthop group

Display the usage of nexthop group resources show command

Usage
admin@sonic:~$ crm show resources nexthop group Usage: crm show resources nexthop group [OPTIONS] COMMAND [ARGS]...

```
  Show CRM information for nexthop group resource

Options:

  --help  Show this message and exit.

Commands:

  member  Show CRM information for nexthop group member resource

  object  Show CRM information for nexthop group resource
```

crm show resources nexthop group member

Display nexthop group member statistic which include used by all components and available resources in the ASIC

Example

```
admin@sonic:~$ crm show resources nexthop group member

Resource Name          Used Count    Available Count
---------------------  ------------  -----------------
nexthop_group_member           0           16384
```

crm show resources nexthop group object

Display nexthop group object statistic which include used by all components and available resources in the ASIC

Example

```
admin@sonic:~$ crm show resources nexthop group object
Resource Name      Used Count    Available Count
-----------------  ------------  -----------------
```

nexthop_group	0	128

crm show resources snat

Display the usage of SNAT resources show command

Example

```
admin@sonic:~$ crm show resources snat
Resource Name      Used Count    Available Count
---------------  ------------  -----------------
snat_entry               0           45056
```

crm show resources srv6-my-sid-entry

(Unsupported in Broadcom platform) Display the usage of srv6-my-sid-entry resources show command.

Example

```
admin@sonic:~$ crm show resources srv6-my-sid-entry
Resource Name      Used Count    Available Count
---------------  ------------  -----------------
srv6-my-sid-entry        0           45056
```

crm show resources srv6-nexthop

(Unsupported in Broadcom platform) Display the usage ofsrv6-nexthop resources show command

Example

```
admin@sonic:~$ crm show resources srv6-nexthop
Resource Name      Used Count    Available Count
```

srv6-nexthop	0	45056

CRM config command

Config command should be extended in order to add "crm" alias to the CRM utility.

crm config

Display the usage of config command

Usage
admin@sonic:~$ crm config Usage: crm config [OPTIONS] COMMAND [ARGS]... CRM related configuration Options: --help Show this message and exit. Commands: polling CRM polling configuration thresholds CRM thresholds configuration

crm config polling interval

Configure the polling interval to fetch available resources from ASIC

Usage
admin@sonic:~$ crm config polling interval

Usage: crm config polling interval [OPTIONS] INTERVAL

Example
admin@sonic:~$ crm config polling interval 400

crm config thresholds

Display the usage of config thresholds command

Usage
admin@as5812-54x:~$ crm config thresholds Usage: crm config thresholds [OPTIONS] COMMAND [ARGS]... CRM thresholds configuration Options: --help Show this message and exit. Commands: acl CRM configuration for ACL resource dnat CRM configuration for Destination NAT resource fdb CRM configuration for FDB resource ipmc CRM configuration for IPMC resource ipv4 CRM resource IPv4 address-family ipv6 CRM resource IPv6 address-family mpls CRM resource MPLS address-family nexthop CRM configuration for nexthop resource

snat	CRM configuration for Source NAT resource
srv6-my-sid-entry	CRM configuration for SRV6 MY_SID resource
srv6-nexthop	CRM configuration for SRV6 Nexthop resource

crm config thresholds acl group counter type

Configure threshold type of ACL group

Usage
admin@sonic:~$ crm config thresholds acl group type Usage: crm config thresholds acl group type [OPTIONS] [percentage|used|free] Try "crm config thresholds acl group type --help" for help.

Example
admin@sonic:~$ crm config thresholds acl group type percentage admin@sonic:~$ crm config thresholds acl group type used admin@sonic:~$ crm config thresholds acl group type free

crm config thresholds acl group counter low|high

Configure low|high threshold of ACL group

Usage
admin@sonic:~$ crm config thresholds acl group low Usage: crm config thresholds acl group low [OPTIONS] VALUE

Try "crm config thresholds acl group low --help" for help. admin@sonic:~$ crm config thresholds acl group high Usage: crm config thresholds acl group high [OPTIONS] VALUE Try "crm config thresholds acl group high --help" for help.

Example
admin@sonic:~$ crm config thresholds acl group high 90 admin@sonic:~$ crm config thresholds acl group low 10

crm config thresholds acl table type

Configure threshold type of ACL table

Usage
admin@sonic:~$ crm config thresholds acl table type Usage: crm config thresholds acl table type [OPTIONS] [percentage|used|free] Try "crm config thresholds acl table type --help" for help.

Example
admin@sonic:~$ crm config thresholds acl table type percentage admin@sonic:~$ crm config thresholds acl table type used admin@sonic:~$ crm config thresholds acl table type free

crm config thresholds acl table low|high

Configure low|high threshold of ACL table

Usage
admin@sonic:~$ crm config thresholds acl table low Usage: crm config thresholds acl table low [OPTIONS] VALUE Try "crm config thresholds acl table low --help" for help. admin@sonic:~$ crm config thresholds acl table high Usage: crm config thresholds acl table high [OPTIONS] VALUE Try "crm config thresholds acl table high --help" for help.

Example
admin@sonic:~$ crm config thresholds acl table low 3 admin@sonic:~$ crm config thresholds acl table high 80

crm config thresholds dnat low|high

(Unsupported in Broadcom platform) Configure low|high threshold of DNAT

Usage
admin@sonic:~$ crm config thresholds dnat low Usage: crm config thresholds dnat low [OPTIONS] VALUE Try "crm config thresholds dnat low --help" for help admin@sonic:~$ crm config thresholds dnat high Usage: crm config thresholds dnat high [OPTIONS] VALUE

Try "crm config thresholds dnat high --help" for help.

Example
admin@sonic:~$ crm config thresholds dnat low 3 admin@sonic:~$ crm config thresholds dnat high 80

crm config thresholds dnat type

(Unsupported in Broadcom platform) Configure threshold type of DNAT

Usage
admin@sonic:~$ crm config thresholds dnat type Usage: crm config thresholds dnat type [OPTIONS] [percentage|used|free] Try "crm config thresholds dnat type --help" for help.

Example
admin@sonic:~$ crm config thresholds dnat type percentage admin@sonic:~$ crm config thresholds dnat type used admin@sonic:~$ crm config thresholds dnat type free

crm config thresholds fdb type

Configure threshold type of FDB

Usage

dmin@sonic:~$ crm config thresholds fdb type Usage: crm config thresholds fdb type [OPTIONS] [percentage|used|free] Try "crm config thresholds fdb type --help" for help.

Example
admin@sonic:~$ crm config thresholds fdb type percentage admin@sonic:~$ crm config thresholds fdb type used admin@sonic:~$ crm config thresholds fdb type free

crm config thresholds fdb low|high

Configure low|high threshold of FDB

Usage
admin@sonic:~$ crm config thresholds fdb low Usage: crm config thresholds fdb low [OPTIONS] VALUE Try "crm config thresholds fdb low --help" for help. admin@sonic:~$ crm config thresholds fdb high Usage: crm config thresholds fdb high [OPTIONS] VALUE Try "crm config thresholds fdb high --help" for help.

Example
admin@sonic:~$ crm config thresholds fdb low 20 admin@sonic:~$ crm config thresholds fdb high 311111

crm config thresholds ipmc low|high

(Unsupported) Configure low|high threshold of IPMC

Usage
admin@sonic:~$ crm config thresholds ipmc low Usage: crm config thresholds ipmc low [OPTIONS] VALUE Try "crm config thresholds ipmc low --help" for help. admin@sonic:~$ crm config thresholds ipmc high Usage: crm config thresholds ipmc high [OPTIONS] VALUE Try "crm config thresholds ipmc high --help" for help.

Example
admin@sonic:~$ crm config thresholds ipmc low 3 admin@sonic:~$ crm config thresholds ipmc high 80

crm config thresholds ipmc type

Configure threshold type of IPMC

Usage
admin@sonic:~$ crm config thresholds ipmc type Usage: crm config thresholds ipmc type [OPTIONS] [percentage|used|free] Try "crm config thresholds ipmc type --help" for help.

Example
admin@sonic:~$ crm config thresholds ipmc type percentage admin@sonic:~$ crm config thresholds ipmc type used admin@sonic:~$ crm config thresholds ipmc type free

crm config thresholds ipv4 neighbor type

Configure threshold type of IPv4 neighbor

Usage
admin@sonic:~$ crm config thresholds ipv4 neighbor type Usage: crm config thresholds ipv4 neighbor type [OPTIONS] [percentage|used|free] Try "crm config thresholds ipv4 neighbor type --help" for help.

Example
admin@sonic:~$ crm config thresholds ipv4 neighbor type percentage admin@sonic:~$ crm config thresholds ipv4 neighbor type used admin@sonic:~$ crm config thresholds ipv4 neighbor type free

crm config thresholds ipv4 neighbor low|high

Configure low|high threshold of IPv4 neighbor

Usage

```
admin@sonic:~$ crm config thresholds ipv4 neighbor low

Usage: crm config thresholds ipv4 neighbor low [OPTIONS] VALUE

Try "crm config thresholds ipv4 neighbor low --help" for help.


admin@sonic:~$ crm config thresholds ipv4 neighbor high

Usage: crm config thresholds ipv4 neighbor high [OPTIONS] VALUE

Try "crm config thresholds ipv4 neighbor high --help" for help.
```

Example

```
admin@sonic:~$ crm config thresholds ipv4 neighbor low 2
admin@sonic:~$ crm config thresholds ipv4 neighbor high 5566
```

crm config thresholds ipv4 nexthop type

Configure threshold type of IPv4 nexthop

Usage

```
admin@sonic:~$ crm config thresholds ipv4 nexthop type

Usage: crm config thresholds ipv4 nexthop type [OPTIONS]
                                               [percentage|used|free]

Try "crm config thresholds ipv4 nexthop type --help" for help.
```

Example

admin@sonic:~$ crm config thresholds ipv4 nexthop type percentage admin@sonic:~$ crm config thresholds ipv4 nexthop type free admin@sonic:~$ crm config thresholds ipv4 nexthop type used

crm config thresholds ipv4 nexthop low|high

Configure low|high threshold of IPv4 nexthop

Usage
admin@sonic:~$ crm config thresholds ipv4 nexthop low Usage: crm config thresholds ipv4 nexthop low [OPTIONS] VALUE Try "crm config thresholds ipv4 nexthop low --help" for help. admin@sonic:~$ crm config thresholds ipv4 nexthop high Usage: crm config thresholds ipv4 nexthop high [OPTIONS] VALUE Try "crm config thresholds ipv4 nexthop high --help" for help.

Example
admin@sonic:~$ crm config thresholds ipv4 nexthop high 90 admin@sonic:~$ crm config thresholds ipv4 nexthop high 9000000

crm config thresholds ipv4 route type

Configure threshold type of IPv4 route

Usage

admin@sonic:~$ crm config thresholds ipv4 route type Usage: crm config thresholds ipv4 route type [OPTIONS] [percentage|used|free] Try "crm config thresholds ipv4 route type --help" for help.

Example
admin@sonic:~$ crm config thresholds ipv4 route type percentage admin@sonic:~$ crm config thresholds ipv4 route type used admin@sonic:~$ crm config thresholds ipv4 route type free

crm config thresholds ipv4 route low|high

Configure low|high threshold of IPv4 route

Usage
admin@sonic:~$ crm config thresholds ipv4 route low Usage: crm config thresholds ipv4 route low [OPTIONS] VALUE Try "crm config thresholds ipv4 route low --help" for help. admin@sonic:~$ crm config thresholds ipv4 route high Usage: crm config thresholds ipv4 route high [OPTIONS] VALUE Try "crm config thresholds ipv4 route high --help" for help.

Example
admin@sonic:~$ crm config thresholds ipv4 route low 11 admin@sonic:~$ crm config thresholds ipv4 route high 800000

crm config thresholds ipv6 neighbor type

Configure threshold type of IPv6 neighbor

Usage
admin@sonic:~$ crm config thresholds ipv6 neighbor type Usage: crm config thresholds ipv6 neighbor type [OPTIONS] [percentage|used|free] Try "crm config thresholds ipv6 neighbor type --help" for help.

Example
admin@sonic:~$ crm config thresholds ipv6 neighbor type percentage admin@sonic:~$ crm config thresholds ipv6 neighbor type used admin@sonic:~$ crm config thresholds ipv6 neighbor type free

crm config thresholds ipv6 neighbor low|high

Configure low|high threshold of IPv6 neighbor

Usage
admin@sonic:~$ crm config thresholds ipv6 neighbor low Usage: crm config thresholds ipv6 neighbor low [OPTIONS] VALUE Try "crm config thresholds ipv6 neighbor low --help" for help. admin@sonic:~$ crm config thresholds ipv6 neighbor high Usage: crm config thresholds ipv6 neighbor high [OPTIONS] VALUE

Try "crm config thresholds ipv6 neighbor high --help" for help.

Example
admin@sonic:~$ crm config thresholds ipv6 neighbor low 100 admin@sonic:~$ crm config thresholds ipv6 neighbor high 50000

crm config thresholds ipv6 nexthop type

Configure threshold type of IPv6 nexthop

Usage
admin@sonic:~$ crm config thresholds ipv6 nexthop type Usage: crm config thresholds ipv6 nexthop type [OPTIONS] [percentage|used|free] Try "crm config thresholds ipv6 nexthop type --help" for help.

Example
admin@sonic:~$ crm config thresholds ipv6 nexthop type percentage admin@sonic:~$ crm config thresholds ipv6 nexthop type used admin@sonic:~$ crm config thresholds ipv6 nexthop type free

crm config thresholds ipv6 nexthop low|high

Configure low|high threshold of IPv6 nexthop

Usage
admin@sonic:~$ crm config thresholds ipv6 nexthop low Usage: crm config thresholds ipv6 nexthop low [OPTIONS] VALUE Try "crm config thresholds ipv6 nexthop low --help" for help. admin@sonic:~$ crm config thresholds ipv6 nexthop high Usage: crm config thresholds ipv6 nexthop high [OPTIONS] VALUE Try "crm config thresholds ipv6 nexthop high --help" for help.

Example
admin@sonic:~$ crm config thresholds ipv6 nexthop low 10 admin@sonic:~$ crm config thresholds ipv6 nexthop high 80000

crm config thresholds ipv6 route type

Configure threshold type of IPv6 route

Usage
admin@sonic:~$ crm config thresholds ipv6 route type Usage: crm config thresholds ipv6 route type [OPTIONS] [percentage|used|free] Try "crm config thresholds ipv6 route type --help" for help.

Example
admin@sonic:~$ crm config thresholds ipv6 route type percentage

```
admin@sonic:~$ crm config thresholds ipv6 route type used
admin@sonic:~$ crm config thresholds ipv6 route type free
```

crm config thresholds ipv6 route low|high

Configure low|high threshold of IPv6 route

Usage
admin@sonic:~$ crm config thresholds ipv6 route low Usage: crm config thresholds ipv6 route low [OPTIONS] VALUE Try "crm config thresholds ipv6 route low --help" for help. admin@sonic:~$ crm config thresholds ipv6 route high Usage: crm config thresholds ipv6 route high [OPTIONS] VALUE Try "crm config thresholds ipv6 route high --help" for help.

Example
admin@sonic:~$ crm config thresholds ipv6 route low 100 admin@sonic:~$ crm config thresholds ipv6 route low 80000

crm config thresholds mpls inseg low|high

(Unsupported in Broadcom platform) Configure low|high threshold of MPLS inseg

Usage
admin@sonic:~$ crm config thresholds mpls inseg low

```
Usage: crm config thresholds mpls inseg low [OPTIONS] VALUE

Try "crm config thresholds mpls inseg low --help" for help

admin@sonic:~$ crm config thresholds mpls inseg high

Usage: crm config thresholds mpls inseg high [OPTIONS] VALUE

Try "crm config thresholds mpls inseg high --help" for help.
```

Example
admin@sonic:~$ crm config thresholds mpls inseg low 3 admin@sonic:~$ crm config thresholds mpls inseg high 80

crm config thresholds mpls inseg type

(Unsupported in Broadcom platform) Configure threshold type of mpls inseg

Usage
admin@sonic:~$ crm config thresholds mpls inseg type Usage: crm config thresholds mpls inseg type [OPTIONS] [percentage|used|free] Try "crm config thresholds mpls inseg type --help" for help.

Example
admin@sonic:~$ crm config thresholds mpls inseg type percentage admin@sonic:~$ crm config thresholds mpls inseg type used admin@sonic:~$ crm config thresholds mpls inseg type free

crm config thresholds mpls nexthop low|high

(Unsupported in Broadcom platform) Configure low|high threshold of MPLS nexthop

Usage
admin@sonic:~$ crm config thresholds mpls nexthop low Usage: crm config thresholds mpls nexthop low [OPTIONS] VALUE Try "crm config thresholds mpls nexthop low --help" for help admin@sonic:~$ crm config thresholds mpls nexthop high Usage: crm config thresholds mpls nexthop high [OPTIONS] VALUE Try "crm config thresholds mpls nexthop high --help" for help.

Example
admin@sonic:~$ crm config thresholds mpls nexthop low 3 admin@sonic:~$ crm config thresholds mpls nexthop high 80

crm config thresholds mpls nexthop type

(Unsupported in Broadcom platform) Configure threshold type of mpls nexthop

Usage
admin@sonic:~$ crm config thresholds mpls nexthop type Usage: crm config thresholds mpls nexthop type [OPTIONS] [percentage|used|free] Try "crm config thresholds mpls nexthop type --help" for help.

Example
admin@sonic:~$ crm config thresholds mpls nexthop type percentage admin@sonic:~$ crm config thresholds mpls nexthop type used admin@sonic:~$ crm config thresholds mpls nexthop type free

crm config thresholds nexthop group member type

Configure threshold type of nexthop group member

Usage
admin@sonic:~$ crm config thresholds nexthop group member type Usage: crm config thresholds nexthop group member type [OPTIONS] [percentage|used|free] Try "crm config thresholds nexthop group member type --help" for help.

Example
admin@sonic:~$ crm config thresholds nexthop group member type percentage admin@sonic:~$ crm config thresholds nexthop group member type used admin@sonic:~$ crm config thresholds nexthop group member type free

crm config thresholds nexthop group member low|high

Configure low|high threshold of nexthop group member

Usage

```
admin@sonic:~$ crm config thresholds nexthop group member low

Usage: crm config thresholds nexthop group member low [OPTIONS] VALUE

Try "crm config thresholds nexthop group member low --help" for help.

admin@sonic:~$ crm config thresholds nexthop group member high

Usage: crm config thresholds nexthop group member high [OPTIONS] VALUE

Try "crm config thresholds nexthop group member high --help" for help.
```

Example
admin@sonic:~$ crm config thresholds nexthop group member low 1000 admin@sonic:~$ crm config thresholds nexthop group member high 12345

crm config thresholds nexthop group object type

Configure threshold type of nexthop group object

Usage
admin@sonic:~$ crm config thresholds nexthop group object type Usage: crm config thresholds nexthop group object type [OPTIONS] [percentage|used|free] Try "crm config thresholds nexthop group object type --help" for help.

Example
admin@sonic:~$ crm config thresholds nexthop group object type percentage admin@sonic:~$ crm config thresholds nexthop group object type used

admin@sonic:~$ crm config thresholds nexthop group object type free

crm config thresholds nexthop group object low|high

Configure threshold type of nexthop group object

Usage
admin@sonic:~$ crm config thresholds nexthop group object low Usage: crm config thresholds nexthop group object low [OPTIONS] VALUE Try "crm config thresholds nexthop group object low --help" for help. admin@sonic:~$ crm config thresholds nexthop group object high Usage: crm config thresholds nexthop group object high [OPTIONS] VALUE Try "crm config thresholds nexthop group object high --help" for help.

Example
admin@sonic:~$ crm config thresholds nexthop group object low 100 admin@sonic:~$ crm config thresholds nexthop group object high 2000

crm config thresholds snat low|high

Configure low|high threshold of SNAT

Usage
admin@sonic:~$ crm config thresholds snat low Usage: crm config thresholds snat low [OPTIONS] VALUE

Try "crm config thresholds snat low --help" for help

admin@sonic:~$ crm config thresholds snat high

Usage: crm config thresholds snat high [OPTIONS] VALUE

Try "crm config thresholds snat high --help" for help.

Example
admin@sonic:~$ crm config thresholds snat low 3 admin@sonic:~$ crm config thresholds snat high 80

crm config thresholds snat type

Configure threshold type of SNAT

Usage
admin@sonic:~$ crm config thresholds snat type Usage: crm config thresholds snat type [OPTIONS] [percentage|used|free] Try "crm config thresholds snat type --help" for help.

Example
admin@sonic:~$ crm config thresholds snat type percentage admin@sonic:~$ crm config thresholds snat type used admin@sonic:~$ crm config thresholds snat type free

crm config thresholds srv6-my-sid-entry low|high

(Unsupported in Broadcom platform) Configure low|high threshold of srv6-my-sid-entry

Usage
admin@sonic:~$ crm config thresholds srv6-my-sid-entry low Usage: crm config thresholds srv6-my-sid-entry low [OPTIONS] VALUE Try "crm config thresholds srv6-my-sid-entry low --help" for help admin@sonic:~$ crm config thresholds srv6-my-sid-entry high Usage: crm config thresholds srv6-my-sid-entry high [OPTIONS] VALUE Try "crm config thresholds srv6-my-sid-entry high --help" for help.

Example
admin@sonic:~$ crm config thresholds srv6-my-sid-entry low 3 admin@sonic:~$ crm config thresholds srv6-my-sid-entry high 80

crm config thresholds srv6-my-sid-entry type

(Unsupported in Broadcom platform) Configure threshold type of srv6-my-sid-entry

Usage
admin@sonic:~$ crm config thresholds srv6-my-sid-entry type Usage: crm config thresholds srv6-my-sid-entry type [OPTIONS] [percentage|used|free] Try "crm config thresholds srv6-my-sid-entry type --help" for help.

Example
admin@sonic:~$ crm config thresholds srv6-my-sid-entry type percentage admin@sonic:~$ crm config thresholds srv6-my-sid-entry type used admin@sonic:~$ crm config thresholds srv6-my-sid-entry type free

crm config thresholds srv6-nexthop low|high

Configure low|high threshold of srv6-nexthop

Usage
admin@sonic:~$ crm config thresholds srv6-nexthop low Usage: crm config thresholds srv6-nexthop low [OPTIONS] VALUE Try "crm config thresholds srv6-nexthop low --help" for help admin@sonic:~$ crm config thresholds srv6-nexthop high Usage: crm config thresholds srv6-nexthop high [OPTIONS] VALUE Try "crm config thresholds srv6-nexthop high --help" for help.

Example
admin@sonic:~$ crm config thresholds srv6-nexthop low 3 admin@sonic:~$ crm config thresholds srv6-nexthop high 80

crm config thresholds srv6-nexthop type

Configure threshold type of srv6-nexthop

Usage
admin@sonic:~$ crm config thresholds srv6-nexthop type Usage: crm config thresholds srv6-nexthop type [OPTIONS] [percentage|used|free] Try "crm config thresholds srv6-nexthop type --help" for help.

Example
admin@sonic:~$ crm config thresholds srv6-nexthop type percentage admin@sonic:~$ crm config thresholds srv6-nexthop type used admin@sonic:~$ crm config thresholds srv6-nexthop type free

15 Device Hostname

This section of commands is used to change the device hostname without traffic being impacted.

Update Device Hostname Configuration Commands

config hostname

This command is used to change the device hostname without traffic being impacted.

Usage
config hostname <new_hostname>

Example
admin@sonic:~$ sudo config hostname CSW06

Note: The configured setting will be lost after a system reboot. To preserve the setting, run config save.

16 DHCP Relay

Table of Contents

These commands are used to add or remove DHCP Relay destination IP addresses for VLAN interfaces.

When the DHCP Relay service is enabled, and the switch sees a DHCP client request from an attached host, it inserts its own IP address into the request so that the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to a DHCP server (destination IP) on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP Relay agent (the switch). The switch then passes the DHCP response received from the server to the client.

DHCP Relay show commands

show vlan brief

This command displays brief information about all the v lans configured in the device. It displays the v lan ID, IP address (if configured for the vlan), list of vlan member ports, whether the port is tagged or in un tagged mode and the DHCP Helper Address.

Usage
show vlan brief show vlan brief --verbose

Example

```
+-----------+-------------+------------+----------+---------+--------------+--------------------------+
|  VLAN ID | IP Address   | Ports      | Port     | Proxy    | DHCP Helper   | DHCP Relay Configuration   |
|          |              |            | Tagging  | ARP      | Address       |                            |
+===========+==============+============+==========+==========+===============+============================
=================+
|      100 | 100.0.0.1/24 | Ethernet512 | tagged    | disabled |               | Source Interface:          |
|          |              | Ethernet513 | tagged    |          |               | Link Selection:            |
|          |              |             |           |          |               | Server Vrf:                |
|          |              |             |           |          |               | Server ID Override:        |
+----------+-------------+------------+----------+---------+--------------+--------------------------+
```

DHCP Relay config commands

config vlan dhcp_relay add

This command adds a DHCP Relay Destination IP address to a VLAN. Note that more that one DHCP Relay Destination IP address can be added on a VLAN interface.

Usage
config vlan dhcp_relay add <vlan_id> <dhcp_relay_destination_ip>

Example
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..

config vlan dhcp_relay delete

This command deletes a configured DHCP Relay destination IP address from a VLAN interface.

Usage
config vlan dhcp_relay del <vlan-id> <dhcp_relay_destination_ip>

Example
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... Running command: systemctl restart dhcp_relay

config vlan dhcp_relay link_selection add

This command is used to enable DHCP relay link selection on a VLAN. Note that users need to add the dhcp relay source interface first.

Usage
config vlan dhcp_relay link_selection add <vlan_id>

Example
admin@sonic:~$ sudo config vlan dhcp_relay link_selection add 1000

Enable DHCP relay link selection for Vlan1000 Restarting DHCP relay service...

config vlan dhcp_relay link_selection del

This command is used to disable DHCP relay link selection on a VLAN.

Usage
config vlan dhcp_relay link_selection del <vlan_id>

Example
admin@sonic:~$ sudo config vlan dhcp_relay link_selection del 1000 Removed DHCP relay link selection from Vlan1000 Restarting DHCP relay service...

config vlan dhcp_relay src_intf add

This command is used to set the DHCP relay source interface on a VLAN.

Usage
config vlan dhcp_relay src_intf add <vlan_id> <dhcp_relay_src_intf>

Example

```
admin@sonic:~$ sudo config vlan dhcp_relay src_intf add 1000 PortChannel0001
Added DHCP relay source interface PortChannel0001 for Vlan1000
Restarting DHCP relay service...
```

config vlan dhcp_relay src_intf del

This command is used to remove the configured DHCP relay source interface from a VLAN. Note that users need to disable the dhcp relay link selection first.

Usage

```
config vlan dhcp_relay src_intf del <vlan_id> <dhcp_relay_src_intf>
```

Example

```
admin@sonic:~$ sudo config vlan dhcp_relay src_intf del 1000 PortChannel0001
Removed DHCP relay source interface PortChannel0001 from Vlan1000
Restarting DHCP relay service...
```

config vlan dhcp_relay server_vrf add

The config vlan dhcp_relay server_vrf add command is used to specify the DHCP relay server vrf on a VLAN.

Usage

```
config vlan dhcp_relay server_vrf add <vlan_id> <dhcp_relay_server_vrf>
```

Example

admin@sonic:~$ sudo config vlan dhcp_relay server_vrf add 1000 Vrf1 Added DHCP relay server vrf Vrf1 for Vlan1000 Restarting DHCP relay service...

config vlan dhcp_relay server_vrf del

The config vlan dhcp_relay server_vrf del command is used to remove the configured DHCP relay server vrf from a VLAN.

Usage
config vlan dhcp_relay server_vrf del <vlan_id>

Example
admin@sonic:~$ sudo config vlan dhcp_relay server_vrf del 1000 Removed DHCP relay server vrf from Vlan1000 Restarting DHCP relay service...

config vlan dhcp_relay server_override add

The config vlan dhcp_relay server_override add command is used to specify the DHCP relay server id override option82 suboption on a VLAN.

Usage
config vlan dhcp_relay server_override add <vlan_id>

Example
admin@sonic:~$ sudo config vlan dhcp_relay server_override add 1000 Enable DHCP relay server override for Vlan1000 Restarting DHCP relay service...

config vlan dhcp_relay server_override del

The config vlan dhcp_relay server_override del command is used to disable DHCP relay server id override option82 suboption on a VLAN.

Usage
config vlan dhcp_relay server_override del <vlan_id>

Example
admin@sonic:~$ sudo config vlan dhcp_relay server_override del 1000 Removed DHCP relay server override from Vlan1000 Restarting DHCP relay service...

17 DHCPv6 Relay

Table of Contents

These commands are used to add or remove DHCPv6 Relay destination IP addresses for VLAN interfaces.

When the DHCPv6 Relay service is enabled, and the switch sees a DHCPv6 client request from an attached host, it inserts its own IP address into the request so that the DHCPv6 server will know the subnet where the client is located. Then, the switch forwards the packet to a DHCPv6 server (destination IP) on another network. When the server receives the DHCPv6 request, it allocates a free IP address for the DHCPv6 client from its defined scope for the DHCPv6 client's subnet, and sends a DHCPv6 response back to the DHCPv6 Relay agent (the switch). The switch then passes the DHCPv6 response received from the server to the client.

DHCPv6 Relay show commands

show dhcprelay_helper ipv6

This command is used to show the config of DHCPv6 Relay.

Usage
show dhcprelay_helper ipv6

Example

```
admin@sonic:~$ show dhcprelay_helper ipv6
 -------- ------------
 Vlan1000  fc02:2000::5
 --------  ------------
```

show dhcpv6_replay counter

This command is used to show the counter of DHCPv6 relay packets

Usage
show dhcp6relay_counters counts

Example

```
admin@sonic:~$ show dhcp6relay_counters counts
  Message Type    Vlan1000
  --------------  ----------
  Unknown          0
  Solicit          2
  Advertise        2
  Request          2
  Confirm          0
  Renew            0
  Rebind           0
```

```
Reply          2
Release        0
Decline        0
Relay-Forward  16
Relay-Reply    4
```

clear dhcpv6_replay counter

This command is used to clear counter of DHCPv6 relay packets

Usage
sudo sonic-clear dhcp6relay_counters

Example

```
admin@sonic:~$ sudo sonic-clear dhcp6relay_counters
admin@sonic:~$ show dhcp6relay_counters counts
  Message Type    Vlan1000
  --------------  ----------
  Unknown          0
  Solicit          0
  Advertise        0
  Request          0
```

```
Confirm          0
Renew            0
Rebind           0
Reply            0
Release          0
Decline          0
Relay-Forward    0
Relay-Reply      0
```

DHCPv6 Relay config commands

config vlan dhcp_relay add

This command is used to add a DHCPv6 Relay Destination IPv6 address to a VLAN.

Usage
config vlan dhcp_relay add <vlan_id> <dhcpv6_relay_destination_ips>

Example
admin@sonic:~$ sudo config vlan dhcp_relay add 1000 fc02:2000::5 Added DHCP relay destination addresses ['fc02:2000::5'] to Vlan1000 Restarting DHCP relay service...

config vlan dhcp_relay delete

This command is used to delete a DHCPv6 Relay Destination IPv6 address.

Usage
config vlan dhcp_relay del <vlan_id> <dhcpv6_relay_destination_ips>

Example
admin@sonic:~$ sudo config vlan dhcp_relay del 1000 fc02:2000::5 Removed DHCP relay destination addresses ['fc02:2000::5'] from Vlan1000 Restarting DHCP relay service...

config sag dhcp_relay add

This command is used to add a DHCPv6 Relay Destination IPv6 address to a SAG.

Usage
config sag dhcp_relay add <sag_id> <dhcpv6_relay_destination_ips>

Example
admin@sonic:~$ sudo config sag dhcp_relay add 1000 fc02:2000::5 Added DHCP relay destination addresses ['fc02:2000::5'] to Sag1000 Restarting DHCP relay service...

config sag dhcp_relay delete

This command is used to delete a DHCPv6 Relay Destination IPv6 address.

Usage
config sag dhcp_relay del <sag_id> <dhcpv6_relay_destination_ips>

Example
admin@sonic:~$ sudo config sag dhcp_relay del 1000 fc02:2000::5 Removed DHCP relay destination addresses ['fc02:2000::5'] from Sag1000 Restarting DHCP relay service...

18 Drop Counters

Table of Contents

This section explains all the configurable drop counters show commands and configuration options that are supported in SONiC.

Drop Counters Show Commands

show dropcounters capabilities

This command is used 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.

Usage
show dropcounters capabilities

Example
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
```

show dropcounters configuration

This command is used to show the current running configuration of the drop counters on this device.

Usage
show dropcounters configuration [-g <group name>]

Example
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
```

show dropcounters counts

This command is used to show the current statistics for the configured drop counters. Standard drop counters are displayed as well for convenience. Because clearing counters (see below) is handled on a per-user basis, different users may see different drop counts.

Usage
show dropcounters counts \[-g <group name>\] \[-t <counter type>\]

Example

```
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
DEVICE  TX_LEGIT
------  --------
sonic      1000
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

Drop Counters Config Commands

config dropcounters install

This command is used to initialize a new drop counter. The user must specify a name, type, and initial list of drop reasons. 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 available counters are already in use on the device.

Usage
config dropcounters install <counter name> <counter type> <reasons list> [-d <description>] [-g <group>] [-a <alias>]

Example
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

config dropcounters add_ reasons

This command is used to add drop reasons to an already initialized counter. This command will fail if any of the specified drop reasons are not supported.

Usage
config dropcounters add_reasons <counter name> <reasons list>

Example
admin@sonic:~$ sudo config dropcounters add_reasons DEBUG_2 \[SIP_CLASS_E\]

config dropcounters remove_reasons

This command is used to remove drop reasons from an already initialized counter.

Usage
config dropcounters remove_reasons <counter name> <reasons list>

Example
admin@sonic:~$ sudo config dropcounters remove_reasons DEBUG_2 \[SIP_CLASS_E\]

config dropcounters delete

This command is used to delete a drop counter.

Usage
config dropcounters delete <counter name>

Example
admin@sonic:~$ sudo config dropcounters delete DEBUG_2

Drop Counters Clear Commands

sonic-clear dropcounters

This command is used to clear drop counters. This is done on a per-user basis.

Usage
sonic-clear dropcounters

Example
admin@sonic:~$ sonic-clear dropcounters Cleared drop counters

Note: Only supports the type PORT_INGRESS_DROPS with two reasons (SMAC_EQUALS_DMAC and EXCEEDS_L3_MTU) on the hardware models uses Broadcom ASIC .

19 Fast Reboot

Fast Reboot Configuration Commands

fast-reboot

Fast-reboot feature enables a switch to reboot up quickly, with minimum disruption to the data plane. It is important for data center networking operation where infrastructure maintenance and upgrade are unavoidable. Fast-reboot is one of the features to minimize traffic impact. This command requires root privilege.

Usage
fast-reboot [options]

Parameters

- -h,-? : get this help
- -v : turn on verbose
- -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

Example
admin@sonic:~$ sudo fast-reboot

20 FDB

Switches store the addresses for all known devices. This information is used to forward traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table or forwarding database (FDB).

FDB Show Commands

show mac

This command displays the MAC (FDB) entries either in full or partial as given below.

1. show mac - displays the full table
2. show mac -v <vlanid> - displays the MACs learnt on the particular VLAN ID.
3. show mac -p <port> - displays the MACs learnt on the particular port.

4. show mac -a <mac_address> - display the MACs that match a specific mac-address
5. show mac -t <type> - display the MACs that match a specific type (static/dynamic/pending)
6. show mac -c - display the count of MAC addresses

Usage
show mac [-v <vlan_id>] [-p <port_name>] [-a <mac_address>] [-t <type>] [-c]

Example

```
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   Pending
 16    1000    DC:2F:D1:08:4B:DE  Ethernet192   Pending
 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
```

Information in table:

- Vlan: The VLAN ID of the MACs
- MacAddress: mac address
- Port: The name of the interface
- Type: The type of the MACs
    - Dynamic: The mac addresses are automatically learned from the source mac field in the ethernet frame.
    - Static: The mac address configured by the "static-fdb add" command.
    - Pending: The mac addresses are automatically learned from the source mac field in the ethernet frame when port access control feature(such as 802.1X) is enabled.

    Traffic is blocked for the MACs before it passes the authentication or remains in this type if authentication is failed.

Optionally, you can specify a VLAN ID or interface name or type or mac-address in order to display only that particular entries

Examples

```
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   Pending
 16   1000   DC:2F:D1:08:4B:DE  Ethernet192   Pending
 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   Pending
 16   1000   DC:2F:D1:08:4B:DE  Ethernet192   Pending
 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 -t Pending
No.    Vlan    MacAddress        Port          Type
-----  ------  -----------------  -----------  -------
  2    1000    AE:DD:67:F3:09:5A  Ethernet192    Pending
  2    1000    DC:2F:D1:08:4B:DE  Ethernet192    Pending
Total number of entries 2
admin@sonic:~$ show mac -c
Total number of entries 18
```

FDB Configuration Commands

sonic-clear fdb

The command is used to clear the MAC address tableT.he command is used for the specified all, vlan, port, and port-vlan.

Usage

sonic-clear fdb <all>|<port>| <vlan_id>|<port-vlan>

Parameter:

- <port>: The name of a physical interface
- <vlan_id>: Vlan ID
- <port-vlan>: The name of a physical interface and Vlan ID
- <all>: All FDB table

Example

```
root@sonic:/home/admin# sonic-clear fdb
Usage: sonic-clear fdb [OPTIONS] COMMAND [ARGS]...

  Clear FDB table

Options:
  -?, -h, --help  Show this message and exit.
```

Commands:

all	Clear All FDB entries
port	Clear FDB entries learned from one PORT
port-vlan	Clear FDB entries learned in one PORT-VLAN
vlan	Clear FDB entries learned in one VLAN

root@sonic:/home/admin# sonic-clear fdb port Ethernet0
Port Ethernet0 FDB entries are cleared.

root@sonic:/home/admin# sonic-clear fdb vlan 100
Vlan100 FDB entries are cleared.

root@sonic:/home/admin# sonic-clear fdb port-vlan Ethernet0 100
Port Ethernet0 + Vlan100 FDB entries are cleared.

root@sonic:/home/admin# sonic-clear fdb all
Dynamic FDB entries are cleared.

config static-mac add

This command shown below is used to add a static mac address on the specified vlan_id and port.

Usage
config static-mac add <mac> <vlan_id> <port>

Parameter:

- <mac>: Static mac address
- <vlan_id>: Vlan ID
- <port>: The name of a physical interface

The example shown below will add a static mac address "00:10:3a:2b:05:67" with vlan 100 on port Etherent2.

Example
root@sonic:/# config static-mac add 00:10:3a:2b:05:67 100 Ethernet2

config static-mac del

This command is used to delete a static mac address on the specified vlan_id.

Usage
config static-mac del [mac] [vlan_id]

Parameter:

- <mac>: Static mac address
- <vlan_id>: Vlan ID

The command shown below will delete a static mac address on vlan 100.

Example
root@sonic:/# config static-mac del 00:10:3a:2b:05:67 100

21 Interfaces

Table of Contents

Table of Contents

Interface Show Commands

This sub-section lists all the possible show commands for the interfaces available in the device. The following example gives a list of possible show commands on interfaces. Subsequent sections explain each of these commands in detail.

Example
admin@sonic:~$ show interfaces -? Usage: show interfaces [OPTIONS] COMMAND [ARGS]... Show details of the network interfaces Options: -?, -h, --help Show this message and exit. Commands: alias Show Interface Name/Alias Mapping autoneg Show interface autoneg information breakout Show Breakout Mode information by interfaces buffer Show interfaces buffer ...

```
counters     Show interface counters
description  Show interface status, protocol and description
diagnostic   Show diagnostic cable test information
fec          Show interface fec information
mpls         Show Interface MPLS status
naming_mode  Show interface naming_mode status
neighbor     Show neighbor related information
pms          Show details of the PMS
portchannel  Show PortChannel information
qos          Show interface qos information
rate-limit
scheduler
status       Show Interface status information
tpid         Show Interface tpid information
transceiver  Show SFP Transceiver information
wred
```

show interfaces alias

Shows the interface name/alias mapping.

Example

```
Name        Alias
----------  -------------
Ethernet0   hundredGigE1
Ethernet4   hundredGigE2
Ethernet8   hundredGigE3
Ethernet12  hundredGigE4
... continue
```

show interfaces arp

Usage
show interfaces arp [INTERFACENAME]

This command display the ARP related configuration information on the interface.

Example
admin@sonic:~$ show interfaces arp Interface Aging(sec) Gratuitous ARP ARP Host Route ---------- ---------- ---------- ---------- Ethernet0 1800 disabled disabled Vlan10 1800 disabled disabled admin@sonic:~$ show interfaces arp Vlan10 Interface Aging(sec) Gratuitous ARP ARP Host Route ---------- ---------- ---------- ---------- Vlan10 1800 disabled disabled

show interfaces autoneg status

Shows the interface auto-negotiation status.

Usage
show interfaces autoneg status show interfaces autoneg status <interface_name>

Example
admin@sonic:~$ show interfaces autoneg status Interface Auto-Neg Mode Oper Speed Adv Speeds Type Adv Types Oper Admin ---------- ---------- ---------- ---------- ------ ---------- ------ ------- Ethernet0 N/A 10G 1000M,10G N/A N/A up up Ethernet1 N/A 10G N/A N/A N/A up up Ethernet2 N/A 10G N/A N/A N/A up up

Ethernet3	N/A	10G	N/A	N/A	N/A	up	up
Ethernet4	N/A	10G	N/A	N/A	N/A	up	up
Ethernet5	N/A	10G	N/A	N/A	N/A	up	up

...

show interfaces breakout

This command displays the port capability for all interfaces, i.e. index, lanes, default break mode (default_brkout_mode), all available breakout modes (breakout_modes), and current breakout mode (brkout_mode). To display the current breakout mode, the "current-mode" subcommand can be used. For a specific interface, provide the <interface name> in the options.

Usage
show interfaces breakout show interfaces breakout current-mode show interfaces breakout current-mode <interface_name>

Example

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 " option is used to display the current breakout mode for all interfaces.

Example (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]            |
 +------------+-----------------------+
```

Example (specific interface)

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

Note:

- breakout_mode: number x speed1 [speed2, speed3]
    - The parent port lanes are split equally to the number of ports denoted by the number. And, the speed for each breakout port defaults to speed1, but is changeable to speed2, speed3 etc.
    - For example: 4x25G[10G] means that all lanes are assigned to one port and are running at 25G by default, but the speed can be changed to 10G later.

show interfaces counters

This show command displays packet counters for all interfaces since the last time the counters were cleared.

Usage
show interfaces counters [-a|--printall] [-p|--period] show interfaces counters errors show interfaces counters rates show interfaces counters rif [-p|--period] [-i <interface_name>]

Options:

- "-a" provides two additional columns - RX-PPS and TX_PPS.
- "-p" specifies the (in seconds) in which to gather counters. period
- "errors" displays the interface error counters.
- "rates" displays only the interface rates.
- "rif" displays Layer 3 counters for a of time or a specific period <interface_name>, which can include router interface, portchannel, and vlan.

Note:

- There is no facility to display counters for one specific Layer 2 interface.
- For RX_BPS and other rate calculations, smoothing is applied. For example, when clearing statistics or experiencing sudden traffic drops, the RX_OK statistics and RX_BPS data may experience temporary desynchronization.

Example (all interfaces)
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
```

Display the error counters only.

Example (error counters)

```
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
```

Display the counters of rates.

Example (rate)

```
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
```

Display the counters of specified interfaces

Example (specific interfaces)

```
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
```

Note: The "-i" option is required when using **show interface counters** and it needs to specify the interface.

Example (rif)

```
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
```

Display the counters of a rif interface.

Example (one interface)

```
admin@sonic:~$ show interfaces counters rif PortChannel0001
PortChannel0001
    RX:
         3269 packets
       778494 bytesq
            3 error packets
          292 error bytes
    TX:
            0 packets
            0 bytes
            0 error packets
            0 error bytes
```

Display the counters for a period of time in seconds.

Example (a period of time)

```
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
```

Example (one interface)

```
admin@sonic:~$ show interfaces counters rif PortChannel0001
PortChannel0001
    RX:
         3269 packets
       778494 bytesq
            3 error packets
          292 error bytes
    TX:
            0 packets
            0 bytes
            0 error packets
            0 error bytes
```

Display the counters for a period of time in seconds.

Example (a period of time)

```
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					

show interfaces description

This command displays the key fields of interfaces, such as Operational Status, Administrative Status, Alias, and Description.

Usage
show interfaces description [<interface_name>]

Example (all interfaces)

```
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
```

Example (a specific interface)

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

Example (a specific interface)

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

show interfaces diagnostic

This command displays information for all the interfaces for the cable TDR(Time Domain Reflectometer) data requested or a specific interface if the optional "interface_name" is specified.

Usage

```
show interfaces diagnostic cable-test [<interface_name>]
```

Example (all interfaces)

```
admin@sonic:~$ show interfaces diagnostic cable-test
Ethernet0: cable (4 pairs, length +/- 10 meters)
      pair A Open, length 0 meters
      pair B Open, length 0 meters
      pair C Open, length 0 meters
      pair D Open, length 0 meters
Ethernet1: cable (4 pairs, length +/- 10 meters)
```

```
    pair A Ok, length 9 meters
    pair B Ok, length 9 meters
    pair C Ok, length 10 meters
    pair D Ok, length 9 meters
Ethernet2: cable (4 pairs, length +/- 10 meters)
    pair A Ok, length 0 meters
    pair B Ok, length 10 meters
    pair C Ok, length 0 meters
    pair D Ok, length 0 meters
Ethernet3: cable (4 pairs, length +/- 10 meters)
    pair A Open, length 0 meters
    pair B Open, length 0 meters
    pair C Open, length 0 meters
    pair D Open, length 0 meters
```

Example (a specific interface)

```
admin@sonic:~$ show interfaces diagnostic cable-test Ethernet12
Ethernet12: cable (4 pairs, length +/- 10 meters)
    pair A Ok, length 9 meters
    pair B Ok, length 9 meters
    pair C Ok, length 9 meters
    pair D Ok, length 5 meters
```

Example (unsupported interface)

```
admin@sonic:~$ show interfaces diagnostic cable-test Ethernet51
Error! could not perform TDR test on Ethernet51
```

show interfaces fec status

This command displays administrative and operational FEC mode mainly and along with the fields such as the operational and administrative status and operational Speed of the interfaces.

Usage
show interfaces fec status show interfaces fec status <interface_name>

Example

admin@sonic:~$ show interface fec status
  Interface Oper Admin FEC Oper FEC Oper Speed
---------- ------ ------- ----- ---------- ------------
  Ethernet0 up up rs rs 100G
  Ethernet8 up up rs rs 100G
 Ethernet16 up up rs rs 100G
 Ethernet24 up up rs rs 100G
 Ethernet32 up up rs rs 100G
 Ethernet40 up up rs rs 100G
 ...

show interfaces link-training status

Use the following command to display the link-training configuration and operational status.

Usage
show interfaces link-training status show interfaces link-training status <interface_name>

Example
admin@sonic:~$ show interfaces link-training status Ethernet0   Interface LT Oper LT Admin Oper Admin ---------- ----------- ---------- ------ -------

Ethernet0 trained on up up

show interfaces neighbor

This command is used to display the list of expected neighbors for all interfaces (or for a particular interface) that is configured.

Usage
show interfaces neighbor expected [<interface_name>]

Example
admin@sonic:~$ show interfaces neighbor expected LocalPort Neighbor NeighborPort NeighborLoopback NeighborMgmt NeighborType ---------- ---------- ---------- ---------- ---------- ---------- Ethernet112 ARISTA01T1 Ethernet1 None 10.16.205.100 ToRRouter Ethernet116 ARISTA02T1 Ethernet1 None 10.16.205.101 SpineRouter Ethernet120 ARISTA03T1 Ethernet1 None 10.16.205.102 LeafRouter Ethernet124 ARISTA04T1 Ethernet1 None 10.16.205.103 LeafRouter

show interface pms status

This command shows the configuration and status of port-mac-security on the entire interface or specified interfaces.

Usage
show interface pms status show interface pms status <interface_name>

Example

```
admin@sonic:~$ show interface pms status
 Interface    PMS Mode    Max Mac Count    Violation Action    Learnt Count    Violation Count
-----------  ---------  --------------  ------------------  --------------  -----------------
  Ethernet0    enabled          1000           Protect            10              N/A
  Ethernet4    enabled          2000           Restrict           2000             10
  Ethernet8    enabled            10           Shutdown            10              N/A
...
admin@sonic:~$ show interface pms status Ethernet0
  Interface    PMS Mode    Max Mac Count    Violation Action    Learnt Count    Violation Count
-----------  ----------  ---------------  ------------------  --------------  -----------------
  Ethernet0    enabled          1000           Protect            10              N/A
```

show interfaces portchannel

This command displays information regarding port-channel interfaces.

Usage

```
show interfaces portchannel
```

Example

```
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)
```

show interfaces status

This command displays some more fields such as Lanes, Speed, MTU, Type, Asymmetric PFC status and also the operational and administrative status of the interfaces.

Usage
show interfaces status [<interface_name>]

Show the status of all interfaces.

Example

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

Show the status of a specific interface.

Example

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

Show the status for a range of interfaces.

Example

```
admin@sonic:~$ show interfaces status Ethernet8,Ethernet168-180
Interface          Lanes    Speed    MTU    Oper FEC         Alias    Oper    Admin    Type    Asym PFC
-------------  ------------  -------  -----  ----------  --------------  ------  -------  ------  ----------
Ethernet8       49,50,51,52    100G    9100       N/A    hundredGigE3    down    down     N/A       N/A
Ethernet168      9,10,11,12    100G    9100       N/A   hundredGigE43    down    down     N/A       N/A
Ethernet172     13,14,15,16    100G    9100       N/A   hundredGigE44    down    down     N/A       N/A
Ethernet176 109,110,111,112    100G    9100       N/A   hundredGigE45    down    down     N/A       N/A
Ethernet180 105,106,107,108    100G    9100       N/A   hundredGigE46    down    down     N/A       N/A
```

intfutil status_ext

This show command displays like , but it also shows extended fields for the specific platforms. show interface status

For the AS8000, which supports PIM hotswap, the extended fields are "PIM slot" and "PIM status".

Example (all interfaces)

```
admin@sonic:~$ intfutil status_ext
  Interface    Lanes    Speed    MTU    FEC          Alias    Vlan    Oper    Admin    Type    Asym PFC
PIM Slot    PIM Status
-----------  -------  -------  -----  -----  ----------------  ------  ------  -------  ------  ----------  ----------  ------------
  Ethernet0      5,6     100G   9100     rs   onehundredGigE0  routed      up      up     N/A       off         2
up
  Ethernet1      7,8     100G   9100     rs   onehundredGigE1  routed      up      up     N/A       off         2
up
  Ethernet2      1,2     100G   9100     rs   onehundredGigE2  routed      up      up     N/A       off         2
up
  Ethernet3      3,4     100G   9100     rs   onehundredGigE3  routed      up      up     N/A       off         2
up
  Ethernet4    37,38     100G   9100     rs   onehundredGigE4  routed      up      up     N/A       off
2          up
  Ethernet5    39,40     100G   9100     rs   onehundredGigE5  routed      up      up     N/A       off
2          up
```

```
 Ethernet6   33,34    100G  9100    rs   onehundredGigE6 routed    up     up   N/A      off
2         up
 Ethernet7   35,36    100G  9100    rs   onehundredGigE7 routed    up     up   N/A      off
2         up
```

show interfaces tpid

This command displays the key fields of the interfaces such as Operational Status, Administrative Status, Alias and TPID.

Usage
show interfaces tpid [<interface_name>]

Display the TPID for all interfaces.

Example (a specific interface)

```
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

Display the TPID for a specific interface.

Example (a specific interface)

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

show storm-control

This command is used to display the current threshold rate and burst size for BUM (broadcast/unknown-multicast/unknown-unicast)

traffic on the physical interface.

Usage

```
show storm-control <command> <args>

show storm-control all

show storm-control interface <interface name>
```

Commands:

- all , Show storm-control settings for all interfaces
- interface , Show storm-control settings for a given interface

  <interface name>, specify interface

Example

```
admin@sonic:~$ show storm-control all
```

```
+----------------+----------------+------------+-----------------+-----------------+
| Interface Name   | Storm Type       |        Cir | Burst Size        |    Meter type     |
+==================+==================+============+=================+=================+
| Ethernet0        | broadcast        |       1000 | 150               |    bytes          |
+----------------+----------------+------------+-----------------+-----------------+
| Ethernet1        | unknown-multicast |       1000 | 150               |    bytes          |
+----------------+----------------+------------+-----------------+-----------------+
| Ethernet2        | unknown-unicast   |       1000 | 150               |    packets        |
+----------------+----------------+------------+-----------------+-----------------+
admin@sonic:~$ show storm-control interface Ethernet1
+----------------+----------------+------------+-----------------+-----------------+
| Interface Name   | Storm Type       |        Cir | Burst Size        |    Meter type     |
+==================+==================+============+=================+=================+
| Ethernet1        | unknown-multicast |       1000 | 150               |    bytes          |
+----------------+----------------+------------+-----------------+-----------------+
```

Interface Clear Counters Commands

sonic-clear clounters

Clear interface counters.

Usage
sonic-clear counters

Example
admin@sonic:~$ sonic-clear counters

sonic-clear rifcounters

Clear Layer 3 interface counters.

Usage
sonic-clear rifcounters

Example (clear rif counters)
admin@sonic:~$ sonic-clear rifcounters

Interface Configuration Commands

Interface configuration commands cover these sub-topics:

- ip - To add or remove an IP address for an interface
- pfc - to set the PFC configuration for an interface
- shutdown - to administratively shut down an interface
- speed - to set the interface speed
- startup - to bring up an administratively shutdown interface
- breakout - to set an interface breakout mode
- tpid - to set interface tpid
- pms - to set the port mac security for an interface

config interface ip add

Configure interface IP address. Add the IP address for an interface.

Usage
config interface ip add <interface_name> <ip_addr> [default_gw]

Note:

- The IP address for a physical interface, portchannel, VLAN interface, or Loopback interface, can all be configured with this command.
- While configuring the IP address for the management interface "eth0", users can provide the default gateway IP address as an optional parameter.
- <interface_name>
    - interface VLAN: use "vlan<vlan-id>". For example, "vlan100: for VLAN-100.

Example (Configure interface on port)
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

Example (Configure interface on vlan)
admin@sonic:~$ sudo config interface ip add vlan100 10.11.12.13/24

config interface remove

Remove an IP address from an interface.

Usage
config interface ip remove <interface_name> <ip_addr>

Example (Remove IP address from an interface - port)
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

Example (Remove IP address from an interface - vlan)
admin@sonic:~$ sudo config interface ip remove vlan100 10.11.12.13/24

config interface ip add/remove --secondary

Since SONiC 202006 Dec. version, the IPv4 addresses for an interface are classified as the primary address and secondary. There is no primary/secondary classification for IPv6 addresses.

The principles are:

- There is only one primary address for an interface. Other addresses should be specified as secondary.
- The first added address SHOULD be the primary address. The secondary address SHOULD be added after the primary one.
- The command syntax for the addition of a primary address is like the original syntax. The syntax for addition of a secondary address is as follows:
- The primary address SHOULD be the last address to be removed from an interface. In order to remove the primary address, you must remove all secondary addresses first.
- The command syntax for the removal of a primary address is like the original syntax. The syntax for the removal of a secondary address is as follows:

Usage (Remove a secondary IPv4 address)
config interface <interface_name> ip remove <ip_addr> --secondary

config interface link-training

Once configured, use Use the following command to enable or disable link-training at a interface when auto-negotiation is disabled. show interfaces link-training status to check the status.

Usage
Format:

config interface link-training <interface_name> <mode> Arguments: interface_name: [mandatory] name of the interface to be configured. e.g: Ethernet0 mode: [mandatory] link training mode, can be either "on" or "off" Return: - error message if interface_name or mode is invalid - empty upon success

Example
admin@sonic:~$ sudo config interface link-training Ethernet0 on admin@sonic:~$ sudo config interface link-training Ethernet8 off

config interface pfc priority

This command is used to set PFC to a given priority on a given interface to either "on" or "off". Once successfully configured, it will show current loss priorities on the given interface. Otherwise, it will show error information.

Usage
config interface pfc priority <interface_name> <priority> (on | off)

Paramters:

<priority> - range in (0..7)

Example
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

config interface pfc asymmetric

This command is used for setting the asymmetric PFC for an interface to either "on" or "off". Once it is configured, use show interfaces status to check the status.

Usage
config interface pfc asymmetric <interface_name> (on | off)

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

config interface shutdown

This command is used to administratively shut down either a physical interface or a port-channel interface. Once configured, use show interfaces status to check the status. interfaces status

Usage
config interface shutdown <interface_name>

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

Example (shutdown multi-interfaces)
admin@sonic:~$ sudo config interface shutdown Ethernet8,Ethernet16-20,Ethernet32

config interface startup

This command is used for administratively bringing up a physical interface or a port-channel interface. Once configured, use show interfaces status to check the status.

Usage
config interface startup <interface_name>

Example

admin@sonic:~$ sudo config interface startup Ethernet63

Example (startup multi-interfaces)
admin@sonic:~$ sudo config interface startup Ethernet8,Ethernet16-20,Ethernet32

config interface speed

This command is used to configure the speed for a physical interface.

The supported speed list can be changed by breakout-mode. Use show interfaces breakout to see the current breakout-mode for the supported speed.

Usage
config interface speed <interface_name> <speed_value>

Parameters:

- <speed_value>, user needs to know the interface configurable speeds
    - 40000 for 40G
    - 100000 for 100G

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

Note:

- breakout_mode: number x speed1 [speed2, speed3]
    - The parent port lanes are split equally to the number of ports denoted by the number. And, the speed for each breakout port defaults to speed1, but is changeable to speed2, speed3 etc.

- For example: 1x100G[40G] means all lanes are assigned to one port and are running at 100G by default, but the speed can be changed to 40G later.

config interface mtu

This command is used to configure the MTU for a physical interface.

The MTU (Maximum Transmission Unit) size range is from 1500 to 9216 bytes. The user-configured value will add 22 bytes and be set to the chip.

Usage
config interface mtu <interface_name> <mtu_value>

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

config interface breakout

This command is used to set an available breakout mode for a user-specified interface.

Use a double tab (i.e. <tab><tab>) to see the available breakout options customized for each interface specified by the user.

Usage
config interface breakout [OPTIONS] <interface_name> <breakout_mode>

Options:

-f, --force-remove-dependencies

Clear all depenedecies internally first.

-l, --load-predefined-config

load predefined user configuration (alias, lanes, speed etc) first.

-y, --yes

-v, --verbose

Enable verbose output

-?, -h, --help

Show this message and exit.

Note:

- breakout_mode: number x speed1 [speed2, speed3]
    - The parent port lanes are split equally to the number of ports denoted by the number. And, the speed for each breakout port defaults to speed1, but is changeable to speed2, speed3 etc.
    - For example: 1x100G[40G] means that all lanes are assigned to one port and running at 100G by default, but the speed can be changed to 40G later.
    - Use show interface breakout to see the supported breakout mode.
- The new breakout ports are created by the default configuration, but you can predefine the port configuration by the option "--load-predefined-config". The file name of the predefined configuration must be "port_breakout_config_db.json" and the file must be placed in the directory /etc/sonic/.
- If the breakout_mode includes parentheses ( ), please add single quotes " for the bash parser. For example: config interface breakout Ethernet0 '1x100G[40G](4)'

Example
admin@sonic:~$ sudo config interface breakout Ethernet0 <tab><tab> <tab provides option for breakout mode> 1x100G[40G] 2x50G 4x25G[10G]

```
admin@sonic:~$ sudo config interface breakout Ethernet48 4x25G -f -l -v -y
Running Breakout Mode : 1x100G[40G]
Target Breakout Mode : 4x25G
Ports to be deleted :
 {
    "Ethernet48": "100000"
}
Ports to be added :
 {
    "Ethernet50": "25000",
    "Ethernet51": "25000",
    "Ethernet49": "25000",
    "Ethernet48": "25000"
}
After running Logic to limit the impact
Final list of ports to be deleted :
 {
    "Ethernet48": "100000"
}
Final list of ports to be added :
 {
    "Ethernet50": "25000",
    "Ethernet51": "25000",
    "Ethernet49": "25000",
    "Ethernet48": "25000"
}
Loaded below Yang Models
['sonic-acl', 'sonic-extension', 'sonic-interface', 'sonic-loopback-interface', 'sonic-port', 'sonic-
portchannel', 'sonic-types', 'sonic-vlan']
Note: Below table(s) have no YANG models:
TACPLUS_SERVER, DEVICE_METADATA, BGP_PEER_RANGE, PORTCHANNEL_MEMBER,
FLEX_COUNTER_TABLE, SYSLOG_SERVER, CRM,
CONTAINER_FEATURE, BGP_NEIGHBOR, PORTCHANNEL_INTERFACE, MGMT_INTERFACE,
NTP_SERVER,
```

DEVICE_NEIGHBOR_METADATA, TELEMETRY, DEVICE_NEIGHBOR, FEATURE, BREAKOUT_CFG, DHCP_SERVER, MGMT_PORT, RESTAPI, VERSIONS, BUFFER_POOL, BUFFER_PROFILE, Breakout process got successfully completed. Please note loaded setting will be lost after system reboot. To preserve setting, run `config save`.

config interface storm-control

This command is used to add the rate and burst size for BUM (broadcast/unknown-multicast/unknown-unicast) traffic, or to threshold delete the previous setting on the physical interface.

All types of storm traffic can be configured on the interface at the same time.

Usage
config interface storm-control <storm_type> add <port_name> <meter_type> <cir> <burst size> config interface storm-control <storm_type> del <port_name>

Parameters:

- <storm_type>: There are three types to choose from:
  - broadcast, configure broadcast storm control.
  - unknown multicast, configure unknown multicast storm control.
  - unknown unicast, configure unknown unicast storm control.
- <port_name>, specifies the interface, can only be a physical interface.
- <meter type>,select the rate limiting type bytes or packets.
- <cir>, traffic speed limit value, in kbps. When equal to 0, all the configured traffic will drop.
- <burst size>, optional. If<burst size>is not specified, when the meter type is bytes, the burst size of the TD3 device is 10 times the MTU of the application interface. Other devices are 1% of the cir, and when the meter type is packets, the burst size is ten times that of the cir.

Example
admin@sonic:~$ sudo config interface storm-control broadcast add Ethernet0 bytes 1000 add broadcast storm-control admin@sonic:~$ sudo config interface storm-control unknown-multicast add bytes Ethernet0 100000 750 add unknown-multicast storm-control

```
admin@sonic:~$ sudo config interface storm-control unknown-unicast add Ethernet0 bytes 50000 150
add unknown-unicast storm-control
admin@sonic:~$ show storm-control all
+----------------+-----------------+-------------+------------------+-------------------+
| Interface Name   | Storm Type      |        Cir  | Burst Size       | Meter type        |
+================+=================+=============+==================+===================+
| Ethernet0      | broadcast       |        1000 | 10               | bytes             |
+----------------+-----------------+-------------+------------------+-------------------+
| Ethernet0      | unknown-multicast |      100000 | 750              | bytes             |
+----------------+-----------------+-------------+------------------+-------------------+
| Ethernet0      | unknown-unicast   |       50000 | 150              | bytes             |
+----------------+-----------------+-------------+------------------+-------------------+
admin@sonic:~$ sudo config interface storm-control broadcast del Ethernet0
del broadcast storm-control
admin@sonic:~$ show storm-control all
+----------------+-----------------+-------------+------------------+-------------------+
| Interface Name   | Storm Type      |        Cir  | Burst Size       | Meter type        |
+================+=================+=============+==================+===================+
| Ethernet0      | unknown-multicast |      100000 | 750              | bytes             |
+----------------+-----------------+-------------+------------------+-------------------+
| Ethernet0      | unknown-unicast   |       50000 | 150              | bytes             |
+----------------+-----------------+-------------+------------------+-------------------+
```

config interface autoneg

This command enables (or disables) the interface auto-negotiation. The referred speed in negotiation is specified in the config interface advertised-speeds command. The referred interface type in negotiation is specified in the config interface advertised-types command.

Usage
config interface autonego <interface> { enabled | disabled }

Note,

- There are 3 kinds of IEEE standard to support autonego. The first one is IEEE 802.3 Clause 28, which is applicable to RJ-45 port to support BASE-T PHYs like 1000Base-T. The second is IEEE 802.3 Clause 37, which is applicable to 1000Base-X.The other one is IEEE 802.3by Clause 73, which is applicable to the port that plugged a DAC cable. Note that IEEE 802.3by Clause 73 is not applicable to the port that plugged an optical transceiver. Enable the autonego on the port which is not applicable to support autonego will cause the unpredictable result and the port may not work correctly.
- When auto-negotiation is enabled, the interface speed is negotiated, which refers to the speed list specified by the config interface advertised-speed command.
- When auto-negotiation is enabled, the interface type is negotiated, which refers to the speed list specified by the config interface advertised-types command.
- When auto-negotiation is disabled, the interface is forced to the speed specified in by the config interface speed command.

This is an example to enable (or disable) auto-negotiation on interface Ethernet0.

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

config interface advertised-speeds

This command specifies a collection of speeds that are available as a linked speed after auto-negotiation. The configuration does not take effect if the interface has not been enabled for auto-negotiation using the command config interface autonego . The change to the advertised speed list takes effect immediately if the interface has auto-negotiation enabled.

Usage
config interface advertised-speeds <interface> { all | <speed-list> }

Parameters:

<interface>

the interface that applies the auto-negotiation advertised speeds.

option, user needs to specify one of the following:

all, set all the advertised-speeds that the interface can support. (default)

<speed list>, speed collection that the user wants to use in auto-negotiation.

Note:

- A user-configured speed may not be the linked speed if the peer cannot support it. For example, a user specifies 100M, 1G, and 10G in <speed list>, and then mis-configures the peer interface for 1G and 10G when it only supports 100M. The port will enter a link down state since there is no proper speed for both ends.
- The whole speed list is not accepted if it contains an invalid speed in the list.
- All advertised speeds are replaced if a user specifies a new set of speeds, even if auto-negotiation is enabled.
- When setting a new speed list, all speeds in the speed list will be examined by the following check order:
    - Supported speed check: Not supported speed in speed list
    - Supported adv-speed check: Not supported adv-speed in speed list

The following example configures an interface (Ethernet0) with a speed list (100M, 1G, 2.5G) or all. After this command, you need to use the config interface autonego Ethernet0 enable command to enable port auto-negotiation.

Example

admin@sonic:~$ sudo config interface advertised-speeds Ethernet0 100,1000,2500 admin@sonic:~$ sudo config interface advertised-speeds Ethernet0 all

Example (Not supported speed in speed list)
admin@sonic:~$ sudo config interface advertised-speeds Ethernet0 10,100000 Invalid speed specified: 10,100000 Valid speeds:1000,10000

Example (Not supported adv-speed in speed list)
admin@sonic:~$ config interface advertised-speeds Ethernet0 1000 Invalid adv-speed specified: 1000 Valid adv-speeds:10000

config interface advertised-types

This command specifies a collection of interface types that are available as a linked type after auto-negotiation. The configuration does not take effect if the interface has not been enabled for auto-negotiation using the command config interface autonego . The change to the type list takes effect immediately if the interface has auto-negotiation enabled.

Usage
config interface advertised-types <interface> { all | <interface_type> }

Parameters:

<interface>

the interface that applies the auto-negotiation interface types

option, user needs to specify one of the following:

all, set all the advertised-types that the interface can support. (default)

<interface type>, interface type collection that the user wants to use in auto-negotiation(KR, KR2, KR4, KR8, CR, CR2, CR4, CR8, and so on).

Note:

The setting is only applicable to IEEE 802.3by Clause73, which means, only applicable to the port that plugged a DAC cable.

The following example configures an interface (Ethernet0) with a interface type list (CR4, KR4) or all. After this command, you need to use the config interface autonego Ethernet0 enable command to enable port auto-negotiation.

Example
admin@sonic:~$ sudo config interface advertised-types Ethernet0 CR4,KR4 admin@sonic:~$ sudo config interface advertised-types Ethernet0 all

config interface type (not supportted)

Configuring interface type takes effect only if auto negotiation is disabled. If auto negotiation is enabled, this command still saves interface type value to CONFIG_DB.

Usage
config interface type <interface> <interface_type>

Parameters:

<interface> the interface that applies the auto-negotiation interface types

<interface type>, interface type, valid value include CR4, KR4, and son on.

Note:

This configuration is only applicable to the port, which is a SFP or QSFP form factor port.

The following example configures an interface (Ethernet0) with a interface type CR4.

Example
admin@sonic:~$ sudo config interface type Ethernet0 CR4 admin@sonic:~$ sudo config interface type Ethernet4 KR4

config interface tpid

This command is used to configure the TPID for the Physical/PortChannel interface. default is 0x8100. Other allowed values if supported by HW SKU (0x9100, 0x9200, 0x88A8).

Usage
config interface tpid <interface_name> <tpid_value>

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

config interface pms <interface_name> enabled

This command enables the interface port-mac-security.

Usage

config interface pms <interface_name> enabled

Parameters:

<interface_name>: Physical interface name.

Note:

- The MAC addresses will be flushed when enabling port-mac-security.
- If the max-mac-count is not configured, the default number of MAC address can access the network through this interface will be 1 .
- If the violation-action is not configured, the default action is "protect " when the violation is occurred.

Example
admin@sonic:~$ sudo config interface pms Ethernet0 enabled

config interface pms <interface_name> disabled

This command disables the interface port-mac-security.

Usage
config interface pms <interface_name> disabled

Parameters:

<interface_name>: Physical interface name.

Note:

The MAC addresses will not be flushed when disabling port-mac-security .

If the admin state of port is down due to a violation, this command can be used to remove the violated state from the port.

Example
admin@sonic:~$ sudo config interface pms Ethernet0 disabled

config interface pms <interface_name> max-mac-count

This command specifies the maximum number of allowed MAC addresses after port-mac-security enabled.

Usage
config interface pms <interface_name> max-mac-count <value>

Parameters:

<interface_name>: Physical interface name.

<value>: maximum number of allowed MAC addresses. Minimum: 1. Maximum: 4097.

Note:

The default maximum number of allowed MAC addresses is 1 if this configuration is not set.

Example
admin@sonic:~$ sudo config interface pms Ethernet0 max-mac-count 1000

config interface pms <interface_name> violation-action

This command specifies the action to be taken when more than the allowed number of MAC addresses is attempted to be learnt on the port.

Usage

config interface pms <interface_name> violation-action { protect | restrict | shutdown }

Parameters:

<interface_name>: Physical interface name.

violation-action:

protect: The violating packets are dropped.

restrict: The violating packets are dropped, and a violation counter is incremented for each violation.

shutdown: The port is administratively shut down.

Note:

The default action is "protect" if this configuration is not set.

If a shutdown action is taken on the port, "config interface pms <interface_name> disabled" can be used to remove the violated state.

Example
admin@sonic:~$ sudo config interface pms Ethernet0 violation-action protect

config interface description

This command is used to configure the description for the Physical interface or Port channel.

Usage
config interface description <interface_name> <interface_description>

Example
admin@sonic:~$ sudo config interface description Ethernet0 Eth1/1

Interface Naming Mode

show interfaces naming_mode

This command displays the current interface naming mode.

Usage
show interfaces naming_mode

Note:

default, display all SONiC interface names in show commands and accept SONiC interface names as parameters in config commands.

alias, display all hardware vendor interface aliases in show commands and accept hardware vendor interface aliases as parameters in config commands.

Interface naming mode originally set to 'default'. Interfaces are referenced by default SONiC interface names. Users can change the naming_mode using the config interface_naming_mode command.

Example
admin@sonic:~$ show interfaces naming_mode alias admin@sonic:~$ show interfaces naming_mode default

config interface_naming_mode

This command is used to change the interface naming mode.

Users can select between the default mode (SONiC interface names) or alias mode (Hardware vendor names).

The user must log out and log back in for the changes to take effect. Note that the newly-applied interface mode will affect all interface-related show/config commands.

Note: Some platforms do not support alias mapping. In such cases, this command is not applicable. Such platforms always use the same SONiC interface names.

Usage
config interface_naming_mode (default | alias)

Note: Interface naming mode is originally set to 'default'. Interfaces are referenced by default SONiC interface names.

Example
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 the user logs out and logs in again, the interfaces are referred to by the hardware vendor alias.

Example
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
```

Interface VRF Binding Commands

By default, all L3 interfaces are bound to the default VRF. Use the config interface vrf bind command to bind to different VRFs.

config interface vrf bind

This command is used to bind an interface to a non default VRF.

Usage
config interface vrf bind <interface_name> <vrf_name>

Example
admin@sonic:~$ show vrf VRF   Interfaces ----- ------------ admin@sonic:~$ config vrf add Vrf1 admin@sonic:~$ show vrf VRF   Interfaces ----- ------------ Vrf1 admin@sonic:~$ config interface vrf bind PortChannel0001 Vrf1 admin@sonic:~$

```
admin@sonic:~$
admin@sonic:~$ show vrf
VRF    Interfaces
-----  ---------------
Vrf1   PortChannel0001
```

config interface vrf unbind

Unbind an interface from a non-default VRF.

Usage
config interface vrf unbind <interface_name>

Example
admin@sonic:~$ config interface vrf unbind PortChannel0001 admin@sonic:~$ admin@sonic:~$ show vrf VRF   Interfaces ----- ------------ Vrf1

Transceiver Config and Show Commands

This chapter introduces the display of optical module information and configuration instructions.

show interfaces transceiver

Usage

```
show interfaces transceiver [OPTIONS] COMMAND [ARGS]...
  Show SFP Transceiver information
Options:
  -?, -h, --help  Show this message and exit.
Commands:
  eeprom    Show interface transceiver EEPROM information
  error-status  Show transceiver error-status
  frequency     Show interface transceiver frequency
  lpmode    Show interface transceiver low-power mode status
  presence  Show interface transceiver presence
```

show interfaces transceiver eeprom

Show interface transceiver EEPROM information.

Usage
show interfaces transceiver eeprom [-d|--dom] [<interface_name>]

Parameters:

"-d" or "-- dom" display DOM (Diginal Optics Monitoring) information

<interface_name> display specific interface transceiver information

Note: Without "-d", this command shows DOM capacity.

Example (eeprom info)
admin@sonic:~$ show interfaces transceiver eeprom Ethernet0: SFP EEPROM detected Application Advertisement: N/A Connector: MPOx12

```
        DOM Capability:
            Rx_power_support: True
            Temp_support: False
            Tx_power_support: True
            Voltage_support: False
        Encoding: 256B257B
        Extended Identifier: Power Class 3(2.5W max), CDR present in Rx Tx
        Extended RateSelect Compliance: QSFP+ Rate Select Version 1
        Identifier: QSFP28 or later
        Length Cable Assembly(m): 50
        Nominal Bit Rate(100Mbs): 255
        Specification compliance:
            Extended Specification compliance: 100GBASE-SR4 or 25GBASE-SR
            Fibre Channel Speed: 100 Mbytes/Sec
        Vendor Date Code(YYYY-MM-DD Lot): 2018-09-14
        Vendor Name: Edgecore
        Vendor OUI: 70-72-cf
        Vendor PN: ET7402-SR4
        Vendor Rev: 01
        Vendor SN: J11837006041
Ethernet240: SFP EEPROM detected
        Application Advertisement: N/A
        Connector: MPOx12
        DOM Capability:
            Rx_power_support: True
            Temp_support: False
            Tx_power_support: True
            Voltage_support: False
        Encoding: 256B257B
        Extended Identifier: Power Class 3(2.5W max), CDR present in Rx Tx
        Extended RateSelect Compliance: QSFP+ Rate Select Version 1
        Identifier: QSFP28 or later
... continue
```

Example (ZR transceiver with dom option)

```
root@sonic:/home/admin# show interfaces transceiver eeprom --dom
Ethernet160: SFP EEPROM detected
        Active App Selection Host Lane 1: 1
        Active App Selection Host Lane 2: 1
        Active App Selection Host Lane 3: 1
        Active App Selection Host Lane 4: 1
        Active App Selection Host Lane 5: 1
        Active App Selection Host Lane 6: 1
        Active App Selection Host Lane 7: 1
        Active App Selection Host Lane 8: 1
        Active Firmware Version: 1.3
        Application Advertisement:
                1: 400GAUI-8 C2M (Annex 120E) | 400ZR, DWDM, amplified
                2: 100GAUI-2 C2M (Annex 135G) | 400ZR, DWDM, amplified
        CMIS Revision: 4.1
        Connector: LC
        Encoding: N/A
        Extended Identifier: Power Class 8 (19.0W Max)
        Extended RateSelect Compliance: N/A
        Hardware Revision: 1.1
        Host Electrical Interface: 400GAUI-8 C2M (Annex 120E)
        Host Lane Assignment Options: 1
        Host Lane Count: 8
        Identifier: QSFP-DD Double Density 8X Pluggable Transceiver
        Inactive Firmware Version: 1.3
        Length Cable Assembly(m): 0.0
        Media Interface Code: 400ZR, DWDM, amplified
        Media Interface Technology: 1550 nm DFB
        Media Lane Assignment Options: 1
        Media Lane Count: 1
        Nominal Bit Rate(100Mbs): 0
        Specification compliance: sm_media_interface
```

Supported Max Laser Frequency: 196100GHz

Supported Max TX Power: -9.0dBm

Supported Min Laser Frequency: 191300GHz

Supported Min TX Power: -14.0dBm

Vendor Date Code(YYYY-MM-DD Lot): 2022-03-28

Vendor Name: MOLEX

Vendor OUI: 00-09-3a

Vendor PN: 1837240006

Vendor Rev: 10

Vendor SN: Z22120BU5

ChannelMonitorValues:

RX1Power: -40.0dBm

RX2Power: -40.0dBm

RX3Power: -40.0dBm

RX4Power: -40.0dBm

RX5Power: -40.0dBm

RX6Power: -40.0dBm

RX7Power: -40.0dBm

RX8Power: -40.0dBm

TX1Power: -40.0dBm

TX2Power: -40.0dBm

TX3Power: -40.0dBm

TX4Power: -40.0dBm

TX5Power: -40.0dBm

TX6Power: -40.0dBm

TX7Power: -40.0dBm

TX8Power: -40.0dBm

ChannelThresholdValues:

RxPowerHighAlarm : 6.0dBm

RxPowerHighWarning: 3.0dBm

RxPowerLowAlarm : -16.003dBm

RxPowerLowWarning : -14.001dBm

TxBiasHighAlarm : 0.0mA

TxBiasHighWarning : 0.0mA

```
            TxBiasLowAlarm    : 0.0mA
            TxBiasLowWarning  : 0.0mA
            TxPowerHighAlarm  : -2.0dBm
            TxPowerHighWarning: -4.0dBm
            TxPowerLowAlarm   : -13.002dBm
            TxPowerLowWarning : -12.007dBm
        ModuleMonitorValues:
            Temperature: 31.941C
            Vcc: 3.353Volts
        ModuleThresholdValues:
            TempHighAlarm  : 80.0C
            TempHighWarning: 75.0C
            TempLowAlarm   : -6.0C
            TempLowWarning : -3.0C
            VccHighAlarm   : 3.7Volts
            VccHighWarning : 3.6Volts
            VccLowAlarm    : 3.0Volts
            VccLowWarning  : 3.05Volts
Ethernet192: SFP EEPROM detected
        Application Advertisement: N/A
        Connector: MPO 1x12
        DOM Capability:
            Rx_power_support: True
            Temp_support: True
            Tx_power_support: True
            Voltage_support: True

... continue
```

show interfaces transceiver vdm

Show interface transceiver versatile diagnostics monitoring for QSFP-DD.

Example

```
root@sonic:/# show interfaces transceiver vdm Ethernet504
Ethernet504:
   Parameter              Unit   Value       Threshold          Threshold
Threshold    Threshold    Threshold    Threshold
                                    High               High
Crossing     Low          Low          Crossing
                                    Alarm              Warning          Alert-High   Alarm      Warning
Alert-Low
   ---------------------- ------ ---------- ------------------- ------------------ ---------- ---------- ---------- ----------
   Laser Tempratur        C      52.31640625  90.0               85.0             False      5.0
8.0          False
   Laser Age              %      0.0          95.0               90.0             False      0.0          0.0
False
   Tx Power               dBm    -8.21        -2.0               -4.0             False      -17.0        -16.0
False
   Rx Total Power         dBm    -40.0        6.0                3.0              False      -22.0        -
20.0         True
   Rx Signal Power        dBm    -40.0        4.0                2.0              False      -22.0        -
20.0         True
   CD-short link          ps/nm  0.0          2400.0             2280.0           False      0.0
0.0          False
   CD-long link           ps/nm  0.0          50000.0            42500.0          False      -655360.0
-655360.0    False
   PDL                    dB     0.0          3.5                3.0              False      0.0          0.0
False
   OSNR                   dB     0.0          256.0              256.0            False      14.0         16.0
True
   eSNR                   dB     0.0          256.0              256.0            False      0.0          0.0
False
   CFO                    MHz    0.0          3000.0             2000.0           False      -3000.0      -
2000.0       False
   DGD                    ps     0.0          220.0              200.0            False      0.0          0.0
False
   Pre-FEC BER Current Media  N/A    1.0          0.02               0.018000000000000002  True
0.0          0.0          False
```

```
   Post-FEC BER Current Media  N/A     1.0         1.0                 2.0              False       0.0
0.0         False
   Pre-FEC BER Current Host    N/A     1.0         1.0                 2.0              False       0.0
0.0         False
   Post-FEC BER Current Host   N/A     1.0         1.0000000000000002e-06  1e-08            True
0.0         0.0         False
   MER                 dB      N/A         N/A                 N/A              N/A         N/A         N/A
N/A
```

show interfaces transceiver pm

Show interface transceiver platform monitoring for ZR.

Example

```
root@sonic:/# show interfaces transceiver pm Ethernet240
Ethernet240:
   Parameter       Unit    Min     Avg     Max     Threshold       Threshold       Threshold       Threshold
Threshold       Threshold
                                                                   High            High            Crossing        Low             Low             Crossing
                                                                   Alarm           Warning         Alert-High      Alarm           Warning         Alert-Low
   --------------  ------  ------  ------  -----  -------------  -------------  ------------  -----------  -----------  -----------
   Tx Power        dBm     -8.18   -8.17   -8.16  0.0            -2.0           False         -18.013      -16.003
False
   Rx Total Power  dBm     -64.04  -43.76  -40.0  13.0           10.0           False         -21.0        -18.0
True
   Rx Signal Power  dBm    -40.0   -40.0   -40.0  13.0           10.0           False         -21.0        -18.0
True
   CD-short link   ps/nm   0.0     0.0     0.0    -1.0           -1.0           True          0.0          0.0          False
   PDL             dB      0.0     0.0     0.0    6553.5         6553.5         False         0.0          0.0          False
   OSNR            dB      0.0     0.0     0.0    6553.5         6553.5         False         0.0          0.0          False
   eSNR            dB      0.0     0.0     0.0    6553.5         6553.5         False         0.0          0.0          False
   CFO             MHz     0.0     0.0     0.0    -1.0           -1.0           True          0.0          0.0          False
   DGD             ps      0.0     0.0     0.0    655.35         655.35         False         0.0          0.0          False
```

SOPMD	ps^2	0.0	0.0	0.0	655.35	655.35	False	0.0	0.0	False
SOP ROC	krad/s	0.0	0.0	0.0	N/A	N/A	N/A	N/A	N/A	N/A
Pre-FEC BER	N/A	1.0	1.0	1.0	0.00999	0.008	True	0.0	0.0	False
Post-FEC BER	N/A	0.0	0.0	0.0	20470000000.0	20470000000.0	False	0.0	0.0	False
EVM	%	0.0	0.0	0.0	N/A	N/A	N/A	N/A	N/A	

show interfaces transceiver status

Show interface transceiver status for QSFP-DD.

Example

```
root@sonic:/home/admin# show interfaces transceiver status Ethernet240
Ethernet240:
        Tx fault flag on media lane 1: False
        Tx fault flag on media lane 2: False
        Tx fault flag on media lane 3: False
        Tx fault flag on media lane 4: False
        Tx fault flag on media lane 5: False
        Tx fault flag on media lane 6: False
        Tx fault flag on media lane 7: False
        Tx fault flag on media lane 8: False
        Rx loss of signal flag on media lane 1: True
        Rx loss of signal flag on media lane 2: False
        Rx loss of signal flag on media lane 3: False
        Rx loss of signal flag on media lane 4: False
        Rx loss of signal flag on media lane 5: False
        Rx loss of signal flag on media lane 6: False
        Rx loss of signal flag on media lane 7: False
        Rx loss of signal flag on media lane 8: False
        Current module state: ModuleReady
```

Reason of entering the module fault state: No Fault detected

Datapath firmware fault: False

Module firmware fault: False

Module state changed: False

Data path state indicator on host lane 1: DataPathActivated

Data path state indicator on host lane 2: DataPathActivated

Data path state indicator on host lane 3: DataPathActivated

Data path state indicator on host lane 4: DataPathActivated

Data path state indicator on host lane 5: DataPathActivated

Data path state indicator on host lane 6: DataPathActivated

Data path state indicator on host lane 7: DataPathActivated

Data path state indicator on host lane 8: DataPathActivated

Tx output status on media lane 1: False

Tx output status on media lane 2: False

Tx output status on media lane 3: False

Tx output status on media lane 4: False

Tx output status on media lane 5: False

Tx output status on media lane 6: False

Tx output status on media lane 7: False

Tx output status on media lane 8: False

Rx output status on host lane 1: False

Rx output status on host lane 2: False

Rx output status on host lane 3: False

Rx output status on host lane 4: False

Rx output status on host lane 5: False

Rx output status on host lane 6: False

Rx output status on host lane 7: False

Rx output status on host lane 8: False

Tx loss of signal flag on host lane 1: True

Tx loss of signal flag on host lane 2: True

Tx loss of signal flag on host lane 3: True

Tx loss of signal flag on host lane 4: True

Tx loss of signal flag on host lane 5: True

Tx loss of signal flag on host lane 6: True

Tx loss of signal flag on host lane 7: True

Tx loss of signal flag on host lane 8: True

Tx clock and data recovery loss of lock on host lane 1: True

Tx clock and data recovery loss of lock on host lane 2: True

Tx clock and data recovery loss of lock on host lane 3: True

Tx clock and data recovery loss of lock on host lane 4: True

Tx clock and data recovery loss of lock on host lane 5: True

Tx clock and data recovery loss of lock on host lane 6: True

Tx clock and data recovery loss of lock on host lane 7: True

Tx clock and data recovery loss of lock on host lane 8: True

Rx clock and data recovery loss of lock on media lane 1: True

Rx clock and data recovery loss of lock on media lane 2: False

Rx clock and data recovery loss of lock on media lane 3: False

Rx clock and data recovery loss of lock on media lane 4: False

Rx clock and data recovery loss of lock on media lane 5: False

Rx clock and data recovery loss of lock on media lane 6: False

Rx clock and data recovery loss of lock on media lane 7: False

Rx clock and data recovery loss of lock on media lane 8: False

Configuration status for the data path of host line 1: ConfigUndefined

Configuration status for the data path of host line 2: ConfigUndefined

Configuration status for the data path of host line 3: ConfigUndefined

Configuration status for the data path of host line 4: ConfigUndefined

Configuration status for the data path of host line 5: ConfigUndefined

Configuration status for the data path of host line 6: ConfigUndefined

Configuration status for the data path of host line 7: ConfigUndefined

Configuration status for the data path of host line 8: ConfigUndefined

Data path configuration updated on host lane 1: False

Data path configuration updated on host lane 2: False

Data path configuration updated on host lane 3: False

Data path configuration updated on host lane 4: False

Data path configuration updated on host lane 5: False

Data path configuration updated on host lane 6: False

Data path configuration updated on host lane 7: False

Data path configuration updated on host lane 8: False

Temperature high alarm flag: False
Temperature high warning flag: False
Temperature low warning flag: False
Temperature low alarm flag: False
Vcc high alarm flag: False
Vcc high warning flag: False
Vcc low warning flag: False
Vcc low alarm flag: False
Tx power high alarm flag on lane 1: False
Tx power high alarm flag on lane 2: False
Tx power high alarm flag on lane 3: False
Tx power high alarm flag on lane 4: False
Tx power high alarm flag on lane 5: False
Tx power high alarm flag on lane 6: False
Tx power high alarm flag on lane 7: False
Tx power high alarm flag on lane 8: False
Tx power high warning flag on lane 1: False
Tx power high warning flag on lane 2: False
Tx power high warning flag on lane 3: False
Tx power high warning flag on lane 4: False
Tx power high warning flag on lane 5: False
Tx power high warning flag on lane 6: False
Tx power high warning flag on lane 7: False
Tx power high warning flag on lane 8: False
Tx power low warning flag on lane 1: False
Tx power low warning flag on lane 2: False
Tx power low warning flag on lane 3: False
Tx power low warning flag on lane 4: False
Tx power low warning flag on lane 5: False
Tx power low warning flag on lane 6: False
Tx power low warning flag on lane 7: False
Tx power low warning flag on lane 8: False
Tx power low alarm flag on lane 1: False
Tx power low alarm flag on lane 2: False

```
        Tx power low alarm flag on lane 3: False
        Tx power low alarm flag on lane 4: False
        Tx power low alarm flag on lane 5: False
        Tx power low alarm flag on lane 6: False
        Tx power low alarm flag on lane 7: False
        Tx power low alarm flag on lane 8: False
...continue
```

show interfaces transceiver error-status [-hw]

Show interface transceiver error-status get from REDIS-DB. If add '-hw', then it would get from sonic-platform API.

Now only support error-status get from sonic-platform API. It would only show "OK" or "Unplugged" in REDIS-DB.

Example

```
Port        Error Status
----------  --------------
Ethernet0   OK
Ethernet8   OK
Ethernet16  Unplugged
Ethernet24  Unplugged
Ethernet32  OK

...continue
```

show interfaces transceiver frequency

Show interface transceiver frequency and space-grid for QSFP-DD. If the transceiver is not QSFP-DD, it would show 'N/A'.

Example

```
Port        Frequency   Grid space
```

```
-----------  -----------  ------------
Ethernet0    N/A          N/A
Ethernet8    N/A          N/A
Ethernet16   193100GHz    75GHz
Ethernet24   N/A          N/A
Ethernet32   N/A          N/A

...continue
```

show interfaces transceiver lpmode

Show interface transceiver low-power mode status.

Example

```
Port        Low-power Mode
----------  ----------------
Ethernet0   On
Ethernet4   On
Ethernet8   On
Ethernet12  On
... continue
```

show interfaces transceiver presence

Show interface transceiver presence.

Example

```
Port        Presence
----------  -----------
Ethernet0   Present
Ethernet4   Not present
Ethernet8   Not present
Ethernet12  Not present
```

```
... continue
```

show interfaces transceiver presence

This command is used to show transceiver presence status.

Example

```
Port        Presence
----------  ----------
Ethernet0   Present
Ethernet4   Not present
Ethernet8   Not present
Ethernet12  Not present
... continue
```

config interface transceiver application

This command is used to set application for CMIS transceiver.

Need to set Vendor PN and application code.

If there is a transceiver plugged into the port, it can set application without Vendor PN, and the Vendor PN would be automatically added to CONFIG_DB.

Usage
config interface transceiver application <interface_name> <application code> -v <Vendor part number>

Parameters:

- <speed_value>, user needs to know the interface configurable speeds
    - 40000 for 40G
    - 100000 for 100G

Example
config interface transceiver application Ethernet0 3 -v DP04QSDD-E30-001

Configure application as auto to automatically select application by port speed and port lane count. If there are multiple matching applications, it would select the first one.

Usage
config interface transceiver application <interface_name> auto

Example
config interface transceiver application Ethernet0 auto

Note:

- The configured application code would be applicable if the following conditions are true.
    - The configured Vendor PN matches the transceiver Vendor PN.
    - The configured application is supported by the transceiver.

    - The host lane count of the configured application matches the breakout mode. For example: The lane count per port in breakout mode 4x100G is 2, and the host lane count of the configured application should be 2.

- If there is no configured application code or there is no applicable configured application, the system would automatically select application by port speed and port lane count.
- Use the "show interfaces transceiver eeprom" to get the supported application. The pattern is "<application code>: <Host Electrical Interface> | <Media Interface>". The host electrical interface and the media interface are based on the SFF8024.

show interfaces transceiver eeprom
Ethernet248: SFP EEPROM detected Active App Selection Host Lane 1: 1 Active App Selection Host Lane 2: 1 Active App Selection Host Lane 3: 1 Active App Selection Host Lane 4: 1 Active App Selection Host Lane 5: 1 Active App Selection Host Lane 6: 1 Active App Selection Host Lane 7: 1 Active App Selection Host Lane 8: 1 Active Firmware Version: 3.3 Application Advertisement: 1: 400GAUI-8 C2M (Annex 120E) | 400ZR, DWDM, amplified 2: 400GAUI-8 C2M (Annex 120E) | ZR400-OFEC-16QAM 3: CAUI-4 C2M (Annex 83E) | ZR200-OFEC-QPSK 4: CAUI-4 C2M (Annex 83E) | ZR100-OFEC-QPSK

- Use the "show logging CMIS" command to check the result of the configuration:

Configure application successfully
root@as9716-32d-2:/# show logging CMIS Jul 7 06:16:16.380853 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: 400G, lanemask=0xff, state=INSERTED, appl=1, retries=0 Jul 7 06:16:16.473915 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248 get configured application 2 Jul 7 06:16:19.705147 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: 400G, lanemask=0xff, state=DP_DEINIT, appl=2, retries=3

Jul 7 06:16:20.945597 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: 400G, lanemask=0xff, state=AP_CONFIGURED, appl=2, retries=3 Jul 7 06:16:25.851871 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: 400G, lanemask=0xff, state=DP_INIT, appl=2, retries=3 Jul 7 06:16:25.971742 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: 400G, lanemask=0xff, state=DP_TXON, appl=2, retries=3 Jul 7 06:17:04.175065 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: 400G, lanemask=0xff, state=DP_ACTIVATION, appl=2, retries=3 Jul 7 06:17:06.494368 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: READY
Configure inapplicable application
root@as9716-32d-2:/# show logging CMIS Jul 7 06:24:12.266125 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: 400G, lanemask=0xff, state=INSERTED, appl=0, retries=0 Jul 7 06:24:12.356151 as9716-32d-2 ERR pmon#xcvrd: CMIS: Ethernet248 the confiugred application_code DP04QSDD-E30-001:3 doesn't applicable for current breakout mode

config interface transceiver frequency

This command is used to set frequency and space-grid for ZR transceiver.

If the configured frequency is not supported, the transceiver will remain on the original frequency.

Usage
config interface transceiver frequency <interface_name> <frequency> <grid_space:75|100>

Example
user@sonic~$ sudo config interface transceiver frequency Ethernet0 193100 75 Set frequency for port Ethernet0... OK user@sonic~$ sudo config interface transceiver frequency Ethernet0 192900 100

Set frequency for port Ethernet0... OK

Note:

Use the "show logging CMIS" command to check the result of the configuration:

Configure frequency successfully
root@as9716-32d-2:/# show logging CMIS Jul 7 05:55:49.769547 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: 400G, lanemask=0xff, state=INSERTED, appl=1, retries=0 Jul 7 05:55:50.674936 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: force Datapath reinit Jul 7 05:55:54.142381 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: 400G, lanemask=0xff, state=DP_DEINIT, appl=1, retries=0 Jul 7 05:55:55.702526 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: 400G, lanemask=0xff, state=AP_CONFIGURED, appl=1, retries=0 Jul 7 05:56:00.560000 as9716-32d-2 NOTICE pmon#xcvrd: message repeated 9 times: [CMIS: Ethernet248: 400G, lanemask=0xff, state=AP_CONFIGURED, appl=1, retries=0] Jul 7 05:56:00.560000 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248 configured laser frequency 193200 GHz grid space 100 GHz Jul 7 05:56:00.908286 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: 400G, lanemask=0xff, state=DP_INIT, appl=1, retries=0 Jul 7 05:56:01.076187 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: 400G, lanemask=0xff, state=DP_TXON, appl=1, retries=0 Jul 7 05:56:38.887624 as9716-32d-2 NOTICE pmon#xcvrd: message repeated 80 times: [CMIS: Ethernet248: 400G, lanemask=0xff, state=DP_TXON, appl=1, retries=0] Jul 7 05:56:38.887624 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: 400G, lanemask=0xff, state=DP_ACTIVATION, appl=1, retries=0 Jul 7 05:56:42.157752 as9716-32d-2 NOTICE pmon#xcvrd: message repeated 5 times: [CMIS: Ethernet248: 400G, lanemask=0xff, state=DP_ACTIVATION, appl=1, retries=0] Jul 7 05:56:42.157752 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: READY
Configure unsupported frequency
root@as9716-32d-2:/# show logging CMIS |tail Jul 7 06:01:34.909414 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: 400G, lanemask=0xff,

```
state=INSERTED, appl=1, retries=0
Jul  7 06:01:35.614400 as9716-32d-2 ERR pmon#xcvrd: CMIS: Ethernet248 configured freq:193200 GHz is not supported in grid 75 GHz
Jul  7 06:01:35.614400 as9716-32d-2 NOTICE pmon#xcvrd: CMIS: Ethernet248: READY
```

config interface transceiver tx_power

This command is used to set tx power for ZR transceiver.

Usage
config interface transceiver tx_power <interface_name> <txpower>

Example
user@sonic~$ sudo config interface transceiver tx_power Ethernet0 -- -9 Setting target Tx output power to -9.0 dBm on port Ethernet0

config interface transceiver lpmode

This command is used to enable or disable the low-power mode of an SFP transceiver.

Usage
config interface transceiver lpmode <interface_name> (enable | disable)

Example
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

config interface transceiver reset

Resets an SFP transceiver module.

Usage
config interface transceiver reset <interface_name>

Example
user@sonic~$ sudo config interface transceiver reset Ethernet0 Resetting port Ethernet0... OK

sfputil show eeprom

This command uses sfp utility to retrieve transceiver's DOM information. Transceiver maker to make sure DOM information can be read and correct in EEPROM.

Example (get transceiver eeprom DOM information)
admin@sonic:~$ sudo sfputil show eeprom --dom Ethernet0: SFP EEPROM detected Application Advertisement: 400GAUI-8 C2M (Annex 120E) - Active Cable assembly with BER < 2.6x10^-4 Connector: No separable connector Encoding: Not supported for CMIS cables

Extended Identifier: Power Class 2(12.0W Max)

Extended RateSelect Compliance: Not supported for CMIS cables

Identifier: QSFP-DD Double Density 8X Pluggable Transceiver

Length Cable Assembly(m): 10

Nominal Bit Rate(100Mbs): Not supported for CMIS cables

Specification compliance: Not supported for CMIS cables

Vendor Date Code(YYYY-MM-DD Lot): 2021-04-07

Vendor Name: Edgecore

Vendor OUI: 68-e8-eb

Vendor PN: ET7502-AOC-10M

Vendor Rev: 10

Vendor SN: L12115000001

ChannelMonitorValues:

RX1Power: 0.4591dBm

RX2Power: 1.1311dBm

RX3Power: 1.3440dBm

RX4Power: 1.1883dBm

RX5Power: -0.0463dBm

RX6Power: 0.7918dBm

RX7Power: 0.8052dBm

RX8Power: 0.7972dBm

TX1Bias: 6.6000mA

TX1Power: 0.6483dBm

TX2Bias: 6.6000mA

TX2Power: 1.1428dBm

TX3Bias: 6.6000mA

TX3Power: 1.1388dBm

TX4Bias: 6.6000mA

TX4Power: 1.3348dBm

TX5Bias: 6.6000mA

TX5Power: 0.7547dBm

TX6Bias: 6.6000mA

TX6Power: 1.0673dBm

TX7Bias: 6.6000mA

TX7Power: 0.9989dBm

TX8Bias: 6.6000mA

TX8Power: 1.1348dBm

ChannelThresholdValues:

RxPowerHighAlarm : 5.0dBm

RxPowerHighWarning: 4.0dBm

RxPowerLowAlarm : -9.3968dBm

RxPowerLowWarning : -8.3983dBm

TxBiasHighAlarm : 15.0mA

TxBiasHighWarning : 14.0mA

TxBiasLowAlarm : 2.0mA

TxBiasLowWarning : 3.0mA

TxPowerHighAlarm : 5.0dBm

TxPowerHighWarning: 4.0dBm

TxPowerLowAlarm : -7.5007dBm

TxPowerLowWarning : -6.4995dBm

ModuleMonitorValues:

Temperature: 36.7773C

Vcc: 3.2323Volts

ModuleThresholdValues:

TempHighAlarm : 75.0C

TempHighWarning: 70.0C

TempLowAlarm : -5.0C

TempLowWarning : 0.0C

VccHighAlarm : 3.6Volts

VccHighWarning : 3.5Volts

VccLowAlarm : 2.9Volts

VccLowWarning : 3.0Volts

Ethernet8: SFP EEPROM detected

Application Advertisement: 400GAUI-8 C2M (Annex 120E) - Active Cable assembly with BER < 2.6x10^-4

Connector: No separable connector

Encoding: Not supported for CMIS cables

Extended Identifier: Power Class 2(12.0W Max)

Extended RateSelect Compliance: Not supported for CMIS cables

Identifier: QSFP-DD Double Density 8X Pluggable Transceiver

…contiune

sfputil show vdm

This command uses sfp utility to retrieve transceiver's versatile diagnostics monitoring.

Example

```
admin@sonic:~$ sfputil show vdm -p Ethernet504
Ethernet504:
   Parameter                        Unit    Value              Threshold          Threshold          Threshold     Threshold     Threshold          Threshold
                                                               High               High               Crossing      Low           Low                Crossing
                                                               Alarm              Warning            Alert-High    Alarm         Warning            Alert-Low
   ---------------------------------------- ------ ------------------ ------------------ ------------------ ------------ ------------------ ------------------ -----------
   TEC Current                      %      -10.467848750267036  79.99816888943144  69.99725333414716  False        -80.00427259132664  -70.00335703604236  False
   Laser Temperature                C      50.578125          85.0               80.0               False        -10.0              -5.0               False
   CD high granularity, short link  ps/nm  0                  2400               2280               False        0                  0                  False
   CD low granularity, long link    ps/nm  0                  50000              42500              False        -655360            -655360            False
   DGD                              ps     0.0                220.0              200.0              False        0.0                0.0                False
   PDL                              dB     0.0                3.5                3.0                False        0.0                0.0                False
   OSNR                             dB     0.0                256.0              256.0              False        14.0               16.0
```

True								
eSNR	dB	0.0	256.0	256.0	False	0.0	0.0	
False								
CFO	MHz	0	3000	2000	False	-3000	-2000	
False								
EVM_modem	%	0.0	100.0	100.0	False	0.0	0.0	
False								
SOP ROC	krad/s	0	80	50	False	0	0	
False								
Tx Power	dBm	-8.2	-2.0	-4.0	False	-17.0	-16.0	
False								
Rx Total Power	dBm	-40.0	6.0	3.0	False	-22.0	-20.0	
True								
Rx Signal Power	dBm	-40.0	4.0	2.0	False	-22.0	-20.0	
True								
Pre-FEC BER Minimum Media Input	N/A	1.0	0.02	0.018000000000000002	True			
0.0	0.0	False						
Pre-FEC BER Maximum Media Input	N/A	1.0	0.02	0.018000000000000002	True			
0.0	0.0	False						
Pre-FEC BER Average Media Input	N/A	1.0	0.02	0.018000000000000002	True			
0.0	0.0	False						
Pre-FEC BER Current Value Media Input	N/A	1.0	0.02	0.018000000000000002	True			
0.0	0.0	False						
Errored Frames Minimum Media Input	N/A	1.0	1.0	2.0	False	0.0		
0.0	False							
Errored Frames Maximum Media Input	N/A	1.0	1.0	2.0	False	0.0		
0.0	False							
Errored Frames Average Media Input	N/A	1.0	1.0	2.0	False	0.0		
0.0	False							
Errored Frames Current Value Media Input	N/A	1.0	1.0	2.0	False	0.0		
0.0	False							
Modulator Bias X/I	%	44.998855573357744	87.99877927824826	85.99984740978103				
False	1.9989318684672313	5.999847409781033	False					
Modulator Bias X/Q	%	43.99938963912413	87.99877927824826	85.99984740978103				
False	1.9989318684672313	5.999847409781033	False					

```
  Modulator Bias Y/I                %     63.96734569314107   87.99877927824826     85.99984740978103
False     1.9989318684672313  5.999847409781033   False
  Modulator Bias Y/Q                %     52.967116807812616  87.99877927824826     85.99984740978103
False     1.9989318684672313  5.999847409781033   False
  Modulator Bias X_Phase            %     59.28282597085527   87.99877927824826     85.99984740978103
False     1.9989318684672313  5.999847409781033   False
  Modulator Bias Y_Phase            %     53.98794537270161   87.99877927824826     85.99984740978103
False     1.9989318684672313  5.999847409781033   False
  Laser Age                         %     0             95            90            False     0           0
False
  Pre-FEC BER Minimum Host Input        N/A   1.0           1.0000000000000002e-06  1e-08           True
0.0           0.0           False
  Pre-FEC BER Maximum Host Input        N/A   1.0           1.0000000000000002e-06  1e-08           True
0.0           0.0           False
  Pre-FEC BER Average Host Input        N/A   1.0           1.0000000000000002e-06  1e-08           True
0.0           0.0           False
  Pre-FEC BER Current Value Host Input  N/A   1.0           1.0000000000000002e-06  1e-08           True
0.0           0.0           False
  Errored Frames Minimum Host Input     N/A   1.0           1.0           2.0           False     0.0
0.0           False
  Errored Frames Maximum Host Input     N/A   1.0           1.0           2.0           False     0.0
0.0           False
  Errored Frames Average Host Input     N/A   1.0           1.0           2.0           False     0.0
0.0           False
  Errored Frames Current Value Host Input  N/A   1.0           1.0           2.0           False     0.0
0.0           False
```

sfputil read-eeprom

用法
sfputil read-eeprom -p [port] -n [page in hex] -o [offset] -s [size]

参数

-p [port]

-n [page in hex]

-o [offset]

-s [size]

示例
root@sonic:/home/admin# sfputil read-eeprom -p Ethernet292 -n 11 -o 128 -s 128 00000080 44 44 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 |DD..............| 00000090 00 00 00 00 00 00 00 00 00 00 3c b9 3c 36 3a d0 |..........<.<6:.| 000000a0 3e c9 00 00 00 00 00 00 00 00 11 c6 11 c6 11 c6 |>...............| 000000b0 11 c6 00 00 00 00 00 00 00 00 35 80 32 48 31 b4 |..........5.2H1.| 000000c0 2f ce 00 00 00 00 00 00 00 00 11 11 00 00 11 11 |/...............| 000000d0 11 11 00 00 00 00 0f 00 00 00 00 00 00 0f 0f 77 |...............w| 000000e0 77 00 00 22 22 00 00 22 22 00 00 00 00 00 00 00 |w..""..""......| 000000f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

sfputil write-eeprom

用法
sfputil write-eeprom -p [port] -n [page in hex] -o [offset] -d [data in hex]

参数

-p [port]

-n [page in hex]

-o [offset]

-d [data in hex]

示例
root@sonic:/home/admin# sfputil write-eeprom -p Ethernet480 -n 10 -o 128 -d ffff root@sonic:/home/admin# sfputil read-eeprom -p Ethernet480 -n 10 -o 128 -s 128 00000080 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................| 00000090 00 10 10 10 10 18 18 18 18 ff 00 00 00 00 00 00 |................| 000000a0 ff ff 66 66 66 66 11 11 11 11 22 22 22 22 00 00 |..ffff....""""..|

```
000000b0 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 |................|
000000c0 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 |................|
000000d0 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 |................|
000000e0 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 |................|
000000f0 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 |................|
```

sfputil lpmode

用法
sfputil lpmode on/off [port]

参数

on/off [port]

示例
root@sonic:/home/admin# sfputil reset Ethernet292 Resetting port Ethernet292 ... OK root@sonic:/home/admin# sfputil lpmode on Ethernet292 Enabling low-power mode for port Ethernet292 ... OK root@sonic:/home/admin# sfputil lpmode off Ethernet292 Disabling low-power mode for port Ethernet292 ... OK

sfputil reset

用法
sfputil reset [port]

参数

[port]

示例

```
root@sonic:/home/admin# sfputil reset Ethernet292
Resetting port Ethernet292 ... OK
```

sfputil show snr

用法

```
sfputil show snr [port]
```

参数

-p [port]

示例

```
sfputil show snr -p Ethernet416
Ethernet416:
  Parameter                          Value
  ---------------------------------------- ----------
  host_side_input_snr_measurement__supported  False
  MediaSideSNRLane1                  21.796875
  MediaSideSNRLane2                  21.796875
  MediaSideSNRLane3                  22.0
  MediaSideSNRLane4                  21.69921875
  MediaSideSNRLane5                  0.0
  MediaSideSNRLane6                  0.0
  MediaSideSNRLane7                  0.0
  MediaSideSNRLane8                  0.0
```

22 IP/IPv6

Table of Contents

IP Show Commands

This sub-section explains the various IP protocol-specific show commands that are used to display the following.

1. routes
2. bgp details - Explained in the bgp section
3. IP interfaces
4. prefix-list
5. protocol

show ip route

This command displays either all the route entries from the routing table or a specific route.

Usage
show ip route [vrf <vrf-name>] [<ip_address>]

Example
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 route, r - rejected 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

Optionally, specify an IP address to display routes to the particular IP address.

Example
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 Last update 00:07:49 ago * directly connected, Ethernet112

Specify <vrf_name> to get IPv4 routes programmed in the <vrf_name>

Example
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, q - queued route, r - rejected 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
```

show ip interfaces

This command displays the details about all the Layer3 IP interfaces in the device for which IP address have been assigned. The type of interfaces include the following.

1. Front panel physical ports
2. PortChannel interfaces
3. VLAN interfaces
4. Loopback interfaces
5. docker interface
6. management interface

```
Usage
```

show ip interfaces

Example
admin@sonic:~$ show ip interfaces Interface Master IPv4 address/mask Admin/Oper BGP Neighbor Neighbor IP Flags ---------- ---------- ---------- ---------- ---------- ---------- ------- Loopback0 1.0.0.1/32 up/up N/A N/A Loopback11 Vrf-red 11.1.1.1/32 up/up N/A N/A Loopback100 Vrf-blue 100.0.0.1/32 up/up N/A N/A PortChannel01 10.0.0.56/31 up/down DEVICE1 10.0.0.57 PortChannel02 10.0.0.58/31 up/down DEVICE2 10.0.0.59 PortChannel03 10.0.0.60/31 up/down DEVICE3 10.0.0.61 PortChannel04 10.0.0.62/31 up/down DEVICE4 10.0.0.63 Vlan100 Vrf-red 1001.1.1/24 up/up N/A N/A Vlan1000 192.168.0.1/27 up/up N/A N/A Docker0 240.127.1.1/24 up/down N/A N/A eth0 10.3.147.252/23 up/up N/A N/A lo 127.0.0.1/8 up/up N/A N/A

show ip prefix-list

This command displays the ip prefix-list.

Usage
show ip prefix-list

Example
admin@sonic:~$ show ip prefix-list BGP: ip prefix-list PL_LoopbackV4: 1 entries   seq 5 permit 10.1.0.32/32

show ip protocol

This command displays the route-map that is configured for the routing protocol. Refer to the routing stack Quagga Command Reference or FRR Command Reference to know more about this command.

Usage
show ip protocol

Example
admin@sonic:~$ show ip protocol VRF: default 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
eigrp     : none
nhrp      : none
hsls      : none
olsr      : none
Table     : none
ldp       : none
vnc       : none
vnc-direct : none
vnc-rn    : none
bgp-direct : none
bgp-direct-to-nve-groups : none
babel     : none
sharp     : none
pbr       : none
bfd       : none
openfabric : none
vrrp      : none
wildcard  : none
any       : none
```

IPv6 Show Commands

This sub-section explains the various IPv6 protocol-specific show commands that are used to display the following.

1. routes
2. IPv6 bgp details - Explained in the bgp section
3. IP interfaces
4. prefix-list

5. protocol

show ipv6 route

This command displays either all the IPv6 route entries from the routing table or a specific IPv6 route

Usage
show ipv6 route [vrf <vrf-name>] [<ip_address>]

Example
admin@sonic:~$ show ipv6 route Codes: K - kernel route, C - connected, S - static, R - RIPng, O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR, f - OpenFabric, > - selected route, * - FIB route, q - queued route, r - rejected route C>* 2018:2001::/126 is directly connected, Ethernet112 C>* 2018:2002::/126 is directly connected, Ethernet116 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.

Example

```
admin@sonic:~$ show ipv6 route fc00:1::32
Routing entry for fc00:1::32/128
  Known via "connected", distance 0, metric 0, best
  Last update 00:26:02 ago
  * directly connected, lo
```

A VRF name can also be specified to see IPv6 routes configured in the VRF.

Example

```
admin@sonic:~$ show ipv6 route vrf Vrf-red
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected 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
```

show ipv6 interfaces

This command displays the details about all the Layer3 IPv6 interfaces in the device for which IPv6 address have been assigned. The type of interfaces include the following.

1. Front panel physical ports
2. PortChannel interfaces
3. VLAN interfaces
4. Loopback interfaces
5. management interface

Usage
show ipv6 interfaces

Example

```
admin@sonic:~$ show ipv6 interfaces
Interface      Master    IPv6 address/mask                 Admin/Oper   BGP Neighbor
Neighbor IP
-----------    -------- ----------------------------------- ------------ --------------
-------------
Bridge              fe80::7c45:1dff:fe08:cdd%Bridge/64      up/up       N/A          N/A
Loopback11     Vrf-red  1100::1/128                        up/up
PortChannel01          fc00::71/126                       up/down     DEVICE1       fc00::72
PortChannel02          fc00::75/126                       up/down     DEVICE2       fc00::76
PortChannel03          fc00::79/126                       up/down     DEVICE3       fc00::7a
PortChannel04          fc00::7d/126                       up/down     DEVICE4       fc00::7e
Vlan100        Vrf-red  100::1/112                        up/up       N/A          N/A
                 fe80::eef4:bbff:fefe:880a%Vlan100/64
```

eth0	fe80::eef4:bbff:fefe:880a%eth0/64	up/up	N/A	N/A
Lo	fc00:1::32/128	up/up	N/A	N/A

show ipv6 prefix-list

This command displays the IPv6 prefix-list.

Usage
show ipv6 prefix-list

Example
admin@sonic:~$ show ipv6 prefix-list BGP: ipv6 prefix-list PL_LoopbackV6: 1 entries seq 5 permit fc00:1::/64

show ipv6 protocol

This command displays the route-map that is configured for the IPv6 routing protocol. Refer to the routing stack Quagga Command Reference or FRR Command Reference to know more about this command.

Usage
show ipv6 protocol

Example

```
admin@sonic:~$ show ipv6 protocol
VRF: default
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
eigrp      : none
nhrp       : none
hsls       : none
olsr       : none
Table      : none
ldp        : none
vnc        : none
vnc-direct : none
vnc-rn     : none
bgp-direct : none
bgp-direct-to-nve-groups : none
babel      : none
sharp      : none
pbr        : none
bfd        : none
openfabric : none
vrrp       : none
wildcard   : none
any        : none
```

23 Kubernetes Configuration

Table of Contents

Kubernetes Server Setting

show the kubernetes server config

This command displays the Kubernetes server configuration if any, otherwise it will report as not configured.

Usage

show kubernetes server config

Example
admin@sonic:~$ show kubernetes server config ip port insecure disable ---------- ------ ---------- --------- 10.250.4.167 6443 True False

show kubernetes server status

This command displays the Kubernetes server status.

Usage
show kubernetes server status

Example
admin@sonic:~$ show kubernetes server status ip port connected update-time ---------- ------ ----------- ------------------- 10.250.4.167 6443 true 2022-4-15 18:25:05

config kubernetes server ip

This command is used to configure the kubernetes server address

Usage

sudo config kubernetes server ip [<server_ip>]

Example
admin@sonic:~$ sudo config kubernetes server ip 10.250.4.167

config kubernetes server disable

To enable or disable the connection between the kubernetes server.

Usage
sudo config kubernetes server disable [on/off]

Example
admin@sonic:~$ sudo config kubernetes server disable off admin@sonic:~$ sudo config kubernetes server disable on

SONiC Feature Setting

config feature owner

Configures the owner of a feature as "local" or "kube". 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 time in the future, the deployment could happen and beyond that time point the feature can run from the 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.

Usage
config feature owner [<feature name>] [local/kube]

Example
admin@sonic:~$ sudo config feature owner snmp kube

show feature config

By executing the command below, the the owner configuration of the corresponding feature can be displayed.

Usage
show feature config [<feature name>]

Example
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
```

show feature status

To see some detailed status like the current owner or the remote state of the feature.

Usage
show feature status [<feature name>]

Example

```
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
```

24 LLDP

Table of Contents

The Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices in the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1AB standard, and can include details such as device identification, capabilities, and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

LLDP Show Commands

show lldp table

This command displays a brief summary of all LLDP neighbors.

Usage
show lldp table

Example
admin@sonic:~$ show lldp table Capability codes: (R) Router, (B) Bridge, (O) Other LocalPort RemoteDevice RemotePortID Capability RemotePortDescr ---------- ---------- ---------- ---------- ---------- Ethernet112 ARISTA01T1 Ethernet1 BR Ethernet116 ARISTA02T1 Ethernet1 BR eth0 00:e0:0c:00:01:05 BR Ethernet Port on unit 1, port 8 ---------- Total entries displayed: 3

show lldp neighbors

This command displays more details about all LLDP neighbors or only the neighbors connected to a specific interface.

Usage
show lldp neighbors <interface_name>

Example 1: Display all neighbors on all interfaces

```
admin@sonic:~$ show lldp neighbors
-------------------------------------------------------------------------------
LLDP neighbors:
-------------------------------------------------------------------------------
Interface:    eth0, via: LLDP, RID: 5, Time: 0 day, 00:04:12
  Chassis:
    ChassisID:    mac 00:e0:0c:00:00:fd
    SysDescr:     ECS4120-28T
    Capability:   Bridge, on
    Capability:   Router, on
  Port:
    PortID:       mac 00:e0:0c:00:01:05
    PortDescr:    Ethernet Port on unit 1, port 8
    TTL:          120
    MFS:          1522
    PMD autoneg:  supported: yes, enabled: yes
      Adv:          10Base-T, HD: yes, FD: yes
      Adv:          100Base-TX, HD: yes, FD: yes
      Adv:          1000Base-T, HD: no, FD: yes
      MAU oper type: 1000BaseTFD - Four-pair Category 5 UTP, full duplex mode
  VLAN:         20, pvid: yes
-------------------------------------------------------------------------------
Interface:    Ethernet112, via: LLDP, RID: 1, Time: 0 day, 00:04:32
  Chassis:
    ChassisID:    mac 52:54:00:02:b9:09
    SysName:      ARISTA01T1
    SysDescr:     Arista Networks EOS version 4.20.15M running on an Arista Networks vEOS
    MgmtIP:       10.250.2.100
    Capability:   Bridge, on
    Capability:   Router, on
  Port:
    PortID:       ifname Ethernet1
    TTL:          120
    MFS:          9236
```

```
  Port is aggregated. PortAggregID: 1000001
------------------------------------------------------------------------------
Interface:    Ethernet116, via: LLDP, RID: 3, Time: 0 day, 00:04:32
 Chassis:
   ChassisID:    mac 52:54:00:25:75:8e
   SysName:      ARISTA02T1
   SysDescr:     Arista Networks EOS version 4.20.15M running on an Arista Networks vEOS
   MgmtIP:       10.250.2.101
   Capability:   Bridge, on
   Capability:   Router, on
 Port:
   PortID:       ifname Ethernet1
   TTL:          120
   MFS:          9236
   Port is aggregated. PortAggregID: 1000001
------------------------------------------------------------------------------
```

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

Example 2

```
admin@sonic:~$ show lldp neighbors Ethernet112
------------------------------------------------------------------------------
LLDP neighbors:
------------------------------------------------------------------------------
Interface:    Ethernet112, via: LLDP, RID: 5, Time: 0 day, 00:05:08
 Chassis:
   ChassisID:    mac 52:54:00:02:b9:09
   SysName:      ARISTA01T1
   SysDescr:     Arista Networks EOS version 4.20.15M running on an Arista Networks vEOS
   MgmtIP:       10.250.2.100
   Capability:   Bridge, on
   Capability:   Router, on
```

```
Port:
  PortID:      ifname Ethernet1
  TTL:         120
  MFS:         9236
  Port is aggregated. PortAggregID: 1000001
------------------------------------------------------------------------------
```

show lldp med location

This command displays the summary of LLDP-MED location configuration of specified port or all ports.

Usage
show lldp med location [port]

Example
admin@sonic:~$ show lldp med location INTERFACE NAME ELIN ---------- ------- Global 1234556

show lldp med policy

This command displays the summary of LLDP-MED policy configuration of specified port or all ports.

Usage
show lldp med policy [port]

Example
admin@sonic:~$ show lldp med policy INTERFACE NAME APPLICATION UNKNOWN TAGGED VLAN PRIORITY DSCP ---------- ---------- ---------- ---------- ---------- ---------- ---------- Global voice True True background 63

show lldp med power

This command displays the summary of LLDP-MED PoE-MDI configuration of a specified port or all ports.

Usage
show lldp med power [port]

Example
admin@sonic:~$ show lldp med power INTERFACE NAME TYPE SOURCE PRIORITY VALUE ---------- ---------- ---------- ---------- ---------- Global pse primary unknown 100

show lldp dot3

This command displays the summary of LLDP Dot3 PoE-MDI configuration of a specified port or all ports.

Usage
show lldp dot3 [port]

Example

```
admin@sonic:~$ show lldp dot3
INTERFACE NAME    TYPE    POWER PAIRS    SUPPORTED    ENABLED    PAIR CONTROL    CLASS    802.3
TYPE    SOURCE    PRIORITY    REQUESTED    ALLOCATED
---------------  ------  -------------  -----------  ---------  --------------  -------  ------------  -----
---  ----------  -----------  -----------
Global          pse     signal       False       False      False
```

show lldp global

This command displays the summary of LLDP global configuration.

Usage
show lldp global

Example
admin@sonic:~$ show lldp global ---------- LLDP Global configuration: ---------- HELLO TIMER 30 SYSTEM NAME as7326-56x-3 SYSTEM DESCRIPTION SONiC Software Version: SONiC.autobuild_172 - HwSku: Accton-AS7326-56X - Distribution: Debian 11.4 - Kernel: 5.10.0-8-2-amd64 MANAGEMENT IP 10.250.0.182 ----------

show lldp interfaces

This command displays the LLDP interfaces status.

Usage
show lldp interfaces [port]

Example
admin@sonic:~$ show lldp interfaces Ethernet0 INTERFACE NAME LLDP ENABLED ---------- ---------- Ethernet0 true

LLDP Config Commands

config lldp med location

This command is used to set the LLDP-MED location.

Usage
config lldp med location <--elin <elin>> [--port <port-name>]

Parameters:

- elin : Emergency Location Identification Number.
- port : Port name. Default is set to all ports.

Note: The configuration cannot be removed after it is configured.

The example below sets the LLDP-MED location to port Ethernet27 and emergency number to 911.

Example
admin@sonic:~$ sudo config lldp med location --elin 911 --port Ethernet27

config lldp med policy voice

This command is used to configure the specific network policy for voice applications advertised by LLDP for a given port or for all ports.

Usage
config lldp med policy voice [--port <port-name>] [--vlan <1-4094>] [--tagged] [--unknown] [--priority (best-effort | background | excellent-effort | critical-applications| video | voice | internetwork-control | network-control)] [--dscp <0-63>]

Parameters:

- port: Port name. Default is set to all ports.
- unknown: Means the network policy for voice application is currently unknown. Default is known.
- tagged: Means the IEEE 802.1Q tagged frame format is used by voice application. Default is untagged.
- vlan: The VLAN ID (the range is from 1 to 4094). Default value is 0.
- priority: IEEE 802.1p Layer 2 Priority, also known as Class of Service(CoS). Default value is best-effort.
    - best-effort (0).
    - background (1).
    - excellent-effort (2).
    - critical-applications (3).
    - video (4).
    - voice (5).
    - internetwork-control (6).
    - network-control (7).
- dscp: DSCP value to be advertised for the given network policy (the range is from 0 to 63). Default value is 0.

Note: The configuration cannot be removed after it is configured.

The example below sets the LLDP-MED policy for the voice VLAN to port Ethernet27, vlan 100 tagged, network policy unknown, priority voice, and dscp 46.

Example
sudo config lldp med policy voice --port Ethernet27 --vlan 100 --tagged --unknown --priority voice --dscp 46

config lldp med power

These commands are used to configure the LLDP-MED PoE-MDI TLV advertised on a given port or all ports.

The following command is used to configure LLDP-MED PoE-MDI TLV of power providers.

Usage
config lldp med power --power-type pse --source (primary | backup) --priority (unknown | critical | high | low) --value <milliwatts> [--port <port-name>]

The following command is used to configure LLDP-MED PoE-MDI TLV of power consumers.

Usage
config lldp med power --power-type pd --source (pse | local | both) --priority (unknown | critical | high | low) --value <milliwatts> [--port <port-name>]

Parameters:

- source: Power source.
  - primary : Primary power source.
  - backup : Backup power source.
  - pse: power source equipment.
  - local : Local power.
  - both : Both pse and local .
- priority : Power priority.
  - unknown
  - critical
  - High
  - low
- value : Total power in milliwatts required by the PD device or available by the PSE device. It shall be divisible by 100.
- port : Port name. Default is set to all ports.

Note: The configuration cannot be removed after it is configured.

The example below sets LLDP-MED PoE-MDI to port Ethernet27, power-type pse, source primary, priority high, and available power 4000 milliwatts.

Example
sudo config lldp med power --port Ethernet27 --power-type pse --source primary --priority high --value 4000

config lldp dot3 power

These commands are used to configure LLDP Dot3 PoE-MDI TLV for a given port or for all ports.

The following command is used to configure LLDP Dot3 PoE-MDI TLV of power providers.

Usage
config lldp dot3 power --power-type pse <--power-pairs (signal | spare)> [--port <port-name>] [--supported] [--

enabled] [--pair-control] [--power-class <0-4>] [--dot3-type (1 | 2) --source (primary | backup) --priority (unknown | critical | high | low) --requested <milliwatts> --allocated <milliwatts>]

The following command is used to configure LLDP Dot3 PoE-MDI TLV of power consumers.

Usage
config lldp dot3 power --power-type pd <--power-pairs (signal | spare)> [--port <port-name>] [--supported] [--enabled] [--pair-control] [--power-class <0-4>] [--dot3-type (1 | 2) --source (pse | local | both) --priority (unknown | critical | high | low) --requested <milliwatts> <--allocated <milliwatts>]

Parameters:

- power-pairs : Power pairs.
    - signal : Signal pair.
    - spare: Spare pair.
- port : Port name. Default is set to all ports.
- supported : Means MDI power is supported on the given port, otherwise default is not supported.
- enabled : Means MDI power is enabled, otherwise the default is disabled.
- pair-control : Means pair selection can be controlled, otherwise the default is cannot be controlled. power-class : Power class (the range is from 0 to 4).
- dot3-type : Type of 802.3.
    - 1 : Type 1, IEEE802.3af.
    - 2 : Type 2, IEEE802.3at.
- source: Power source.
    - primary : Primary power source.
    - backup : Backup power source.
    - pse: Power source equipment.
    - local : Local power.
    - both : Both pse and local .
- priority : Power priority.
    - unknown
    - critical
    - high
    - low

- requested : Requested power in milliwatts. It shall be divisible by 100.
- allocated : Allocated power in milliwatts. It shall be divisible by 100.

Note: The configuration cannot be removed after it is configured.

The example below sets LLDP Dot3 PoE-MDI to port Ethernet27, power-type pse, power pairs signal, power class 3, MDI power supported and enabled, 802.3at type 1, source backup, priority critical, requested 10000 milliwatts, and allocated 10000 milliwatts.

Example
sudo config lldp dot3 power --port Ethernet27 --power-type pse --power-pairs signal --power-class 3 --supported --enabled --dot3-type 1 --source backup --priority critical --requested 10000 --allocated 10000

config lldp global hello_timer

The command is used to configure the transmission frequency of LLDP PDU updates in seconds. The range is 5 to 65534 seconds.

Usage
config lldp global hello_timer <seconds>

Example
sudo config lldp global hello_timer 10

config lldp global management_ip

The command is used to configure the management address to be advertised in LLDP PDUs.

Usage
config lldp global management_ip <ip_str>

Example
sudo config lldp global management_ip 192.168.1.1

config lldp global system_description

The command is used to configure the system description to be advertised in LLDP PDUs.

Usage
config lldp global system_description <desc>

Example
sudo config lldp global system_description “Networks"

config lldp global system_name

The command is used to configure the system name to be advertised in LLDP PDUs.

Usage
config lldp global system_name <name>

Example

```
sudo config lldp global system_name "SONiC DUT"
```

25 Management VRF

Table of Contents

Management Virtual Routing and Forwarding (VRF) supports a separate routing table for management traffic that is forwarded by out-of-band management ports on a switch. This enables management traffic to be routed across a management network and still remain secure and separate from network data traffic.

Management VRF Show Commands

show mgmt-vrf

This command displays whether the management VRF and in-band management VRF are enabled or disabled. It also displays the details about the links (eth0, mgmt, lo-m, L3 interface) that are related to the management VRF.

Usage
show mgmt-vrf

Example
admin@sonic:~$ show mgmt-vrf ManagementVRF : Enabled In-band 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 66: Ethernet104: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9100 qdisc pfifo_fast 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.

show mgmt-vrf routes

This command displays the routes that are present in the management VRF routing table.

Usage
show mgmt-vrf routes

Example
admin@sonic:~$ show mgmt-vrf ManagementVRF : Enabled In-band 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 66: Ethernet104: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9100 qdisc pfifo_fast 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.

show management_interface address

This command displays the IP addresses configured for the management interface "eth0" and the management network default gateway.

Usage
show management_interface address

Example
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

Management VRF Config Commands

config vrf add mgmt

This command enables 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 the management VRF. That is, data VRFs should not use these reserved VRF names.

Usage
config vrf add mgmt

Example
admin@sonic:~$ sudo config vrf add mgmt

config vrf del mgmt

This command disables 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 the management VRF. That is, data VRFs should not use these reserved VRF names.

Usage
config vrf del mgmt

Example:
admin@sonic:~$ sudo config vrf del mgmt

config in-band-mgmt

This command is used to enable or disable the in-band management VRF in the system. Globally, in-band management VRF is disabled by default.

Usage
config in-band-mgmt <enable|disable>

Example
admin@sonic:~$ sudo config in-band-mgmt enable

26 MC LAG

Table of Contents

This section explains all the MCLAG (Multi-Chassis Link Aggregation Group) commands that are supported in SONiC.

MCLAG show commands

show mclag brief

This command displays brief information about an MCLAG domain.

Usage
show mclag brief

Example
admin@sonic:~$ show mclag brief Domain ID : 5 Role : Active Session Status : Up Peer Link Status : Up Source Address : 192.168.1.1 Peer Address : 192.168.1.2 Peer Link : PortChannel30 Keepalive Interval : 1 secs Session Timeout : 15 secs System MAC : b8:6a:97:73:6c:96

Number of MCLAG Interfaces : 2 MCLAG Interface Local/Remote Status PortChannel50 Up/Up PortChannel60 Up/Up

show mclag interface

This command displays interface information in an MCLAG domain.

Usage
show mclag interface <domain-id> <portchannel-name>

Example
admin@sonic:~$ show mclag interface 5 PortChannel50 Local/Remote Status : Up/Up IsolateWithPeerLink : Yes

show mclag unique ip

This command displays the unique IP status.

Usage
show mclag unique-ip

Example
admin@sonic:~$ show mclag unique-ip

Unique IP: : Vlan200, Vlan300

MCLAG Configuration Commands

In this section, it describes how to configure a MCLAG domain, add MCLAG member, enable/disable unique IP, and configure timer for keep-alive and session timeout.

config mclag add/del

Use this command to configure MCLAG domain attributes.

Usage
config mclag {add | del} <domain-id> <local-ip-addr> <peer-ip-addr> [<peer-ifname>]

Parameters:

- domain-id - MCLAG node's unique domain ID; this domain-id should be the same as peer node.
- local-ip-addr - MCLAG node's local IPv4 address
- peer-ip-addr - MCLAG node's peer IPv4 address
- peer-ifname - MCLAG peer interface name; optional for L3 MCLAG, mandatory for L2 MCLAG config

Example
admin@sonic:~$ sudo config mclag add 5 192.168.1.1 192.168.1.2 PortChannel30

config mclag member add/del

Use this command to configure a domain's MCLAG interfaces.

Usage
config mclag member {add | del} <domain-id> <portchannel-name>

Note:

- MCLAG interfaces can be only portchannel.

Example
admin@sonic:~$ sudo config mclag member add 5 PortChannel50

config mclag unique-ip add/del

Use this command to configure the unique IP status on a specified VLAN. User may enable (or disable) unique IP on different VLANs but this configuration should be the same in both active node and standby node. When the unique IP of a VLAN is enabled, active node and standby node should use different IP addresses, that is, the assigned IP address of active node and standby node on the VLAN cannot be the same.

Usage
config mclag unique-ip {add | del} <Vlan-interface>n

Parameter:

- add - enable unique IP on the VLAN. After enabled, the active node and standby node should not assign the same IP address on the VLAN.
- del - disable unique IP on the VLAN. After disabled, the active node and standby node share the same IP address on the VLAN. Vlan-interface - VLAN interface for which a unique IP can be configured.

Before applying this command, please make sure

- The MCLAG Domain should be created.
- VLAN interface should not be bound to VRF.
- There are not any IP address on VLAN interface.

Note, this restriction is derived from following user scenario

- when enabling (or disabling) the unique IP on a VLAN, the IP address should be re-assigned after the command executed.
- the IP address re-assignment should be manually configured by user. This command would not automatically clean (or assign) the IP address.

- as the IP address is re-assigned, the routing tables of VRF should be not referred any more.
- Due to the re-assignment is manually, the command will check the MCLAG domain, IP assignment, and bound on VRF before execution.

Example
admin@sonic:~$ sudo config mclag unique-ip add Vlan200

config mclag keepalive-interval

Use this command to configure keep-alive timer.

Usage
config mclag keepalive-interval <domain-id> <keepalive-timer-val>

Note

- keepalive-timer-val - keepalive-timer in the range of 1 to 60 seconds with default value of 1 seconds.
- session-timeout should be at least greater than 3 times keepalive-timer value.

Example
admin@sonic:~$ sudo config mclag keepalive-interval 5 5

config mclag session-timeout

Use this command to configure session timeout.

Usage
config mclag session-timeout <domain_id> <time_in_secs>

Note:

- time_in_ secs - session-timeout in the range of 3 to 3600 seconds with default value of 15 seconds

- session-timeout should be at least greater than 3 times keepalive-timer value.

Example
admin@sonic:~$ sudo config mclag session-timeout 5 20

27 Mirroring

Table of Contents

Mirroring Show Commands

show mirror_session

The command show mirror_session displays all the mirror sessions that are configured.

Example
admin@sonic:~$ show mirror_session ERSPAN Sessions 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 0x88be 8 100 UC0 SPAN Sessions Name Status DST Port SRC Port Direction Queue Policer ---------- -------- ---------- ------------- ----------- ------- ------- mrr_port0 active Ethernet0 PortChannel10 rx

Mirroring Configuration Commands

config mirror_session add

The command config mirror_session add is used to add mirroring sessions. A mirror session is identified by a "session_name".

This command supports configuring both Switch Port Analyzer (SPAN) and Encapsulated Remote SPAN (ERSPAN) sessions. For a SPAN session, you can configure mirroring for a list of source ports/LAG to a destination port in ingress, egress, or both directions. For an ERSPAN session, you can configure mirroring for a list of source ports/LAG to a destination IP. Both SPAN/ERSPAN support ACL-based mirroring and can be used in ACL configurations.

The ERSPAN mirror session below command is used to create ERSPAN mirror session

Usage
config mirror_session erspan add <session-name> <src_ip> <dst_ip> <dscp> <ttl> [gre_type] [queue] [src_port] [direction] [--policer policer_name>]

or

Usage (backward compatible, to be deprecated)
config mirror_session add <session_name> <src_ip> <dst_ip> <dscp> <ttl> [gre_type] [queue]

ERSPAN mirror session Parameters:

1. Session name
2. Source IP address
3. Destination IP address
4. DSCP (QoS) value with which mirrored packets are forwarded
5. TTL value
6. Optional - GRE type in a GRE tunnel packet. The default value is 0x88be. Valid values are:
    a. 0x88be: ERSPAN Type I.
    b. 0x22eb: ERSPAN Type III (Only support on Intel devices).
    c. 0x8949: AS9746-128D supports this value only.
7. Optional - Queue in which packets shall be sent out of the device. The default value is 0. Only support to change the value

on Intel devices. Valid values are 0..7.

8. Optional - List of source ports that can have both Ethernet and LAG ports.
9. Optional - Direction - Mirror session direction when configured along with source port. (Supported rx/tx/both. default

direction is both.)

10. Optional - Policer that will be used to control the rate at which frames are mirrored. (refer Policer)

The example below shows how to create an ERSPAN session with name mrr_legacy, source address 1.2.3.4, destination address 20.21.2 2.23, DSCP 8, TTL 100, and GRE-type 0x888be.

Example1

```
admin@sonic:~# config mirror_session add mrr_legacy 1.2.3.4 20.21.22.23 8 100 0x88be 0
admin@sonic:~# show mirror_session
ERSPAN Sessions
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  0x88be      8  100    UC0
SPAN Sessions
Name    Status    DST Port    SRC Port    Direction    Queue    Policer
------  --------  ----------  ----------  -----------  -------  ---------
admin@sonic:~#
```

The example below shows how to create an ERSPAN session with name mrr_abcd, source address 1.2.3.4, destination address 20.21.22. 23, DSCP 8, TTL 100, and GRE-type 0x88be.

Example2

```
admin@sonic:~# config mirror_session erspan add mrr_abcd 1.2.3.4 20.21.22.23 8 100 0x88be 0
admin@sonic:~# show mirror_session
ERSPAN Sessions
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  0x88be      8  100    UC0
SPAN Sessions
Name    Status    DST Port    SRC Port    Direction    Queue    Policer
------  --------  ----------  ----------  -----------  -------  ---------
admin@sonic:~#
```

The example below shows how to create an ERSPAN session with name mrr_port, source address 1.2.3.4, destination address 20.21.22. 23, DSCP 8, TTL 100, GRE-type 0x88be, and source port Ethernet0.

Example3
admin@sonic:~# config mirror_session erspan add mrr_port 1.2.3.4 20.21.22.23 8 100 0x88be 0 Ethernet0 admin@sonic:~# show mirror_session ERSPAN Sessions 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 0x88be 8 100 UC0 Ethernet0 both SPAN Sessions Name Status DST Port SRC Port Direction Queue Policer ------ -------- ---------- ---------- ----------- ------- --------- admin@sonic:~#

config mirror_session span add

The command is used to create a SPAN mirror session

Usage
config mirror_session span add <session_name> <dst_port> [src_port] [direction] [queue] [--policer <policer_name>]

SPAN mirror session parameters are:

1. Session name
2. Destination port
3. Optional - List of source ports- List of source ports that can have both Ethernet and LAG ports.
4. Optional - Direction - Mirror session direction when configured along with source port. (Supported rx/tx/both. Default direction is both.)

5. Optional - Queue in which packets shall be sent out of the device. The default value is 0. Only support to change the value on Intel devices. Valid values are 0..7.

6. Optional - Policer that will be used to control the rate at which frames are mirrored.

The example below shows how to create a SPAN session with name mrr_port0, destination port Ethernet0 and source ports Ethernet4, PortChannel10,Ethernet8.

Example
admin@sonic:~# config mirror_session span add mrr_port0 Ethernet0 Ethernet4,PortChannel10,Ethernet8 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 ---------- -------- ---------- ------------------------------ ----------- ------- --------- mrr_port0 active Ethernet0 Ethernet4,PortChannel10,Ethernet8 both UC0 admin@sonic:~#

config mirror_session remove

The command shown below is used to remove the existing mirroring sessions and requieres a parameter named session name.

Usage
config mirror_session remove <session-name>

The below example shows how to remove a mirror session with session name mrr_port0.

Example

```
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
---------  --------  ----------  ----------------------------  -----------  -------  ---------
mrr_port0  active    Ethernet0   Ethernet4,PortChannel10,Ethernet8  both         UC0
admin@sonic:~# config mirror_session remove mrr_port0
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
------  --------  ----------  ----------  -----------  -------  ---------
```

28 NAT

Table of Contents

Network Address Translation (NAT) is a standard method of mapping “internal” (private) network IP addresses to “external”(public) IP address on devices at the edge of a network. Typically, NAT not only translates the inbound and outbound IP addresses of network traffic, but also Layer 4 ports. This allows multiple internal IP addresses to "share" one public external IP address and also provides a level of security for private network hosts that remain "hidden" from the public network.

NAT Show Commands

show nat config

This command displays the NAT configuration.

Usage

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

With no optional arguments, the whole NAT configuration is displayed.

Example

```
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
```

show nat statistics

This command displays the NAT translation statistics for each entry.

Usage
show nat statistics

Example

```
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
```

show nat translations

This command displays the NAT translation entries.

Usage
show nat translations [count]

Giving the optional count argument displays only the details about the number of translation entries.

Example

```
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
```

NAT Configuration Commands

config nat add static

This command adds a static NAT or NAPT entry. When configuring a static NAT entry, you have to specify the following fields with these "basic" keywords.

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

When configuring a static NAPT entry, you have to specify the following fields.

1. IP protocol type (tcp / udp)
2. Global IP address + Port
3. Local IP address + Port
4. NAT type (snat / dnat) to be applied on the Global IP address + Port. Default value is dnat. This is an optional argument.
5. Twice NAT Id. This is an optional argument used in the case of twice NAT configuration.

Usage
config nat add static (basic <global-ip> <local-ip> | (tcp | udp) <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.

Usage
config nat remove static (basic <global-ip> <local-ip> | (tcp | udp) <global-ip> <global-port> <local-ip> <local-port> | all)

Example
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
```

config nat add pool

This command creates a NAT pool used for dynamic source NAT or NAPT translations. The pool can be configured in one of the following combinations.

1. Global IP address range (or)
2. Global IP address + L4 port range (or)
3. Global IP address range + L4 port range.

Usage
config nat add pool <pool-name> <global-ip-range> <global-port-range>

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

Usage
config nat remove (pool <pool-name> | pools)

Example
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

config nat add binding

This command creates a NAT binding between a pool and an ACL. The following fields are needed for configuring the binding.

1. ACL is an optional argument. If an ACL argument is not given, the NAT binding is applicable to match all traffic.
2. NAT type is an optional argument. Only DNAT type is supported for binding.
3. 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.

Usage
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 following command.

Usage
config nat remove (binding <binding-name> | bindings)

Example
admin@sonic:~$ sudo config nat add binding bind1 pool1 acl1

config nat add interface

This command is used to configure a NAT zone on an L3 interface. The default value of a NAT zone on an L3 interface is 0. The valid range of zone values is 0-3 (On Intel devices, the valid values are: 0, 1).

Usage
config nat add interface <interface-name> -nat_zone <value>

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

Usage
config nat remove (interface <interface-name> | interfaces)

Example:
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

config nat set

This command is used to set NAT timeout values. Different timeout values can be configured for the NAT entry timeout, NAPT TCP entry timeout, and NAPT UDP entry timeout. The range for the Global NAT entry timeout is 300 sec to 432000 sec, the default value is 600 sec. The range for the TCP NAT/NAPT entry timeout is 300 sec to 432000 sec, the default value is 86400 sec. The range for the UDP NAT/NAPT entry timeout is 120 sec to 600 sec, the default value is 300 sec.

Usage
config nat set (tcp-timeout <value> | timeout <value> | udp-timeout <value>)

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

Usage
config nat reset (tcp-timeout | timeout | udp-timeout)

Example
admin@sonic:~$ sudo config nat add set tcp-timeout 3600 admin@sonic:~$ show nat config globalvalues Admin Mode : enabled Global Timeout : 600 secs TCP Timeout : 600 secs UDP Timeout : 300 secs

config nat feature

This command is used to enable or disable the NAT feature.

Usage
config nat feature (enable | disable)

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

NAT Clear Commands

sonic-clear nat translations

This command is used to clear the dynamic NAT and NAPT translation entries.

Usage

sonic-clear nat translations

sonic-clear nat statistics

This command is used to clear the statistics of all NAT and NAPT entries.

Usage
sonic-clear nat statistics

29 NDP

NDP Show Commands

show ndp

This command displays the IPv6 neighbors.

Usage
show ndp [-if|--iface <interface_name>] <ipv6_address>

Example (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

Example (a 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

Example (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
```

NDP Config Command

config vlan proxy_arp

Usage
config vlan proxy_arp < vid > { enabled | disable }

Note:

Configuring NDP proxy will also configure NDP proxy. Currently, independent configuration of NDP proxy is not supported; it can only be configured through NDP proxy settings.

NDP proxy is disabled by default and can only be configured on VLAN interfaces.

Use **show vlan brief** to show the configuration.

Usage
admin@sonic:~$ sudo config vlan proxy_arp 10 enabled

```
admin@sonic:~$ sudo config vlan proxy_arp 10 disabled
```

config interface nd aging

Usage
config interface nd aging <interface_name> <interface_nd_aging>

Parameter:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- <interface_nd_aging>: The default ND aging time is 1800s, and the configuration range is 300~86400

Note:

- If you have already learned ND, configuring ND aging time will not take effect immediately. You need to wait for ND aging before the aging time configuration will take effect.
- Use **show interfaces nd** command, you can view **NDP** aging configuration information on the interface.

Usage
admin@sonic:~$ sudo config interface nd aging Vlan10 10000

config vlan nd_host_route

Usage
config vlan nd_host_route < vid > { enabled | disable }

Note:

- ND host routing is disabled by default and can only be configured on VLAN interfaces. ND to host routing converts ND to "K" type routing.
- Use **show interfaces nd** command, you can view ND nd_host_route configuration information on the interface.

Usage
admin@sonic:~$ sudo config vlan nd_host_route 10 enabled admin@sonic:~$ sudo config vlan nd_host_route 10 disabled

30 NTP

NTP Show Commands

show ntp

This command displays a list of NTP peers known to the server as well as a summary of their state.

Usage
show ntp

Example
admin@sonic:~$ show ntp synchronised to NTP server (204.2.134.164) at stratum 3 time correct to within 326797 ms polling server every 1024 s remote refid st t when poll reach delay offset jitter == 23.92.29.245 .XFAC. 16 u - 1024 0 0.000 0.000 0.000 *204.2.134.164 46.233.231.73 2 u 916 1024 377 3.079 0.394 0.128

NTP Config Commands

This sub-section of commands is used to add or remove the configured NTP servers.

config ntp add

This command is used to add an NTP server IP address to the NTP server list. Note that more than one NTP server IP address can beadded in the device.

Usage
config ntp add <ip_address>

Parameters:

- <ip_address>: NTP server's IP address, IPv4 or IPv6 address.
- When the NTP service is started, it listens on eth0 by default. This means that the NTP server must be accessible from eth0.

The following example shows how to add a NTP server.

Example
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 2000::2 NTP server 2000::2 added to configuration Restarting ntp-config service...

config ntp delete

This command is used to delete a configured NTP server IP address.

Usage
config ntp del <ip_address>

Parameters:

- <ip_address>: NTP server's IP address, IPv4 or IPv6 address.

The following example shows how to remove an NTP server.

Example
admin@sonic:~$ sudo config ntp del 9.9.9.9 NTP server 9.9.9.9 removed from configuration Restarting ntp-config service...

30.1 NTP

Table of Contents

NTP display command

show ntp

This command displays a list of NTP peers known to the server and a summary of their status.

Usage

show ntp

Example
admin@sonic:~$ show ntp synchronised to NTP server (204.2.134.164) at stratum 3 time correct to within 326797 ms polling server every 1024 s remote refid st t when poll reach delay offset jitter == 23.92.29.245 .XFAC. 16 u - 1024 0 0.000 0.000 0.000 *204.2.134.164 46.233.231.73 2 u 916 1024 377 3.079 0.394 0.128

show ntp global

This command displays the global configuration information of server NTP.

Usage
show ntp global

Example
admin@sonic:~$ show ntp global State: enabled Authentication: disabled VRF: default DHCP: enabled Server Role: enabled

show ntp key

This command displays the NTP key for server configuration.

Usage
show ntp key

Example
admin@sonic:~$ show ntp key KEY ID TYPE TRUSTED -------- ------ --------- 1 md5 yes

show ntp server

This command displays the NTP server configured for the server

Usage
show ntp server

Example
admin@sonic:~$ show ntp server SERVER STATE TYPE KEY ID VERSION IBURST TRUSTED -------- ------- ------ -------- --------- -------- --------- 1.1.1.1 enabled server 1 3 on

show runningconfiguration ntp

This command displays the NTP source interface, source IP, and NTP server configured for the server.

Usage
show runningconfiguration ntp

Example
admin@sonic:~$ show runningconfiguration ntp NTP source-interface : eth0 NTP source-ip : NTP Servers ---------- 1.1.1.1

NTP configuration command

This command section is used to add or remove configured NTP servers.

config ntp server add

This command is used to add the NTP server IP address to the NTP server list.

Please note that multiple NTP server IP addresses can be added to the device.

Usage
config ntp server add <ip_address>

Parameters:

- <ip_address>: NTP server's IP address, IPv4 or IPv6 address.
- When the NTP service is started, it listens on eth0 by default. This means that the NTP server must be accessible from eth0.
- -t: NTP server type server | pool, default is server
- -k: ntp keyID
- -v: ntpd version 3|4， default NTPv4

The following example shows how to add a NTP server.

Example
admin@sonic:~$ sudo config ntp server add 9.9.9.9 NTP server 9.9.9.9 added to configuration Restarting ntp-config service... admin@sonic:~$ sudo config ntp server add 2000::2 NTP server 2000::2 added to configuration Restarting ntp-config service... admin@sonic:~$ sudo config ntp server add 1.1.1.1 -k 1 -v 3 NTP server 1.1.1.1 added to configuration Restarting ntp-config service...

config ntp del

This command is used to delete the configured NTP server IP address.

Usage
config ntp server del <ip_address>

Parameters:

- <ip_address>: NTP server's IP address, IPv4 or IPv6 address.

The following example shows how to delete an NTP server.

Example
admin@sonic:~$ sudo config ntp server del 9.9.9.9 NTP server 9.9.9.9 removed from configuration Restarting ntp-config service...

config ntp server state

This command is used to modify the parameters of an added NTP server.

Usage
config ntp server state <ntpserver_ip_address>

Parameters:

•disabled: Make the specified NTP server IP invalid.

•enabled： Make the specified NTP server IP effective.

•iburst： off|on， The default is on. When the NTP service is first started, multiple NTP messages will be sent to the NTP server to quickly synchronize the time

•key-id: ntp keyID

•trusted: trust the server yes|no ,

•version: ntpd version 3|4 ， default NTPV4

The following example shows how to add an NTP server.

Example
admin@sonic:~$ sudo config ntp server state 1.1.1.1 disabled Configure NTP server 1.1.1.1 disabled admin@sonic:~$ sudo config ntp server state 1.1.1.1 enabled Configure NTP server 1.1.1.1 enabled admin@sonic:~$ sudo config ntp server state 1.1.1.1 iburst off Configure NTP server 1.1.1.1 iburst off admin@sonic:~$ sudo config ntp server state 1.1.1.1 iburst on Configure NTP server 1.1.1.1 iburst on admin@sonic:~$ sudo config ntp server state 1.1.1.1 trusted yes Configure NTP server 1.1.1.1 trusted yes admin@sonic:~$ sudo config ntp server state 1.1.1.1 trusted no Configure NTP server 1.1.1.1 trusted no admin@sonic:~$ sudo config ntp server state 1.1.1.1 version 3 Configure NTP server 1.1.1.1 version 3 admin@sonic:~$ sudo config ntp server state 1.1.1.1 version 4

Configure NTP server 1.1.1.1 version 4 admin@sonic:~$ sudo config ntp server state 1.1.1.1 key-id 1 Configure NTP server 1.1.1.1 key id 1

config ntp authentication

This command is used to enable/disable NTP authentication on the device.

Usage
config ntp server add [OPTIONS]

Parameters:

disabled : Disable NTP authentication， default disabled

enabled: Enable NTP authentication

Example
admin@sonic:~$ sudo config ntp authentication disabled NTP authentication is already disabled. root@sonic:/home/admin# admin@sonic:~$ sudo config ntp authentication enabled Restarting ntp-config service... root@sonic:/home/admin#

config ntp dhcp

This command is used to enable/disable obtaining NTP servers from DHCP servers.

Usage
config ntp dhcp [OPTIONS]

Parameters:

disabled : Disable obtaining NTP server from DHCP server

enabled: Enable obtaining NTP server from DHCP server, default enabled

Example
admin@sonic:~$ sudo config ntp dhcp disabled NTP authentication is already disabled. root@sonic:/home/admin# admin@sonic:~$ sudo config ntp dhcp enabled Restarting ntp-config service... root@sonic:/home/admin#

config ntp key add

This command is used to add NTP key.

Usage
config ntp key add <key_id> <key_value>

Parameters:

<key_id>: key id ,value 1-65535

<key_value>: Key string

--type:Encryption method, one of [md5 | sha1 | sha256 | sha384 | sha512]

--trusted :trust [yes|no]

Example
admin@sonic:~$ sudo config ntp key add 1 password --type md5 --trusted yes NTP key 1 added to configuration Restarting ntp-config service...

config ntp key del

This command is used to delete NTP key.

Usage
config ntp key del <key_id>

Parameters:

<key_id>: key id

Example
admin@sonic:~$ sudo config ntp key del 1 NTP key 1 removed from configuration Restarting ntp-config service...

config ntp server-role

This command is used to enable/disable obtaining NTP servers from DHCP servers.

Usage
config ntp server-role [OPTIONS]

Parameters:

disabled : Disable the function of acting as an NTP server.

enabled: Enable the function of acting as an NTP server, which is enabled by default.

Example
admin@sonic:~$ sudo config ntp server-role disabled NTP server_role is already disabled. root@sonic:/home/admin#

```
admin@sonic:~$ sudo config ntp dhcp enabled
Restarting ntp-config service...
root@sonic:/home/admin#
```

config ntp source-ip set

This command is used to configure NTP source IP.

Usage
config ntp source-ip set <ip_address>

Parameters:

- <ip_address>: IPv4 or IPv6 address on a certain interface.

Example
admin@sonic:~$ sudo config ntp source-ip set 80.1.1.4 Restarting ntp-config service...

config ntp source-ip unset

This command is used to unconfigure the NTP source IP.

Usage
config ntp source-ip unset <ip_address>

Parameters:

- <ip_address>: IPv4 or IPv6 address on a certain interface.

Example

```
admin@sonic:~$ sudo config ntp source-ip unset 80.1.1.4
Restarting ntp-config service...
```

config ntp source-interface set

This command is used to configure NTP source IP.

Usage
config ntp source-interface set <interface_name>

Parameters:

- <interface_name>: a certain interface.

Example
admin@sonic:~$ sudo config ntp source-interface set Loopback0 Restarting ntp-config service...

config ntp source-ip unset

This command is used to unconfigure the NTP source IP.

Usage
config ntp source-ip unset <interface_name>

Parameters:

- <interface_name>: a certain interface.

Example
admin@sonic:~$ sudo config ntp source-interface unset Loopback0 Restarting ntp-config service...

config ntp state

This command is used to turn on/off NTP.

Usage
config ntp state [disabled|enabled]

Parameters:

disabled : Disable NTP function.

enabled: Enable NTP function, default enabled.

Example
admin@sonic:~$ sudo config ntp state disabled admin@sonic:~$ sudo config ntp state enabled Restarting ntp-config service...

config ntp vrf

This command is used to configure ntp vrf.

Usage
config ntp state [default|mgmt]

Parameters:

default:

mgmt:

Example
admin@sonic:~$ sudo config ntp vrf default admin@sonic:~$ sudo config ntp vrf mgmt

```
Restarting ntp-config service...
```

31 PFC

Table of Contents

PFC Show commands

show pfc asymmetric

This command displays the status of asymmetric PFC for all interfaces or a given interface.

Usage
show pfc asymmetric [<interface>]

Example: Show on factory default
admin@sonic:~$ show pfc asymmetric Interface Asymmetric ---------- ---------- Ethernet0 N/A Ethernet4 N/A

Note: The factory default of asymmetric PFC is disabled and show as N/A.

Example: Show after configured
admin@sonic:~$ show pfc asymmetric Interface Asymmetric ---------- ---------- Ethernet0 on Ethernet2 off Ethernet4 off Ethernet6 off Ethernet8 off Ethernet10 off Ethernet12 off

Ethernet14 off

Example: Show on specify interface
admin@sonic:~$ show pfc asymmetric Ethernet0 Interface Asymmetric ---------- ---------- Ethernet0 off

show pfc priority

This command displays the lossless priorities for all interfaces or a given interface.

Usage
show pfc priority [<interface>]

Example
admin@sonic:~$ show pfc priority Interface Lossless priorities ---------- ---------- Ethernet0 3,4 Ethernet2 3,4 Ethernet8 3,4 Ethernet10 Ethernet16 3,4

Example

```
admin@sonic:~$ show pfc priority Ethernet0
Interface    Lossless priorities
-----------  --------------------
Ethernet0    3,4
```

show pfc counters

This command displays the details of Rx and Tx priority-flow-control (PFC) for all ports.

Usage
show pfc counters

Example

```
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
```

show qos pfc-priority-queue

This command displays the PFC-priority-to-queue mapping.

Usage
show qos pfc-priority-queue [<profile_name>]

Parameters:

- <profile_name>: Profile name.

Example
admin@sonic:~$ show qos pfc-priority-queue pfc-queue policy: pfc_queue_profile PFC Priority Queue ---------- ------- 0 0 1 2 2 2

show interface pfc config

This command displays the PFC configuration for all interfaces or a given interface.

Usage
show interface pfc config [<interface_name>]

Parameters:

<interface_name>: Physical interface name. For example: "Ethernet0".

Example
admin@sonic:~$ show interfaces pfc config Ethernet88 PFC mode: Symmetric PFC Lossless Priorities: 0,1 PFC to Queue: pfc_q_prof PFC Queue ----- ------- 0 2 1 2

PFC Configuration Commands

config interface pfc asymmetric

This command is used to set PFC asymmetric of an interface to "on"(enable) or "off"(disable).

Usage
config interface pfc asymmetric <interface_name> (on | off)

To disable PFC asymmetric on Ethernet0, use the following command:

Example
admin@sonic:~$ sudo config interface pfc asymmetric Ethernet0 on

config interface pfc priority

This command is used to enable ("on") or disable ("off") a PFC priority on an interface.

Usage
config interface pfc priority <interface_name> {0 | 1 | 2 | 3 | 4 | 5 | 6 | 7} {on | off}

To enable PFC priority 7 on Ethernet0, use the following command.

Example
admin@sonic:~$ sudo config interface pfc priority Ethernet0 7 on

Note:

- After configuring the aforementioned two types of PFC switches with traffic ports, it is necessary to restart the syncd Docker as follows:

  docker restart syncd

config qos pfc-priority-queue add

This command is used to create a profile of PFC-priority-to-queue mapping.

Usage
config qos pfc-priority-queue add <profile_name> --pfc-priority <pfc-priority> --queue <queue>

Parameters:

- <profile_name>: Profile name.
- <pfc-priority>: List of PFC priority. Minimum: 0. Maximum: 7. For example: "1", "1,2-3".
- <queue>: Queue. Minimum: 0. Maximum: 7.

Note:

- This command is only supported on the devices using Broadcom ASIC.

Example
sudo config qos pfc-priority-queue add pfc_queue_profile --pfc-priority 0 --queue 0

config qos pfc-priority-queue update

This command is used to modify an existing profile of PFC-priority-to-queue mapping.

Usage
config qos pfc-priority-queue update <profile_name> --pfc-priority <pfc-priority> [--queue <queue>] [--remove]

Parameters:

- <profile_name>: Profile name.
- <pfc-priority>: List of PFC priority. Minimum: 0. Maximum: 7. For example: "1", "1,2-3".
- <queue>: Queue. Minimum: 0. Maximum: 7.

- remove: Remove the mapping. For example: "--pfc-priority 1 --remove".

Note:

- This command is only supported on the devices using Broadcom ASIC.

Example
sudo config qos pfc-priority-queue update pfc_queue_profile --pfc-priority 1,2 --queue 2

config qos pfc-priority-queue del

This command is used to delete a profile of PFC-priority-to-queue mapping.

Usage
config qos pfc-priority-queue del <profile_name>

Parameters:

- <profile_name>: Profile name.

Note:

- This command is only supported on the devices using Broadcom ASIC.

Example
sudo config qos pfc-priority-queue del pfc_queue_profile

config interface qos pfc-priority-queue bind

This command is used to configure the PFC-priority-to-queue mapping on the specified interface.

Usage
config interface qos pfc-priority-queue bind <interface_name> <profile_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- <profile_name>: Profile name.

Default mapping:

PFC Priority	Queue
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Any packet field value that is not specified in the configuration is assigned to a default value.

Note:

- This command is only supported on the devices using Broadcom ASIC.

Example
sudo config interface qos pfc-priority-queue bind Ethernet0 pfc_queue_profile

config interface qos pfc-priority-queue unbind

This command is used to reset the PFC-priority-to-queue mapping on the specified interface.

Usage
config interface qos pfc-priority-queue unbind <interface_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".

Note:

- This command is only supported on the devices using Broadcom ASIC.

Example
sudo config interface qos pfc-priority-queue unbind Ethernet0

PFC Clear Commands

sonic-clear pfccounters

This command is used to clear the counters of Rx and Tx priority-flow-control for all ports.

Usage
sonic-clear pfccounters

Example
admin@sonic:~$ sonic-clear pfccounters Clear saved counters

32 PFC Watchdog

Table of Contents

A detailed description of the PFC Watchdog can be fount on this wiki page.

PFC Watchdog Configure Command

config pfcwd start

This command starts the PFC Watchdog.

Usage
config pfcwd start [--action (drop | forward | alert)] [--restoration-time <ms_value>] ports (all | <PORTS>) detection-time <ms_value>

Parameters

- all: All ethernet ports
- <PORTS> : <ethernet_interface_name> seperate by space ' ', e.g Ethernet0 Ethernet1 Ethernet2

Example: Sef pfcwd on all ethernet port
admin@sonic:~$ config pfcwd start --action drop --restoration-time 400 ports all detection-time 400

Example: Sef pfcwd on Ethernet0
admin@sonic:~$ config pfcwd start --action drop --restoration-time 400 ports Ethernet0 detection-time 400

Example: Sef pfcwd on Ethernet0 and Ethernet4
admin@sonic:~$ config pfcwd start --action drop --restoration-time 400 ports Ethernet0 Ethernet4 detection-time 400

config pfcwd stop

This command stops the PFC Watchdog.

Usage
config pfcwd stop

Example: Stop pfcwd on all ports
admin@sonic:~$ config pfcwd stop

config pfcwd interval

This command sets the PFC Watchdog counter polling interval (ms).

Usage
config pfcwd interval <interval_in_ms>

Example
admin@sonic:~$ config pfcwd interval 200

config pfcwd counter_poll

This command enables or disables the PFC Watchdog related counters polling.

Usage
config pfcwd counter_poll (enable | disable)

Example
admin@sonic:~$ config pfcwd counter_poll disable

config pfcwd big_red_switch

This command enables or disables the PFC Watchdog's "BIG RED SWITCH"(BRS). When enabled, the BRS PFC Watchdog will be disabled on all ports/queues it is configured for no matter whether a storm was detected or not.

Usage
config pfcwd big_red_switch (enable | disable)

Example
admin@sonic:~$ config pfcwd big_red_switch enable

(Not supported) config pfcwd start_default

This command starts the PFC Watchdog with the default settings.

Usage
config pfcwd start_default

Default values are the following:

- detection time - 200ms
- restoration time - 200ms
- polling interval - 200ms
- action - 'drop'
- Additionally, if the number of ports in the system exceeds 32, all times will be multiplied by roughly <num_ports>/32 + 1.

Example
admin@sonic:~$ config pfcwd start_default

Note: Due to the incomplete implementation of config pfcwd start_default , this command malfunctions.

PFC Watchdog Show Command

show pfcwd config

This command shows the current PFC Watchdog configuration.

Usage
show pfcwd config

Example
admin@sonic:~$ show pfcwd config PORT ACTION DETECTION TIME RESTORATION TIME --------- -------- ---------------- ------------------ Ethernet0 drop 400 400

show pfcwd stats

This command shows the current PFC Watchdog statistics (storms detected, packets dropped, etc).

Usage
show pfcwd stats

Example
admin@sonic:~$ show pfcwd stats QUEUE STATUS STORM DETECTED/RESTORED TX OK/DROP RX OK/DROP TX LAST OK/DROP RX LAST OK/DROP ----------- ----------- ------------------------ ------------ ------------ -----------------

```
----------------
Ethernet0:3     stormed                 1/0     100/300     100/300          0
/200            0/200
Ethernet0:4  operational                2/2     100/100     100/100          0
/0              0/0
```

33 Policer

Table of Contents

This section explains various show and configuration commands available for users.

Policer Show Commands

show policer

This command displays a summary of the policer configuration.

Usage
show policer

Example
admin@sonic:~$ show policer Name Type Mode Color Source CIR CBS PIR PBS Green Packet Action YellowPacket Action Red Packet Action ---------- ------ ------ ---------- ----- ----- ----- ----- ---------- ---------- ---------- POLICER_TR_TCM bytes tr_tcm blind 1500 3000 2000 4000 forward forward drop

SP4 Example
admin@sonic:~$ show policer Name Type Mode Color Source CIR CBS PIR PBS Green Packet Action Yellow Packet Action Red Packet Action ---------- ------ ------ ---------- ------ ----- ----- ----- ---------- ---------- ---------- POLICER_TR_TCM bytes tr_tcm blind 1 Mbps 1 Kib 2 Mbps 3 Kib forward forward drop

Note: If the type of mellanox switch policer is bytes, the value will be converted to the corresponding unit. If the type is pakcets, it will be consistent with the display of Broadcom switches

Policer Config Commands

config policer add

This command is used to add a policer.

Usage
config policer add <policer_name> sr_tcm <meter_type> <color_source> [--cir <cir>] [--cbs <cbs>] [--pbs <pbs>] [--green_packet_action <green_packet_action> | --green_set_tc <green_set_tc> | --green_set_dscp <green_set_dscp> | --green_set_cos <green_set_cos>] [--yellow_packet_action <yellow_packet_action> | --yellow_set_tc <yellow_set_tc> | --yellow_set_dscp <yellow_set_dscp> | --yellow_set_cos <yellow_set_cos>] [--red_packet_action <red_packet_action> | --red_set_tc <red_set_tc> | --red_set_dscp <red_set_dscp> | --red_set_cos <red_set_cos>] config policer add <policer_name> tr_tcm <meter_type> <color_source> [--cir <cir>] [--cbs <cbs>] [--pir <pir>] [--pbs <pbs>] [--green_packet_action <green_packet_action> | --green_set_tc <green_set_tc> | --green_set_dscp <green_set_dscp> | --green_set_cos <green_set_cos>] [--yellow_packet_action <yellow_packet_action> | --yellow_set_tc <yellow_set_tc> | --yellow_set_dscp <yellow_set_dscp> | --yellow_set_cos <yellow_set_cos>] [--red_packet_action <red_packet_action> | --red_set_tc <red_set_tc> | --red_set_dscp <red_set_dscp> | --red_set_cos <red_set_cos>] config policer add <policer_name> storm_control <meter_type> <color_source> [--cir <cir>] [--cbs <cbs>] [--green_packet_action <green_packet_action> | --green_set_tc <green_set_tc> | --green_set_dscp <green_set_dscp> | --green_set_cos <green_set_cos>] [--red_packet_action <red_packet_action> | --red_set_tc <red_set_tc> | --red_set_dscp <red_set_dscp> | --red_set_cos <red_set_cos>]

Parameters:

- policer_name: Policer name. The maximum length is 16.
- meter_type: The unit of metering. Valid options are the following:
  - bytes
  - packets, packets mode is only supported on Broadcom switches.
- color_source: Be aware of or ignore the pre-coloring of packets.
  - aware
  - blind
- cir: Bandwidth limit for guaranteed traffics. It ranges from:

  - 1000 to 12500000000 in bytes mode,
  - 1 to 148809523 in packets mode.
- cbs: Maximum packet size permitted for bursts of data that exceed the c ir. It ranges from:
  - 2000 to 256000000 in bytes mode,
  - 1 to 536576 in packets mode.
- pir: Bandwidth limit for peak traffics. It ranges from:
  - 1000 to 12500000000 in bytes mode,
  - 1 to 148809523 in packets mode.
- pbs: Maximum packet size permitted for bursts of data that exceed the pir. It ranges from:
  - 2000 to 256000000 in bytes mode,
  - 1 to 536576 in packets mode.
- green_packet_action: Specifies the action for green packets. Valid options are as follows:
  - forward
  - drop, drop mode is only supported on Broadcom switches.
- yellow_packet_action: Specifies the action for yellow packets. Valid options are the following:
  - forward
  - drop, drop mode is only supported on Broadcom switches.
- red_packet_action: Specifies the action for red packets. Valid options are the following:
  - forward
  - drop
- green_set_cos: Enables changing the VLAN PCP value for green packets. The valid range is 0 to 7. This action is only available for ACL. (Supported only on Broadcom switches.)
- yellow_set_cos: Enables changing the VLAN PCP value for yellow packets. Valid range is 0 to 7. This action is only ava liable for ACL. (Supported only on Broadcom switches.)
- red_set_cos: Enables changing the VLAN PCP value for red packets. Valid range is 0 to 7. This action is only ava liable for ACL. (Supported only on Broadcom switches.)
- green_set_dscp: Enables changing the DSCP for green packets. Valid range is 0 to 63. This action is only ava liable for ACL. (Supported only on Broadcom switches.)
- yellow_set_dscp: Enables changing the DSCP for yellow packets. Valid range is 0 to 63. This action is only ava liable for ACL. (Supported only on Broadcom switches.)

- red_set_dscp: Enables changing the DSCP for red packets. Valid range is 0 to 63. This action is only ava liable for ACL. （Supported only on Broadcom switches.）
- green_set_tc: Enables changing the Traffic Class (TC) for green packets. Valid range is 0 to 7. This action is only ava liable for ACL. （Supported only on Broadcom switches.）
- yellow_set_tc: Enables changing the Traffic Class (TC) for yellow packets. Valid range is 0 to 7. This action is only ava liable for ACL. （Supported only on Broadcom switches.）
- red_set_tc: Enables changing the Traffic Class (TC) for red packets. Valid range is 0 to 7. This action is only ava liable for ACL. （Supported only on Broadcom switches.）

The following example shows how to create a policer named "POLICER_TR_TCM" with tr_tcm mode, meter type "bytes", color source "blind", cir = 1000, cbs = 2000, pir = 2000, pbs = 4000, which drops packets marked red by the meter.

Example
admin@sonic:~$ sudo config policer add POLICER_TR_TCM tr_tcm bytes blind --cir 1000 --cbs 2000 --pir 2000 --pbs 4000 --green_packet_action forward --yellow_packet_action forward --red_packet_action drop

The following example shows how to create a policer named "POLICER_TR_TCM" with the "tr_tcm" mode, meter type "bytes", color source "blind", cir = 1000, cbs = 2000, pir = 2000, pbs = 4000, which remarks IP DSCP by the meter's marked color: green to 8, yellow to 16, and red to 24.

Example
admin@sonic:~$ sudo config policer add POLICER_TR_TCM tr_tcm bytes blind --cir 1000 --cbs 2000 --pir 2000 -- pbs 4000 --green_set_dscp 8 --yellow_set_dscp 16 --red_set_dscp 24

config policer update

This command is used to update an existing policer.

Usage
config policer update <policer_name> [--cir <cir>] [--cbs <cbs>] [--pir <pir>] [--pbs <pbs>]

Parameters:

- cir: Bandwidth limit for guaranteed traffics. It ranges from:
  - 1000 to 12500000000 in bytes mode,
  - 1 to 148809523 in packets mode.
- cbs: Maximum packet size permitted for bursts of data that exceed the c ir. It ranges from:
  - 2000 to 256000000 in bytes mode,
  - 1 to 536576 in packets mode.
- pir: Bandwidth limit for peak traffics. It ranges from:
  - 1000 to 12500000000 in bytes mode,
  - 1 to 148809523 in packets mode.
- pbs: Maximum packet size permitted for bursts of data that exceed the pir. It ranges from:
  - 2000 to 256000000 in bytes mode,
  - 1 to 536576 in packets mode

The following example updates a policer named POLICER_TR_TCM with cir = 1500, cbs = 3000.

Example
admin@sonic:~$ sudo config policer update POLICER_TR_TCM --cir 1500 --cbs 3000

config policer remove

This command is used to remove a policer.

Usage
config policer remove <policer_name>

The following example removes a policer named POLICER_TR_TCM.

Example
admin@sonic:~$ sudo config policer remove POLICER_TR_TCM

34 Port Channels

This section includes port channel creation, addition (or removal) of members, and deletion.

While creating a port channel, the user may specify whether the port channel is static (manually configured) or dynamic (running LACP protocol) which should be consistent with the peer switch.

Port Channel Show Commands

show interfaces portchannel

The **show interfaces portchannel** command displays all the port channels that are configured in the device and their status.

Example

```
admin@sonic:~$ show interfaces portchannel
Flags: A - active, I - inactive, Up - up, Dw - Down, N/A - not available,
       S - selected, D - deselected, * - not synced,
       M - mixed speed

  No.  Team Dev       Protocol     Ports                  Oper Key  Admin Key  Fast Rate
System ID    System Priority    Dev Number      Max Ports
-----  ------------   -----------  -------------------------  --------  ---------  ---------
---------    ----------------   ----------      ---------
   0  PortChannel0    LACP(A)(Up)  Ethernet0(S) Ethernet4(S)    1        1         false
N/A         N/A              N/A           64
   2  PortChannel2    NONE(-)(Up)  Ethernet2(S) Ethernet1(S)    N/A      N/A       N/A
N/A         N/A              N/A           64
   5  PortChannel5    LACP(A)(Dw)  N/A                    N/A      auto      false
N/A         N/A              N/A           64
   8  PortChannel8(M) LACP(A)(Up)  Ethernet8(S) Ethernet12(S)   8        8         ture
N/A         N/A              N/A           64
  24  PortChannel24   LACP(A)(Up)  Ethernet28(S) Ethernet24(S)  124      auto      false
N/A         N/A              N/A           64
  40  PortChannel40   LACP(A)(Up)  Ethernet44(S) Ethernet40(S)  40       40        false
N/A         N/A              N/A           64
  48  PortChannel48   LACP(A)(Up)  Ethernet52(S) Ethernet48(S)  48
N/A         N/A              N/A           64
```

The parameters are as below:

- Protocol
    - LACP protocol mode, active (A) or inactive(I) on the port channel.
        - LACP(A) means LACPDU frames are sent along the configured links periodically .

        - LACP(I) means the port channel is not in an active negotiating state. It acts as "speak when spoken to", does respond to incoming LACP packets.
    - The 'NONE(-)' keyword means static port channel.
    - The port channel state, (Up) or (Dw).
- Ports
    - S - selected, the port is already attached to the port channel and ready to transmit and receive.
    - D - deselected, the port is not attached to the port channel yet.
    - * - not synced, the port is not synchronized. It is currently not in the right aggregation.
- Oper Key and Admin Key
    - The Admin Key is specified value in "--lacp-key" option of config portchannel add command.
    - The Oper Key is value of actually participating in the LACP protocol.
    - The Admin Key and Oper Key are always N/A for static port channel.
- Fast Rate
    - It is used to set the rate at which the LACP control packets are sent from partner.
        - true means LACP fast rate mode, request partner to transmit LACPDUs every 1 second
        - false means LACP slow rate mode, request partner to transmit LACPDUs every 30 seconds N/A, it is meaningless for static port channel.
- Mix Speed
    - M - Show which portchannel is in mixed speed mode.
        - In mixed speed mode, it is allowed to combine ports with different speeds into a single port channel.

Note

- If user creates a LACP port channel, and sets lacp-key as "auto", the "Oper Key" value will be generated automatically after first port channel member is added to port channel.

Port Channel Config Commands

This sub-section explains how to configure a port channel and its member ports.

config portchannel

The command config portchannel is used to add or delete a port channel. User can specify some attributes of

the port channel when adding the port channel name.

Usage
config portchannel add <portchannel_name> [--min-links <num_min_links>] [--fallback {true | false}] [--lacp-key {auto | <num_lacp_key>}] [--static {true | false}] [--fast-rate (true | false)] [--mix-speed (true |false)] [--system-id <system_id_value>] [--system-priority <system_priority_value>] [--dev-num <dev_num_value>] [--mode {active | passive}] [--max-ports <num_max_ports>]
config portchannel del <portchannel_name>

Parameters:

- add , add a new port-channel name in the system.
    - default attributes: LACP protocol, if no options specified or if the option " –static" not specified.
- del , delete the port-channel name from the system. User doesn't need to specify any options.
- <portchannel_name> , the port channel name to be added or deleted.
    - The syntax of port channel name is "PortChannel"+<suffix> where <suffix> range is 0..9999
    - For example, <suffix> uses "200", the name could be "PortChannel200".
- --min-links <num_min_links> , minimum number of links in the LACP port channel before the LACP port channel can be brought up and active.
    - The default value is 1.
    - The range from 1 to 1024.
- --fallback option , LACP fallback feature can be enabled/disabled.
    - true , enable LACP fallback, which keep the port channel stays in "up" before receiving any LACP PDUs from peer DUT.
    - false , disable LACP fallback, turn the port channel state to down when it does not receive the LACP PDUs from peer DUT.
    - The default value is false.
- --lacp-key , specify the exchanged lacp-key in LACP protocol, either auto or <num_lacp_key>
    - auto, it concatenates "1"+<suffix> as the key. For example, <suffix> uses "200", the lacp_key would be "1200" .
    - <num_lacp_key> , the range of given number from 1 to 65535.
    - The default value is auto.
- --lacp-system-id - Specifies the LACP system ID in the format of xxxx.xxxx.xxxx. If not specified, it will be the MAC of the DUT.

- --lacp-system-priority - Configures the LACP system priority. The value ranges from 0 to 65535. The default value is 65535.
- --dev-number - It's used to extended the actor port id, the formula for calculating the extended port id is: port + (dev-number - 1) * 10000. The value ranges from 1 to 6. The default value is 1.
- --static , specify the port channel type, either true for static port channel or false for dynamic LACP port channel.
- --fast-rate , specify LACP rate mode.
    - true, LACP fast rate mode, request partner to transmit LACPDUs every 1 second. LACP timeout is 3 seconds.
    - false, LACP slow rate mode, request partner to transmit LACPDUs every 30 seconds. LACP timeout is 90 seconds.
    - the default value is false.
- --mix-speed , specify whether the port channel is allowed to combine ports with different speeds into a single port channel. Default is false.
- --mode, specifies the operation mode of the port within the aggregation group, which is divided into two modes: active and passive. The default is active.
    - active, in active mode, the device will proactively send LACP packets to establish link aggregation.
    - passive, in passive mode, the device does not proactively send LACP packets but can respond to LACP packets sent from the peer to establish link aggregation.
- --max-ports, specifies the maximum number of ports in the aggregation group. The default is 64, with a range from 1 to 64.

Note

1. The member of a portchannel cannot be added into another portchannel.

   If any port is already a member of a port channel and a user tries to add the same port to another port channel (without first deleting it from the current port channel), the command fails and error message is printed. In such cases, remove the member port from the current port channel and then add it to new port channel.

2. Portchannel cannot be deleted if there is any configured member.

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.

3. Refer to https://github.com/Azure/SONiC/blob/master/doc/lag/LACP Fallback Feature for SONiC_v0.5.md for more details about the fallback feature.

4. Only --static option is required when adding static port channel. Extra option, such as lacp_key, min_link, fast_rate, fallback or mode, would cause an error.

5. The attributes of created port channel cannot be modified or changed.

   If port channel is already created and user tries to specify options to change port channel attributes, the command fails and error message is printed.

Example of creating a LACP port channel with the name: "PortChannel200".

Example 1
admin@sonic:~$ sudo config portchannel add PortChannel200

Example of creating a static port channel with the name "PortChannel300" and specify "--static true".

Example 2
admin@sonic:~$ sudo config portchannel add PortChannel300 --static true

Example of creating a mixed speed port channel with the name "PortChannel300", and specify "--mix speed".

Example 3
admin@sonic:~$ sudo config portchannel add PortChannel300 --mix-speed true

Example of deleting a port channel with the name "PortChannel200".

Example 4
admin@sonic:~$ sudo config portchannel del PortChannel200

config portchannel member

The command config portchannel adds or deletes a member port to/from the existing port channel.

Usage
config portchannel member {add | del} <portchannel_name> <member_portname>

Example: add interface Ethernet4 as a member of port channel "PortChannel200".

Example
admin@sonic:~$ sudo config portchannel member add PortChannel200 Ethernet4

35 Port Rate Limit

Table of Contents

This section explains the commands of limiting the rate of transmission. It could be counted in bytes or packets.(Only supported on Broadcom switches of this chapter.)

Port Rate Limit Show Commands

show interface rate-limit

To display the rate limit configuration on an interface, use show interface rate-limit command.

Usage
show interface rate-limit [<interface_name>]

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".

Example
admin@sonic:~$ show interface rate-limit Interface Meter Type Rate Burst Size ---------- ---------- --------- ---------- Ethernet0 bytes 100 kbps 1 Kib

Port Rate Limit Configuration Commands

config interface rate-limit add

To enable to limit the in comming traffic rate on a port, use config interface rate-limit add command.

Usage
config interface rate-limit add <interface_name> --meter-type {bytes|packets} --rate <rate> [--burst-size <burst_size>>]

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- meter-type: Meter type. Valid values are:
    - bytes : Meter type as bytes mode.
    - packets : Meter type as packets mode.
- <rate>: Maximum rate of ingress traffic in kilo-bits/second (kbps) or packet/second (pps). Valid values are:
    - If meter-type is bytes :
        - The format is a decimal number or a decimal number followed by the abbreviation k (1,000), m (1,000,000), or g (1,000,000,000). Minimum: 8 kbps (32 kbps for AS8000 and AS9746-32D). Maximum: 400,000,000 kbps. For example: "10", "10k".
    - If meter-type is packets :
        - Minimum: 1 pps. Maximum: 148,809,523 pps.
- <burst_size>: The burst size in bytes or packets. If burst size is not given, the default value of bytes mode and packet mode are <rate> × 10 and <rate> ÷ 8 × 10 milliseconds respectively. Valid values are:
    - If meter-type is bytes :
        - The format is a decimal number of a decimal number followed by the abbreviation k (210), or m (220). Minimum: 2,000 bytes. Maximum: 256,000,000 bytes. For example: "100", "100k".
    - If meter-type is packets :
        - Minimum: 1 pps. Maximum: 536,576 pps.

Example
sudo config interface rate-limit add Ethernet0 --meter-type bytes --rate 10g --burst-size 9100

config interface rate-limit del

Disable to limit the in comming raffic rate on a port, use config interface rate-limit del command.

Usage
config interface rate-limit del <interface_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".

Example
sudo config interface rate-limit del Ethernet0

36 PVST

Table of Contents

This section describes PVST (STP) feature and commands which are supported in SONiC.

PVST (Per VLAN Spanning Tree) is a feature in SONiC, SONiC_PVST_HLD, which planned in 202106 branch. It supports STP (802.1D Spanning Tree) for those ports, assigned to un tagged VLAN1, but there is an issue - dual root bridge when interacts with 802.1D switch.

To resolve this, MX SONiC adding stp mode in config spanning-tree command, which runs a single spanning tree instance for all portswhich is a member of any VLAN, and disables other instances in PVST.

PVST show commands

show spanning-tree

This command displays spanning tree information .

Note:

- VLAN related settings cannot be displayed when spanning-tree mode is stp.

Usage
show spanning-tree show spanning-tree vlan <vlanid> show spanning-tree vlan <vlanid> interface <ifname>

Example
admin@sonic:~$ show spanning-tree vlan 100 Spanning-tree Mode: PVST VLAN 100 - STP instance 3 ---------- STP Bridge Parameters: Bridge Bridge Bridge Bridge Hold LastTopology Topology Identifier MaxAge Hello FwdDly Time Change Change hex sec sec sec sec sec cnt 8000002438eefbc3 20 2 15 1 0 0 RootBridge RootPath DesignatedBridge RootPort Max Hel Fwd Identifier Cost Identifier Age lo Dly hex hex sec sec sec 8000002438eefbc3 0 8000002438eefbc3 Root 20 2 15 STP Port Parameters: Port Prio Path Port Uplink State Designated Designated Designated Name rity Cost Fast Fast Cost Root Bridge Ethernet13 128 4 Y N FORWARDING 0 8000002438eefbc3 8000002438eefbc3

show spanning-tree bpdu_guard

This command displays the interfaces which are BPDU guard enabled and also the state if the interface is disabled due to BPDU guard.

Usage
show spanning-tree bpdu_guard

Example
admin@sonic:~$ show spanning-tree bpdu_guard PortNum Shutdown Port shut Configured due to BPDU guard --- Ethernet1 Yes Yes Ethernet2 Yes No Port-Channel2 No NA

show spanning-tree root_guard

This command displays the interfaces where root guard is active and the pending time for root guard timer expiry

Usage
show spanning-tree root_guard

Example
admin@sonic:~$ show spanning-tree root_guard

```
Root guard timeout: 120 secs
Port        VLAN    Current State
------------------------------------------------
Ethernet1   1       Inconsistent state (102 seconds left on timer)
Ethernet8   100     Consistent state
```

show spanning-tree statistics

show spanning-tree statistics vlan <vlanid>

This command displays the spanning-tree bpdu statistics. Statistics will be synced to APP DB every 10 seconds

Usage
show spanning-tree statistics show spanning-tree statistics vlan <vlanid>

Example

```
admin@sonic:~$ show spanning-tree statistics vlan 100
VLAN 100 - STP instance 3
---------------------------------------------------------------------
PortNum          BPDU Tx    BPDU Rx    TCN Tx     TCN Rx
Ethernet13       10         4          3          4
PortChannel15    20         6          4          1
```

PVST configuration commands

config spanning-tree

This command enables/disables the spanning tree mode for the device. pvst and stp are exclusive. User's configuration should be one of (pvst, stp, disable).

Usage
config spanning-tree {enable|disable} {pvst | stp}

option

- pvst: Per VLAN Spanning Tree mode. When enabled, it enables multi-spanning tree instances for first 255 VLANs. The first
- instance is for VLAN 1 and delivers BPDU for untagged member interface.
- stp: (802.1D) Spanning Tree mode. When enabled, it enables 1st spanning tree instance with system id (0) and disable other instance. All ports which is member of VLAN, either tagged or untagged, are joined the instance.

Note:

- Only one mode can be enabled at any given time. That is, the configuration should be one of (disable, pvst, stp).
- When switching the mode, eg pvst to stp, it will stop pvst and then start stp.

Example
admin@sonic:~$ sudo config spanning-tree enable pvst

config spanning-tree forward_delay

This command allows configuring the forward delay time in seconds (default = 15), range 4-30.

Note:

- 2*(forward_delay-1) >= max_age >= 2*(hello_time +1).
- The specified value on the global level command will also apply to value on these VLAN if original per-VLAN value is same as the global one.

Usage
config spanning-tree forward_delay <value>

Example
admin@sonic:~$ sudo config spanning-tree forward_delay 30

config spanning-tree hello

This command allow configuring the hello interval in secs for transmission of bpdus (default = 2), range 1-10.

Note:

- 2*(forward_delay-1) >= max_age >= 2*(hello_time +1).
- The specified value on the global level command will also apply to value on these VLAN if original per-VLAN value is same as the global one.

Usage
config spanning-tree hello <value>

Example
admin@sonic:~$ sudo config spanning-tree hello 10

config spanning-tree max_age

This command allows configuring the maximum time to listen for root bridge in seconds (default = 20), range 6-40.

Note:

- 2*(forward_delay-1) >= max_age >= 2*(hello_time +1).
- The specified value on the global level command will also apply to value on these VLAN if original per-VLAN value is same as the global one.

Usage

config spanning-tree max_age <value>

Example
admin@sonic:~$ sudo config spanning-tree max_age 40

config spanning-tree priority

This command allows configuring the bridge priority in increments of 4096 (default = 32768), range 0-61440.

Note:

- The specified value on the global level command will also apply to value on these VLAN if original per-VLAN value is same as the global one.

Usage
config spanning-tree priority <value>

Example
admin@sonic:~$ sudo config spanning-tree priority 61440

config spanning-tree root_guard_timeout

This command allows configuring a root guard timeout value. Once superior BPDUs stop coming on the port, device will wait for a

period until root guard timeout before moving the port to forwarding state(default = 30 secs), range 5-600.

Usage

config spanning-tree root_guard_timeout <value>

Example
admin@sonic:~$ sudo config spanning-tree root_guard_timeout 600

config spanning-tree vlan

This command allows enabling or disabling spanning-tree on a VLAN.

Note:

- VLAN related settings cannot be configured when spanning-tree mode is stp.

Usage
config spanning-tree vlan {enable|disable} <vlan>

Example
admin@sonic:~$ sudo config spanning-tree vlan enable 1

Below commands are similar to the global level commands but allow configuring on per VLAN basis.

Usage
config spanning-tree vlan forward_delay <vlan> <fwd-delay-value> config spanning-tree vlan hello <vlan> <hello-value> config spanning-tree vlan max_age <vlan> <max-age-value> config spanning-tree vlan priority <vlan> <priority-value>

Example
admin@sonic:~$ sudo config spanning-tree vlan priority 1 61440

config spanning-tree vlan interface cost

This command allows to configure the port level cost value for a VLAN, range 1 - 200000000

Usage
config spanning-tree vlan interface cost <vlan> <ifname> <value>

Example
admin@sonic:~$ sudo config spanning-tree vlan interface cost 1 Ethernet0 10

config spanning-tree vlan interface priority

This command allows to configure the port level priority value for a VLAN, range 0 - 240 (default 128)

Usage
config spanning-tree vlan interface priority <vlan> <ifname> <value>

Example
admin@sonic:~$ sudo config spanning-tree vlan interface priority 1 Ethernet0 240

config spanning-tree interface

This command allows enabling or disabling of STP on an interface, by default STP will be enabled on the interface if global STP mode is configured.

Usage
config spanning-tree interface {enable|disable} <ifname>

Example
admin@sonic:~$ sudo config spanning-tree interface enable Ethernet0

config spanning-tree interface root_guard

This command allow enabling or disabling of root guard on an interface.

Usage
config spanning-tree interface root_guard {enable|disable} <ifname>

Example
admin@sonic:~$ sudo config spanning-tree interface root_guard enable Ethernet0

config spanning-tree interface bpdu_guard

Below command allows enabling or disabling of bpdu guard on an interface.

Usage

config spanning-tree interface bpdu_guard {enable|disable} <ifname>

By default, BPDU guard will only generate a syslog indicating the condition, for taking an action like disabling the port below

command can be used with shutdown option

Usage
config spanning-tree interface bpdu_guard {enable|disable} <ifname> [--shutdown | -s]

Example
admin@sonic:~$ sudo config spanning-tree interface bpdu_guard enable Ethernet0

config spanning-tree interface portfast

Below command allows enabling or disabling of portfast on an interface.

Usage
config spanning-tree interface portfast {enable|disable} <ifname>

Example
admin@sonic:~$ sudo config spanning-tree interface portfast enable Ethernet0

config spanning-tree interface uplink_fast

Usage

config spanning-tree interface uplink_fast {enable|disable} <ifname>

Example
admin@sonic:~$ sudo config spanning-tree interface uplink_fast enable Ethernet0

config spanning-tree interface priority

This command allows to configure the port level priority value, range 0 - 240 (default 128)

Usage
config spanning-tree interface priority <ifname> <value>

Example
admin@sonic:~$ sudo config spanning-tree interface priority Ethernet0 240

configure spanning-tree interface cost

This command allows to configure the port level cost value, range 1 - 200000000

Usage
config spanning-tree interface cost <ifname> <value>

Example
admin@sonic:~$ sudo config spanning-tree interface cost Ethernet0 1000

PVST debug commands

debug spanning-tree

Following debug commands will be supported for enabling additional logging which can be viewed in

/var/log/stpd.log, orchangent related logs can be viewed in /var/log/syslog.

Usage
debug spanning-tree debug spanning-tree bpdu [tx|rx] debug spanning-tree event debug spanning-tree interface <ifname> debug spanning-tree verbose debug spanning-tree vlan <id>

Note

- This "debug spanning-tree" command must be enabled for logs to be written to log file, after enabling any of the below commands.

Example
admin@sonic:~$ debug spanning-tree Command: sudo stpctl dbg enable admin@sonic:~$ debug spanning-tree bpdu tx Command: sudo stpctl dbg bpdu tx-on admin@sonic:~$ debug spanning-tree event Command: sudo stpctl dbg event on admin@sonic:~$ debug spanning-tree verbose Command: sudo stpctl dbg verbose on admin@sonic:~$ debug spanning-tree vlan 1 Command: sudo stpctl dbg vlan 1 on admin@sonic:~$ debug spanning-tree interface Ethernet3

Command: sudo stpctl dbg port Ethernet3 on

To disable the debugging controls enabled '-d' or '--disable' option can be used, an example of disabling bpdu debugging is shown below.

Usage
debug spanning-tree bpdu -d

Example
admin@sonic:~$ debug spanning-tree bpdu -d Command: sudo stpctl dbg bpdu off

Follow commands can be used to reset and display the debugging controls enabled respectively

Usage
debug spanning-tree reset debug spanning-tree show

Example
admin@sonic:~$ debug spanning-tree bpdu -d Command: sudo stpctl dbg bpdu off admin@sonic:~$ debug spanning-tree show Command: sudo stpctl dbg show STP Debug Parameters ---------- STP debugging is : ON Verbose : ON Event : ON BPDU-RX : OFF

BPDU-TX : OFF Ports: 3 VLANs: 1

Following debug commands will be supported for displaying internal data structures

Usage
debug spanning-tree dump global debug spanning-tree dump vlan <vid> debug spanning-tree dump interface <vid> <ifname>

Example
admin@sonic:~$ debug spanning-tree dump interface 2 Ethernet3 Command: sudo stpctl port 2 Ethernet3 PORT CLASS - VLAN 2 PORT 3(Ethernet3) ========== port_id = 8 3 state = FORWARDING path_cost = 2000 designated_root = 0x800268215f8101b6 designated_cost = 0 designated_bridge = 0x800268215f8101b6 designated_port = Pri-8, Num-3 topology_change_acknowledge = 0 config_pending = 0 change_detection_enabled = 1 self_loop = 0 auto_config = 1 message_age_timer = INACTIVE 0 forward_delay_timer = INACTIVE 0

hold timer = INACTIVE 0 root_protect_timer = INACTIVE 0 forward_transitions = 1 rx_config_bpdu = 0 tx_config_bpdu = 266 rx_tcn_bpdu = 0 tx_tcn_bpdu = 0

PVST clear commands

sonic-clear spanning-tree

Following clear commands will be supported

Usage
sonic-clear spanning-tree statistics sonic-clear spanning-tree statistics vlan <vid> sonic-clear spanning-tree statistics vlan-interface <vid> <ifname> sonic-clear spanning-tree statistics interface <ifname>

Example
admin@sonic:~$ sonic-clear spanning-tree statistics All stats cleared admin@sonic:~$ sonic-clear spanning-tree statistics vlan 1 Stats cleared for VLAN 1 admin@sonic:~$ sonic-clear spanning-tree statistics vlan-interface 1 Ethernet0 Stats cleared for VLAN 1 Ethernet0 admin@sonic:~$ sonic-clear spanning-tree statistics interface Ethernet0 Stats cleared for Ethernet0

37 QoS

Table of Contents

Qos Classification

Classification Show Commands

show qos dot1p-tc

This command is used to display the Dot1p-to-TC profile(s).

Usage
show qos dot1p-tc [<profile_name>]

Parameters:

- <profile_name>: Profile name.

Example
admin@sonic:~$ show qos dot1p-tc dot1p-tc policy: dot1p_to_tc_profile Dot1p TC ------- ---- 0 2 1 3 2 4 dot1p-tc policy: dot1p_to_tc_profile2 Dot1p TC ------- ---- 2 3 3 3 4 3 5 3

show qos dscp-tc

This command is used to display the DSCP-to-TC profile(s).

Usage
show qos dscp-tc [<profile_name>]

Parameters:

- <profile_name>: Profile name.

Example
admin@sonic:~$ show qos dscp-tc dscp-tc policy: dscp_to_tc_profile

DSCP	TC
0	0
8	1
16 24	2

show qos tc-pg

This command is used to display the TC-to-PG profile(s).

Usage
show qos tc-pg [<profile_name>]

Parameters:

- <profile_name>: Profile name.

Example
admin@sonic:~$ show qos tc-pg tc-pg policy: tc_pg_prof1 TC PG ---- ---- 2 3 3 3 4 3 5 3

show qos tc-queue

This command is used to display the Tc-to-queue profile(s).

Usage
show qos tc-queue [<profile_name>]

Parameters:

- <profile_name>: Profile name.

Example
admin@sonic:~$ show qos tc-queue tc-queue policy: tc_to_queue_profile TC Queue ---- ------- 0 0 1 2 2 2

SP4 Example
admin@sonic:~$ show qos tc-queue tc-queue policy: tc_to_queue_profile TC Queue ---- ------- 0 [0] 1 [2] 2 [2]

show interface qos

This command is used to display the QoS configuration for all interfaces or a given interface.

Usage
show interface qos [<interface_name>]

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".

Example
admin@sonic:~$ show interface qos Ethernet0: TC to Queue: tc_to_queue_profile Ethernet16:

Dot1p to TC: AZURE PFC to Queue: AZURE TC to PG: AZURE TC to Queue: AZURE Ethernet18: pfc-priority: 0 PFC to Queue: AZURE

Example
admin@sonic:~$ show interface qos Ethernet0 TC to Queue: tc_to_queue_profile

QoS Classification Configuration Commands

config qos dot1p-tc add

This command is used to create a Dot1p-to-TC profile.

Usage
config qos dot1p-tc add <profile_name> --dot1p <dot1p> --tc <tc>

Parameters:

- <profile_name>: Profile name.
- <dot1p>: List of dot1p. Minimum: 0. Maximum: 7. For example: "1", "1,2-3".
- <tc>: Traffic Class. Minimum: 0. Maximum: 7.

Example
sudo config qos dot1p-tc add dot1p_to_tc_profile --dot1p 0,1,2,3 --tc 0

config qos dot1p-tc update

This command is used to modify an existing Dot1p-to-TC profile.

Usage

config qos dot1p-tc update <profile_name> --dot1p <dot1p> [--tc <tc>] [--remove]

Parameters:

- <profile_name>: Profile name.
- <dot1p>: List of dot1p. Minimum: 0. Maximum: 7. For example: "1", "1,2-3".
- <tc>: Traffic Class. Minimum: 0. Maximum: 7.
- remove: Remove the mapping. For example: "--dot1p 1 --remove".

Example
sudo config qos dot1p-tc update dot1p_to_tc_profile --dot1p 0 --tc 1
sudo config qos dot1p-tc update dot1p_to_tc_profile --dot1p 4 --tc 0
sudo config qos dot1p-tc update dot1p_to_tc_profile --dot1p 1 --tc 0 --remove

config qos dot1p-tc del

This command is used to delete a Dot1p-to-TC profile.

Usage
config qos dot1p-tc del <profile_name>

Parameters:

- <profile_name>: Profile name.

Example
sudo config qos dot1p-tc del dot1p_to_tc_profile

config interface qos dot1p-tc bind

This command is used to configure Dot1p-to-TC mapping on the specified interface.

Usage
config interface qos dot1p-tc bind <interface_name> <profile_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".

- <profile_name>: Profile name.

Default mapping： The following table shows the default mapping on Broadcom platform.

DOT1P	TC
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Any packet field value that is not specified in the configuration is assigned to a default value.

Example
sudo config interface qos dot1p-tc bind Ethernet0 dot1p_to_tc_profile

config interface qos dot1p-tc unbind

This command is used to reset Dot1p-to-TC mapping on the specified interface.

Usage
config interface qos dot1p-tc unbind <interface_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".

Example
sudo config interface qos dot1p-tc unbind Ethernet0

config qos dscp-tc add

This command is used to create a DSCP-to-TC profile.

Usage
config qos dscp-tc add <profile_name> --dscp <dscp> --tc <tc>

Parameters:

- <profile_name>: Profile name.
- <dscp>: List of DSCP. Minimum: 0. Maximum: 63. For example: "1", "1,2-3".
- <tc>: Traffic Class. Minimum: 0. Maximum: 7.

Example
sudo config qos dscp-tc add dscp_to_tc_profile --dscp 0,1,2,3 --tc 0

config qos dscp-tc update

This command is used to modify an existing DSCP-to-TC profile.

Usage
config qos dscp-tc update <profile_name> --dscp <dscp> [--tc <tc>] [--remove]

Parameters:

- <profile_name>: Profile name.
- <dscp>: List of DSCP. Minimum: 0. Maximum: 63. For example: "1", "1,2-3".
- <tc>: Traffic Class. Minimum: 0. Maximum: 7.
- remove: Remove the mapping. For example: "--dscp 1 --remove".

Example
sudo config qos dot1p-tc update dot1p_to_tc_profile --dot1p 0 --tc 1 sudo config qos dot1p-tc update dot1p_to_tc_profile --dot1p 4 --tc 0 sudo config qos dot1p-tc update dot1p_to_tc_profile --dot1p 1 --tc 0 --remove

config qos dscp-tc del

This command is used to delete a DSCP-to-TC profile.

Usage
config qos dscp-tc del <profile_name>

Parameters:

- <profile_name>: Profile name.

Example
sudo config qos dscp-tc del dscp_to_tc_profile

config interface qos dscp-tc bind

This command is used to configure the DSCP-to-TC mapping on the specified interface.

Usage
config interface qos dscp-tc bind <interface_name> <profile_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- <profile_name>: Profile name.

Default mapping:

DSCP	TC
0 ~ 63	0

Any packet field value that is not specified in the configuration is assigned to a default value.

Example
sudo config interface qos dscp-tc bind Ethernet0 dscp_to_tc_profile

config interface qos dscp-tc unbind

This command is used to reset the DSCP-to-TC mapping on the specified interface.

Usage

config interface qos dscp-tc unbind <interface_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".

Example
sudo config interface qos dscp-tc unbind Ethernet0

config qos tc-pg add

This command is used to create a TC-to-PG profile.

Usage
config qos tc-pg add <profile_name> --tc <tc> --pg <pg>

Parameters:

- <profile_name>: Profile name.
- <tc>: the TC (Traffic Class), or switch-priority, the value could be a list that is comma separated, valid range is 0 to 7. <pg>: the priority group value, valid range is 0 to 7 for Broadcom platform, 1 to 5 for Intel platform.

Example
sudo config qos tc-pg add tc_to_pg_profile --tc 0,1,2,3 --pg 0

config qos tc-pg update

This command is used to modify an existing TC-to-PG profile.

Usage
config qos tc-pg update <profile_name> --tc <tc> --pg <pg> [--remove]

Parameters:

- <profile_name>: Profile name.
- <tc>: the TC (Traffic Class), or switch-priority, the value could be a list that is comma separated, valid range is 0 to 7. <pg>: the priority group value, valid range is 0 to 7 for Broadcom platform, 1 to 5 for Intel platform.
- remove: Remove the mapping. For example: "--tc 1 --remove".

Example
sudo config qos tc-pg update tc_to_pg_profile --tc 0 --pg 1 sudo config qos tc-pg update tc_to_pg_profile --tc 4 --pg 0 sudo config qos tc-pg update tc_to_pg_profile --tc 1 --pg 0 --remove

config qos tc-pg del

This command is used to delete a TC-to-PG profile.

Usage
config qos tc-pg del <profile_name>

Parameters:

- <profile_name>: Profile name.

Example
sudo config qos tc-pg del tc_to_pg_profile

config interface qos tc-pg bind

This command is used to configure the TC-to-PG mapping on the specified interface.

Usage
config interface qos tc-pg bind {<interface_name> | all} <profile_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- all: All physical interfaces.
- <profile_name>: Profile name.

Default mapping:

The following table shows the default mapping on Broadcom Trident2plus, Trident3, Tomahawk and Tomahawk2 switches.

TC	PG
0 ~ 7	7

The following table shows the default mapping on Broadcom Trident4, Tomahawk3, and Tomahawk4 switches.

TC	PG
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

The following table shows the default mapping on Intel platform.

TC	PG
0 ~ 7	0

Any packet field value that is not specified in the configuration is assigned to a default value.

Example
sudo config interface qos tc-pg bind Ethernet0 tc_to_pg_profile

config interface qos tc-pg unbind

This command is used to reset the TC-to-PG mapping on the specified interface.

Usage
config interface qos tc-pg unbind {<interface_name> | all}

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- all: All physical interfaces.

Example

sudo config interface qos tc-pg unbind Ethernet0

config qos tc-queue add

This command is used to create a TC-to-queue profile.

Usage
config qos tc-queue add <profile_name> --tc <tc> --queue <queue>

SP4 Usage
config qos tc-queue add <profile_name> --tc <tc> --uc-queue <queue>

Parameters:

- <profile_name>: Profile name.
- <tc>: the TC (Traffic Class), or switch-priority, the value could <queue>: the queue value, valid range is 0 to 7.

Note:

- On the devices using Intel ASIC, it only supports one profile per system. The configuration is applied immediately after profile is added. Any packet field value that is not specified in the configuration is assigned to a default value.

Example
sudo config qos tc-queue add tc_to_queue_profile --tc 0,1,2,3 --queue 0

Sp4 Example
sudo config qos tc-queue add tc_to_queue_profile --tc 0,1,2,3 --uc-queue 0

config qos tc-queue update

This command is used to modify an existing TC-to-queue profile. The configuration is applied immediately after profile is updated on Intel platform.

Usage
config qos tc-queue update <profile_name> --tc <tc> --queue <queue> [--remove]

Sp4 Usage
config qos tc-queue update <profile_name> --tc <tc> --uc-queue <queue> [--remove]

Parameters:

- <profile_name>: Profile name.
- <tc>: the TC (Traffic Class), or switch-priority, the value could could be a list that is comma separated, valid range is 0 to 7.
- <queue>: the queue value, valid range is 0 to 7.
- remove: Remove the mapping. For example: "--tc 1 --remove".

Note:

- On the devices using Intel ASIC, it only supports one profile per system. The configuration is applied immediately after profile is added. Any packet field value that is not specified in the configuration is assigned to a default value.

Example
sudo config qos tc-queue update tc_to_queue_profile --tc 0 --queue 1 sudo config qos tc-queue update tc_to_queue_profile --tc 4 --queue 2 sudo config qos tc-queue update tc_to_queue_profile --tc 1 --queue 2 --remove

Sp4 Example
sudo config qos tc-queue update tc_to_queue_profile --tc 0 --uc-queue 1 sudo config qos tc-queue update tc_to_queue_profile --tc 4 --uc-queue 2 sudo config qos tc-queue update tc_to_queue_profile --tc 1 --uc-queue 2 --remove

config qos tc-queue del

This command is used to delete a TC-to-queue profile.

Usage

config qos tc-queue del <profile_name>

Parameters:

- <profile_name>: Profile name.

Example
sudo config qos tc-queue del tc_to_queue_profile

config interface qos tc-queue bind

This command is used to configure the TC-queue mapping on the specified interface. This command is not supported on Intel platform because configuration is applied immediately after profile is added or updated.

Usage
config interface qos tc-queue bind {<interface_name> | all} <profile_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- all: All physical interfaces.
- <profile_name>: Profile name.

Default mapping:

The following table shows the default mapping on Broadcom platform.

TC	Queue
0	0
1	1
2	2
3	3
4	4
5	5
6	6

7	7

Any packet field value that is not specified in the configuration is assigned to a default value.

Note:

- This command is only supported on the devices using Broadcom ASIC.

Example
sudo config interface qos tc-queue bind Ethernet0 tc_to_queue_profile

config interface qos tc-queue unbind

This command is used to reset the TC-to-queue mapping on the specified interface.

Usage
config interface qos tc-queue unbind {<interface_name> | all}

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- all: All physical interfaces.

Note:

- This command is only supported on the devices using Broadcom ASIC.

Example
sudo config interface qos tc-queue unbind Ethernet0

Qos Marking

QoS Marking Show Commands

show qos remark dot1p

This command is used to display the dot1p remarking profile(s).

Usage

show qos remark dot1p [<profile_name>]

Parameters:

- <profile_name>: Profile name.

Example
admin@sonic:~$ show qos remark dot1p dot1p policy: remark_dot1p_profile TC Dot1p ---- ------- 0 0 1 1 2 2

show qos remark dscp

This command is used to display the DSCP remarking profile(s).

Usage
show qos remark dscp [<profile_name>]

Parameters:

- <profile_name>: Profile name.

Example
admin@sonic:~$ show qos remark dscp dscp policy: remark_dscp_profile TC DSCP ---- ------ 0 2 1 9 2 17

QoS Marking Configuration Commands

config qos remark dot1p add

This command is used to create a Dot1p remarking profile.

Usage
config qos remark dot1p add <profile_name> --tc <tc> --dot1p <dot1p>

Parameters:

- <profile_name>: Profile name.
- <tc>: List of Traffic Class. Minimum: 0. Maximum: 7. For example: "1", "1,2-3"
- <dot1p>: Dot1p. Minimum: 0. Maximum: 7.

Example
sudo config qos remark dot1p add remark_dot1p_profile --tc 0 --dot1p 0

config qos remark dot1p update

This command is used to modify an existing Dot1p remarking profile.

Usage
config qos remark dot1p update <profile_name> --tc <tc> [--dot1p <dot1p>] [--remove]

Parameters:

- <profile_name>: Profile name.
- <tc>: List of Traffic Class. Minimum: 0. Maximum: 7. For example: "1", "1,2-3".
- <dot1p>: Dot1p. Minimum: 0. Maximum: 7
- remove: Remove the mapping. For example: "--tc 1 --remove".

Example
sudo config qos remark dot1p update remark_dot1p_profile --tc 1 --dot1p 1

config qos remark dot1p del

This command is used to delete a Dot1p remarking profile.

Usage
config qos remark dot1p del <profile_name>

Parameters:

- <profile_name>: Profile name.

Example
sudo config qos remark dot1p del remark_dot1p_profile

config interface qos remark dot1p bind

This command is used to enable Dot1p remarking on the specified interface.

Usage
config interface qos remark dot1p bind <interface_name> <profile_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- <profile_name>: Profile name.

Default mapping:

TC	Dot1p
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Any TC value that is not specified in the configuration is assigned to a default Dot1p value for rewriting.

Example
sudo config interface qos remark dot1p bind Ethernet0 remark_dot1p_profile

config interface qos remark dot1p unbind

This command is used to disable Dot1p remarking on the specified interface.

Usage
config interface qos remark dot1p unbind <interface_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".

Example
sudo config interface qos remark dot1p unbind Ethernet0

config qos remark dscp add

This command is used to create a DSCP remarking profile.

Usage
config qos remark dscp add <profile_name> --tc <tc> --dscp <dscp>

Parameters:

- <profile_name>: Profile name.
- <tc>: List of Traffic Class. Minimum: 0. Maximum: 7. For example: "1", "1,2-3".
- <dscp>: DSCP. Minimum: 0. Maximum: 63.

Example
sudo config qos remark dscp add remark_dscp_profile --tc 0 --dscp 2

config qos remark dscp update

This command is used to modify an existing DSCP remarking profile.

Usage
config qos remark dscp update <profile_name> --tc <tc> [--dscp <dscp>] [--remove]

Parameters:

- <profile_name>: Profile name.
- <tc>: List of Traffic Class. Minimum: 0. Maximum: 7. For example: "1", "1,2-3"
- <dscp>: DSCP. Minimum: 0. Maximum: 63.
- remove: Remove the mapping. For example: "--tc 1 --remove".

Example
sudo config qos remark dscp update remark_dscp_profile --tc 1 --dscp 9 sudo config qos remark dscp update remark_dscp_profile --tc 2 --dscp 17

config qos remark dscp del

This command is used to delete a DSCP remarking profile.

Usage
config qos remark dscp del <profile_name>

Parameters:

- <profile_name>: Profile name.

Example
sudo config qos remark dscp del remark_dscp_profile

config interface qos remark dscp bind

This command is ued to enable DSCP remarking on the specified interface.

Usage
config interface qos remark dscp bind <interface_name> <profile_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- <profile_name>: Profile name.

Default mapping:

TC	DSCP
0 ~ 7	0

Any TC value that is not specified in the configuration is assigned to a default DSCP value for rewriting.

Example
sudo config interface qos remark dscp bind Ethernet0 remark_dscp_profile

config interface qos remark dscp unbind

This command is used to disable DSCP remarking on the specified interface.

Usage
config interface qos remark dscp unbind <interface_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".

Example
sudo config interface qos remark dscp unbind Ethernet0

Qos Configuration Commands

config qos clear

This command is used 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. DOT1P_TO_TC_MAP
6. MPLS_TC_TO_TC_MAP
7. SCHEDULER
8. PFC_PRIORITY_TO_PRIORITY_GROUP_MAP
9. PORT_QOS_MAP
10. WRED_PROFILE

11. QUEUE
12. CABLE_LENGTH
13. BUFFER_POOL
14. BUFFER_PROFILE
15. BUFFER_PG
16. BUFFER_QUEUE

Usage
config qos clear

Example
admin@sonic:~$ sudo config qos clear

config qos reload

This command is used to clear and load the predefined lossless buffer configuration. The config qos clear command is issued by this command to clear all the QoS configuration. After this command, use config save command to save the configuration file, then use reboot command to restart the switch to take the change effect.

Usage
config qos reload

Example
admin@sonic:~$ sudo config qos reload Running command: /usr/local/bin/sonic-cfggen -d -t /usr/share/sonic/device/x86_64-dell_z9100_c2538-r0 /Force10-Z9100-C32/buffers.json.j2 >/tmp/buffers.json Running command: /usr/local/bin/sonic-cfggen -d -t /usr/share/sonic/device/x86_64-dell_z9100_c2538-r0

/Force10-Z9100-C32/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
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.

38 Rate

Rate Config Commands

config rate smoothing-interval

This command is used to change the window size of exponential moving average to make the rates and utilization values more smooth in the output of "show interface counters"

Usage
config rate smoothing-interval <interval>

Parameter:

- <interval>: The window size of exponential moving average.(The range is from 1 to 1000)

Example
admin@sonic:~$ sudo config rate smoothing-interval 20

39 Routing Stack

The SONiC software is agnostic of the routing software that is being used in the device. For example, users can use either the Quagga or FRR routing stack as per their requirement. A separate shell (vtysh) is provided to configure such routing stacks. Once users enter v tysh , they can use the routing stack specific commands as given in the following example.

Example (FRR Routing Stack)
admin@sonic:~$ vtysh Hello, this is FRRouting (version 7.2.1-sonic). Copyright 1996-2005 Kunihiro Ishiguro, et al. sonic# show route-map ZEBRA: route-map: RM_SET_SRC Invoked: 82595

```
permit, sequence 10 Invoked 82595
 Match clauses:
 Set clauses:
  src 10.1.0.32
 Call clause:
 Action:
  Exit routemap
```

Refer to the routing stack Quagga Command Reference or FRR Command Reference to know more about about the routing stack configuration.

40 SAG

Table of Contents

config sag ipv4 enable/disable

config sag ipv6 enable/disable

config sag interface sag ip add/del

SAG Show Commands

show sag

This command displays the global SAG configuration.

Usage
show sag

Example
admin@sonic:~#show sag Static Anycast Gateway Information MacAddress IPv4 IPv6 ---------- ------ ------ 00:11:22:33:44:55 enable enable

show sag ip

This command displays the configured SAG IPv4 addresses.

Usage
show sag ip

Example
admin@sonic~#show sag ip Vlan Interface Name IPv4 address/mask ---------- ---------- Vlan100 1.1.1.254/24

show sag ipv6

This command displays the configured SAG IPv6 addresses.

Usage
show sag ipv6

Example
admin@sonic~#show sag ipv6 Vlan Interface Name IPv6 address/mask ---------- ---------- Vlan100 2001:1000::FE/64

SAG Configuration Commands

config sag mac_address add/del

This command is used to add/delete the SAG MAC address.

This setting is global and only a single MAC address is allowed.

Usage
config sag mac_address <add|del> <mac-address>

Parameters:

- mac-address: Specifies the MAC address used for SAG interface.

Example
admin@sonic:~# sudo config sag mac_address add 00:11:22:33:44:55 admin@sonic:~# sudo config sag mac_address del 00:11:22:33:44:55

config sag ipv4 enable/disable

This command is used to enable/disable the IPv4 address on the SAG interface.

Usage
config sag ipv4 <enable|disable>

Example
admin@sonic:~# sudo config sag ipv4 enable admin@sonic:~# sudo config sag ipv4 disable

config sag ipv6 enable/disable

This command is used to enable/disable the IPv6 address on the SAG interface.

Usage
config sag ipv6 <enable|disable>

Example

```
admin@sonic:~# sudo config sag ipv6 enable
admin@sonic:~# sudo config sag ipv6 disable
```

config sag interface sag ip add/del

This command is used to add/del the IPv4/IPv6 address on the SAG interface, and the VLAN interface that the SAG interface is based on.

Usage
config interface sag ip <add|del> <vlan-name> <ip-address>

Parameters:

- vlan-name: Specifies the SAG's parent VLAN interface name.
- ip-address: Specifies the IPv4/IPv6 address used on the SAG interface.

Example
admin@sonic:~# sudo config interface sag ip add Vlan1 192.168.1.1/24 admin@sonic:~# sudo config interface sag ip del Vlan1 192.168.1.1/24

41 Scheduling & Shaping

Table of Contents

This section explain the commands for queue scheduling and shaping, either in bytes or packets.

Scheduling & Shaping Show Commands

show scheduler

This command is used to display the scheduler profile(s).

Usage
show scheduler [<profile_name>]

Parameters:

- <profile_name>: Profile name.

Example
admin@as5835-54t-2:~$ show scheduler Name Scheduling Type Weight Shaper Type Bandwidth ---------- ---------- -------- ---------- ---------- scheduler_profile_queue0 WRR 20 bytes 10 Gbps

show interface scheduler

This command is used to display the scheduling and shaping for all interfaces or a given interface.

Usage
show interface scheduler [<interface_name>]

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".

Example
admin@sonic:~$ show interface scheduler Ethernet0 Type Queue Profile Scheduling Mode Weight Shaper Type Bandwidth ------ ------- ------------------------ ---------------- -------- ------------ ---------- Port N/A egress_port_shaper_profile DWRR N/A bytes 10 Gbps Queue 0 scheduler_profile_queue0 WRR 20 bytes 20 Gbps

Scheduling & Shaping Configuration Commands

User may create a schedule profile and bind/unbind the profile with port or egress queue of a port.

config scheduler add

This command is used to create a scheduler profile.

Usage
config scheduler add <profile_name> [--sched_type {WRR | DWRR | STRICT}] [--weight <weight>] [--shaper_type {bytes | packets}] [--bandwidth <bandwidth>]

Parameters:

- profile_name>: Profile name
- sched-type: Scheduling mode. Valid values are:
    - WRR : Weighted Round Robin.

        - note : mode WRR is not supported in Intel ASIC; for example Wedge100BF-32X/32QS/65X or AS9516-32D.
        - note: mellanox chips do not support the WRR mode. For example, AS9746-128D.
    - DWRR : Deficit Weighted Round Robin.
        - Default value for Intel ASIC.
    - STRICT : Strict mode.
- <weight>: Weight of the mode; in the range (1..100)
    - Default: 1.
- shaper-type: Shaper type of shaping. Valid values are:
    - bytes : Bytes mode.
    - packets : Packets mode. (mellanox chips do not support this parameter.)
- <bandwidth>: Maximum rate of traffic can pass through in kilo-bits/second (kbps) or packet/second (pps). Valid values are:
    - If meter-type is bytes :
        - The format is a decimal number or a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). Minimum: 8 kbps (32 kbps for AS8000 and AS9746-32D). Maximum: 400,000,000 kbps. For example:"10", "10k".
    - If meter-type is packets :
        - Minimum: 1 pps (2 pps for AS9746-32D). Maximum: 148,809,523 pps (67,108,608 pps for AS9746-32D).

Example
sudo config scheduler add scheduler_profile_queue0 --sched_type DWRR --weight 10 --meter_type bytes --bandwidth 1250000

config scheduler update

This command is used to modify an existing scheduler profile.

Usage
config scheduler update <profile_name> [--sched-type {WRR | DWRR | STRICT}] [--weight <weight>] [--shaper-

type {bytes | packets}] [--bandwidth <bandwidth>] [--no-shaping]

Parameters:

- <profile_name>: Profile name
- sched-type: Scheduling mode. (This parameter is required for Intel platform) Valid values are:
    - WRR : Weighted Round Robin.
        - note : mode WRR is not supported in Intel ASIC; for example Wedge100BF-32X/32QS/65X or AS9516-32D.
        - DWRR : Deficit Weighted Round Robin.
        - Default value for Intel ASIC.
    - STRICT : Strict mode.
- <weight>: Weight of the mode; in the range (1..100)
    - Default: 1..
- shaper-type: Shaper type of shaping. Valid values are:
    - bytes : Bytes mode.
    - packets : Packets mode.
- <bandwidth>: Maximum rate of traffic can pass through in kilo-bits/second (kbps) or packet/second (pps). Valid values are:
    - If meter-type is bytes :
        - The format is a decimal number or a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). Minimum: 8 kbps (32 kbps for AS8000 and AS9746-32D). Maximum: 400,000,000 kbps. For example:"10", "10k".
    - If meter-type is packets :
        - Minimum: 1 pps (2 pps for AS8000 and AS9746-32D). Maximum: 148,809,523 pps (67,108,608 pps for AS8000 and AS9746-32D).
- no-shaping: Disable the traffic shaping.

Example
sudo config scheduler update scheduler_profile_queue0 --sched_type WRR --weight 20 --meter_type bytes --bandwidth 2500000

config scheduler del

This command is used to delete a scheduler profile.

Usage
config scheduler del <profile_name>

Parameters:

- <profile_name>: Profile name.

Example
sudo config scheduler del scheduler_profile_queue0

config interface scheduler bind queue

This command is used to configure the scheduling and shaping setting on the specified queue.

Usage
config interface scheduler bind queue <interface_name> <queue> <profile_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- <queue>: Queue. Minimum: 0. Maximum: 7.
- <profile_name>: Profile name.

Example
sudo config interface scheduler bind queue Ethernet0 0 scheduler_profile_queue0

config interface scheduler unbind queue

This command is used to reset the scheduling and shaping setting on the specified queue.

Usage
config interface scheduler unbind queue <interface_name> <queue>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- <queue>: Queue. Minimum: 0. Maximum: 7.

Example
sudo config interface scheduler unbind queue Ethernet0 0

config interface scheduler bind port

This command is used to configure the shaping setting on the specified interface.

Usage
config interface scheduler bind port <interface_name> <profile_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- <profile_name>: Profile name.

Note :

- This command is only supported on Intel switches.

Example
sudo config interface scheduler bind port Ethernet0 egress_port_shaper_profile

config interface scheduler unbind port

This command is used to reset the shaping setting on the specified interface.

Usage
config interface scheduler unbind port <interface_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- <profile_name>: Profile name.

Note :

- This command is only supported on Intel switches.

Example
sudo config interface scheduler unbind port Ethernet0

42 sFlow

Table of Contents

Sampled flow, or sFlow, collects sampled packets and counters from traffic at a predefined sampling rate, encapsulates the data in sFlow packets, and then delivers them to remote collectors. This section describes the sFlow command syntax and usage.

sFlow Show Commands

show sflow

This command displays the global sFlow configuration that includes the admin state, collectors, the Agent ID, and counter polling interval.

Usage
show sflow

Example
admin@sonic:~# show sflow sFlow Global Information: sFlow Admin State: up sFlow Polling Interval: default sFlow AgentID: lo 2 Collectors configured: Name: collector_A IP addr: 10.11.46.2 UDP port: 6343 Name: collector_lo IP addr: 127.0.0.1 UDP port: 6343

show sflow interface

This command displays each interface's sFlow admin status and the sampling rate.

Usage
show sflow interface

Example
admin@sonic:~# show sflow interface sFlow interface configurations +------------+--------------+----------------+ | Interface | Admin State | Sampling Rate | +=============+===============+=================+ | Ethernet0 | up | 4000 | +------------+--------------+----------------+ | Ethernet1 | up | 4000 | +------------+--------------+----------------+ ... +------------+--------------+----------------+ | Ethernet61 | up | 4000 | +------------+--------------+----------------+ | Ethernet62 | up | 4000 | +------------+--------------+----------------+ | Ethernet63 | up | 4000 | +------------+--------------+----------------+

sFlow Config Commands

config sflow collector add

This command adds an sFlow collector.

Usage
config sflow collector add <collector-name> {<ipv4-address | ipv6-address>} [--port <number>] [--vrf {default | mgmt}]

Parameters:

- <collector-name>, a unique name for the collector, max length is 16. The maximum number of collectors that can be configured is 2.
- <ipv4-address>, IPv4 address of the collector in dotted decimal format.
- <ipv6-address>, IPv6 address of the collector in x: x: x: x::x format, where :: notation specifies successive hexadecimal fields of zeros.
- port (OPTIONAL), specifies the UDP port of the collector.
    - valid range is from 0 to 65535. (default is 6343)
- vrf (OPTINAL), specifies the VRF of the collector. (default is default)
    - default , connects using the default VRF.
    - mgmt , connects using the mgmt VRF. If the mgmt VRF doesn't be created yet, the default VRF will be used to conntect to server.

The following example configures a collector "collect_A" whose IP address is 10.11.46.2.

Example
admin@sonic:~# sudo config sflow collector add collector_A 10.11.46.2

config sflow collector del

This command deletes an sFlow collector whose name is specified.

Usage
config sflow collector del <collector-name>

Parameters:

- <collector-name>, the collector to be removed.

This example deletes a collector "collector_A".

Example
admin@sonic:~# sudo config sflow collector del collector_A

config sflow agent-id add

This command configures an interface as the sampling agent ID.

Usage
config sflow agent-id add <interface-name>

Parameters:

- <interface-name>, the interface whose IPv4 or IPv6 address is to be used as the agent address in sFlow packets.

Note:

- This setting is global and applied to configured collector(s).
- If there is a configured agent ID, you need to delete it before adding a new one.

This example specifies interface lo as the agent ID.

Example
admin@sonic:~# sudo config sflow agent-id add lo

config sflow agent-id del

This command removes the current agent ID.

Usage
config sflow agent-id del

Example
admin@sonic:~# sudo config sflow agent-id del

config sflow enable

Enables (or disables) sFlow sampling, which starts (or stops) the sFlow daemon monitoring the traffic on the interface(s).

Usage
config sflow {enable | disable}

This example starts sFlow monitoring.

Example
admin@sonic:~# sudo config sflow enable

config sflow interface

Enables/disables sFlow monitoring for sampling on an interface or all interfaces.

Usage
config sflow interface {enable | disable} {<interface-name> | all}

Parameters:

- <interface-name>, the interface on which the flow is monitored. It can be enabled or disabled individually.
  all, apply this configuration to all interfaces.

Note:

- To enable sFlow sampling correctly, you need to configure COPP. Here is a sample configuration that is appended to /usr/share /sonic/templates/copp_cfg.j2 .

copp_cfg.j2

```
{
        "COPP_GROUP": {
                "queue2_group1": {
                        "cbs": "1000",
                        "cir": "1000",
                        "genetlink_mcgrp_name": "packets",
                        "genetlink_name": "psample",
                        "meter_type": "packets",
                        "mode": "sr_tcm",
                        "queue": "2",
                        "red_action": "drop",
                        "trap_action": "trap",
                        "trap_priority": "1"
                }
        },
        "COPP_TRAP": {
                "sflow": {
                        "trap_group": "queue2_group1",
                        "trap_ids": "sample_packet"
                }
        }
}
```

The following example shows how to disable flow sampling on Ethernet40.

Example

```
admin@sonic:~# sudo config sflow interface disable Ethernet40
```

config sflow interface sample-rate

Configure the sampling rate of an interface.

Usage
config sflow interface sample-rate <interface-name> <value>

Parameters:

- <interface-name>, the interface on which the sampling rate is applied.
- <value>, sampling rate. Valid range: (100..8388608)
    - The 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."
- default sampling rates for link speeds

	link speed	sampling rate
1	1G	100
2	10G	1,000
3	40G	4,000
4	50G	5,000
5	100G	10,000
6	400G	40,000

Note:

- The Broadcom MAC chip supports a maximum of 4 different sampling rates per switch. It is recommended to use the default sampling rate unless it is a MUST.

The following example shows to how set a sampling rate of 1000 on interface Ethernet32.

Example
admin@sonic:~# sudo config sflow interface sample-rate Ethernet32 1000

config sflow polling-interval

This command is used to set the counter polling interval.

Usage
config sflow polling-interval <value>

Parameters:

- <value>, polling interval
    - valid range: 0, 5 to 300 seconds.
        - 0: disable counter polling
        - default: 20 seconds.

The following example shows how to set the polling interval to 30 seconds.

Example
admin@sonic:~# sudo config sflow polling-interval 30

43 Shared Buffer

Table of Contents

Shared buffer is used to buffer the ingress packets, process, and insert into egress queue before transmitting out from the device.

In some applications, it needs trigger notification to send (back pressure) pause frame to inform transmitting device slow down, user needs to adjust the threshold on ingress or egress.

Shared Buffer Show Commands

show buffer pool

This command is used to display the buffer pool configuration.

Usage
show buffer pool <[pool_name]>

Parameters:

- <pool_name>: Pool name.

Example

```
admin@sonic:~$ show buffer pool
Pool                Type    Size          Xoff
------------------- ------- ------------- -------------
egress_lossless_pool   egress   6,383,104 Bytes
egress_lossy_pool      egress   6,383,104 Bytes
ingress_lossless_pool  ingress  1,148,959 Bytes  5,744,794 Bytes
ingress_lossy_pool     ingress  5,872,456 Bytes
```

show buffer profile

This command is used to display the buffer profile configuration.

Usage
show buffer profile <[profile_name]>

Parameters:

- <profile_name>: Profile name.

Example

```
admin@sonic:~$ show buffer profile
Profile             Pool              Size    Shared Mode    Shared Size    Xoff
Xon    Xon-offset
--------------------- ------------------- ------- ------------ ------------ -------------
------ ------------
```

egress_lossless_profile egress_lossless_pool 0 Bytes dynamic 66% egress_lossy_profile egress_lossy_pool 0 Bytes dynamic 66% ingress_lossless_profile ingress_lossless_pool 0 Bytes dynamic 66% 5,744,794 Bytes 18 KiB ingress_lossy_profile ingress_lossy_pool 0 Bytes dynamic 66%

show interface buffer priority-group

This command is used to display the buffer configuration of the priority-group (PG) for all interfaces or a given interface.

Usage
show interface buffer priority-group <interface_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".

Example
admin@sonic:~$ show interface buffer priority-group Interface PG Profile ---------- ---- ---------- Ethernet0 0-2 buffer_prof1

show interface buffer queue

This command is used to display the buffer configuration for the queue for all interfaces or a given interface.

Usage
show interface buffer queue <interface_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".

Example
admin@sonic:~$ show interface buffer queue

```
Interface      Queue  Profile
-----------  -------  ------------
Ethernet0          0  buffer_prof2
```

show buffer_pool

This command is used to display the watermark of shared buffer for buffer pools.

Usage
show buffer_pool {watermark | persistent-watermark}

Parameters:

- watermark: show how user watermark for buffer pools.
- persistent-watermark: show persistent watermark for buffer pools.

Example

```
admin@sonic:~$ show buffer_pool watermark
Shared pool maximum occupancy:
              Pool    Bytes
--------------------  -------
 egress_lossless_pool   982320
   egress_lossy_pool        0
ingress_lossless_pool   919680
  ingress_lossy_pool        0
admin@sonic:~$
admin@sonic:~$ show buffer_pool persistent-watermark
Shared pool maximum occupancy:
              Pool    Bytes
--------------------  -------
 egress_lossless_pool   982320
   egress_lossy_pool        0
ingress_lossless_pool   919680
  ingress_lossy_pool        0
```

show headroom-pool

This command is used to display the watermark of shared buffer for headroom pools.

Usage
show headroom-pool {watermark | persistent-watermark}

Parameters:

- watermark: show how user watermark for headroom pools.
- persistent-watermark: show persistent watermark for headroom pools.

Example
admin@sonic:~$ show headroom-pool watermark Headroom pool maximum occupancy: Pool Bytes ---------- ------- ingress_lossless_pool 197866 admin@sonic:~$ show headroom-pool persistent-watermark Headroom pool maximum occupancy: Pool Bytes ---------- ------- ingress_lossless_pool 197866

Shared Buffer Configuration Commands

config buffer pool add

This command is used to create a buffer pool profile.

Usage
config buffer pool add {pool_name} --type {ingress | egress} --size <size> [--xoff-size <xoff-size>]

Parameters:

- <pool_name>: Pool name.
- type: Stage. Valid values are:
    - ingress : Ingress stage.
    - egress: Egress stage.
- <size>: The size of the shared buffer in bytes.

- <xoff-size>: The size of the shared headroom in bytes. Available only for ingress stage.

Note: If changed the buffer pool setting, it is needed to restart the switch for the setting to take effect.

Example
sudo config buffer pool add ingress_pool --type ingress --size 9600000 --xoff-size 300000

Example
sudo config buffer pool add egress_pool --type egress --size 8400000

config buffer pool del

This command is used to delete a buffer pool profile.

Usage
config buffer pool del {pool_name}

Parameters:

- <pool_name>: Pool name.

Note: If changed the buffer pool setting, it is needed to restart the switch for the setting to take effect.

Example
sudo config buffer pool del ingress_pool sudo config buffer pool del egress_pool

config buffer profile add

This command is used to create a buffer profile.

Usage
config buffer profile add <profile_name> --pool <buffer_pool_name> {--size <size>} {--shared-size <shared_size> | --shared-percent <shared_percent>} [--xoff <xoff_size> --xon <xon_size> --xon-offset <xon_offset>]

Parameters:

- <profile_name>: Profile name.
- <buffer_pool_name>: Pool name.
- <size>: Reserved size in bytes.
- <shared_size>: Shared size in bytes.
- <shared_percent>: Shared size in percentage. The shared size is "the free size of buffer pool × shared percentage". Valid values are:
    - 0.78: 0.78% (alpha: 1/128) (only available on Broadcom platform).
    - 1.5: 1.5% (alpha: 1/64).
    - 3: 3% (alpha: 1/32).
    - 6: 6% (alpha: 1/16).
    - 11: 11% (alpha: 1/8).
    - 20: 20% (alpha: 1/4).
    - 33: 33% (alpha: 1/2).
    - 50: 50% (alpha: 1).
    - 66: 66% (alpha: 2).
    - 80: 80% (alpha: 4).
    - 89: 89% (alpha: 8) (only available on Broadcom platform).
- <xoff_size>: Headroom size in bytes. Only for ingress lossless profile.
- <xon_size>: Resume size in bytes. Only for ingress lossless profile.
- <xon_offset_size>: Resume offset size in bytes. Only for ingress lossless profile. This size doesn't support on Intel platform.

Example
sudo config buffer profile add ingress_profile_lossy --pool ingress_pool --shared_percent 1 --size 0

config buffer profile update

This command is used to modify an existing buffer profile.

Usage
config buffer profile update <profile_name> {--shared-percent <shared_percent>} [--xon <xon_size>]

Parameters:

- <profile_name>: Profile name.
- <shared_percent>: Shared size in percentage. The shared size is "the free size of buffer pool × shared percentage". Valid values are:
    - 0.78: 0.78% (alpha: 1/128) (only available on Broadcom platform).
    - 1.5: 1.5% (alpha: 1/64).
    - 3: 3% (alpha: 1/32).
    - 6: 6% (alpha: 1/16).

    - 11: 11% (alpha: 1/8).
    - 20: 20% (alpha: 1/4).
    - 33: 33% (alpha: 1/2).
    - 50: 50% (alpha: 1).
    - 66: 66% (alpha: 2).
    - 80: 80% (alpha: 4).
    - 89: 89% (alpha: 8) (only available on Broadcom platform).
- <xon_size>: Resume size in bytes. Only for ingress lossless profile.

Example
sudo config buffer profile update ingress_profile_lossy --pool ingress_pool --shared_percent 66 --size 100

config buffer profile del

This command is used to delete a buffer profile.

Usage
config buffer profile del <profile_name>

Parameters:

- <profile_name>: Profile name.

Example
sudo config buffer profile del ingress_profile_lossy

config interface buffer bind priority-group

This command is used to bind the buffer profile to the ingress priority group.

Usage
config interface buffer bind priority-group {<interface_name> | all} <pg> <profile_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- all: All physical interfaces.
- <pg>: Priority Group. Valid values are:
    - Minimum: 0. Maximum: 7. (Broadcom platform)
    - Minimum: 1. Maximum: 5. (Intel platform)

- <profile_name>: Profile name.

Example
sudo config interface buffer bind priority-group Ethernet0 0 ingress_profile_lossy

config interface buffer unbind priority-group

This command is used to unbind the buffer profile from the ingress priority group.

Usage
config interface buffer unbind priority-group {<interface_name> | all} <pg>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- all: All physical interfaces.
- <pg>: Priority Group.

Here is an example for unbinding profile "ingress_profile_lossy" from interface "Ethernet0" pg 0.

Example
sudo config interface buffer unbind priority-group Ethernet0 0

config interface buffer bind queue

This command is used to bind the buffer profile to the egress queue.

Usage
config interface buffer bind queue {<interface_name> | all} <queue> <profile_name>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- all: All physical interfaces.
- <queue>: Queue. Minimum: 0. Maximum: 7.
- <profile_name>: Profile name.

Example
sudo config interface buffer bind queue Ethernet0 0 egress_profile

config interface buffer unbind queue

This command is used to unbind the buffer profile from the egress queue.

Usage
config interface buffer unbind queue {<interface_name> | all} <queue>

Parameters:

- <interface_name>: Physical interface name. For example: "Ethernet0".
- all: All physical interfaces.
- <queue>: Queue. Minimum: 0. Maximum: 7.

Example
sudo config interface buffer unbind queue Ethernet0 0

Queue and Priority-Group

This sub-section describes some queue and priority-group parameters. It can be displayed in show queue commands or show priority-group commands.

queue counters

queue watermark

priority-group

Queue and Priority-Group Show Commands

show queue counters

This command displays packet and byte counters for all queues of all ports or one specific-port specified as an argument.

Display packet and byte counters of interface(s).

Usage
show queue counters [<interface_name>]

Parameters:

- <interface name>: The interface of associated counter. Without this, it shows all ports.

Example

```
admin@sonic:~$ show queue counters
    Port    TxQ    Counter/pkts    Counter/bytes    Drop/pkts    Drop/bytes
---------  -----  --------------  ---------------  -----------  ------------
Ethernet0    UC0               0                0            0             0
Ethernet0    UC1               0                0            0             0
Ethernet0    UC2               0                0            0             0
Ethernet0    UC3               0                0            0             0
Ethernet0    UC4               0                0            0             0
Ethernet0    UC5               0                0            0             0
Ethernet0    UC6               0                0            0             0
Ethernet0    UC7               0                0            0             0
Ethernet0    UC8               0                0            0             0
Ethernet0    UC9               0                0            0             0
Ethernet0    MC0               0                0            0             0
Ethernet0    MC1               0                0            0             0
Ethernet0    MC2               0                0            0             0
Ethernet0    MC3               0                0            0             0
Ethernet0    MC4               0                0            0             0
Ethernet0    MC5               0                0            0             0
Ethernet0    MC6               0                0            0             0
Ethernet0    MC7               0                0            0             0
Ethernet0    MC8               0                0            0             0
Ethernet0    MC9               0                0            0             0
    Port    TxQ    Counter/pkts    Counter/bytes    Drop/pkts    Drop/bytes
---------  -----  --------------  ---------------  -----------  ------------
Ethernet4    UC0               0                0            0             0
Ethernet4    UC1               0                0            0             0
Ethernet4    UC2               0                0            0             0
Ethernet4    UC3               0                0            0             0
Ethernet4    UC4               0                0            0             0
Ethernet4    UC5               0                0            0             0
Ethernet4    UC6               0                0            0             0
```

```
Ethernet4    UC7            0            0            0            0
Ethernet4    UC8            0            0            0            0
Ethernet4    UC9            0            0            0            0
Ethernet4    MC0            0            0            0            0
Ethernet4    MC1            0            0            0            0
Ethernet4    MC2            0            0            0            0
Ethernet4    MC3            0            0            0            0
Ethernet4    MC4            0            0            0            0
Ethernet4    MC5            0            0            0            0
Ethernet4    MC6            0            0            0            0
Ethernet4    MC7            0            0            0            0
Ethernet4    MC8            0            0            0            0
Ethernet4    MC9            0            0            0            0
...
```

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

Example

```
admin@sonic:~$ show queue counters Ethernet72
     Port    TxQ    Counter/pkts    Counter/bytes    Drop/pkts    Drop/bytes
---------  -----  --------------  ---------------  -----------  ------------
Ethernet72    UC0             0              0            0             0
Ethernet72    UC1             0              0            0             0
Ethernet72    UC2             0              0            0             0
Ethernet72    UC3             0              0            0             0
Ethernet72    UC4             0              0            0             0
Ethernet72    UC5             0              0            0             0
Ethernet72    UC6             0              0            0             0
Ethernet72    UC7             0              0            0             0
Ethernet72    UC8             0              0            0             0
Ethernet72    UC9             0              0            0             0
Ethernet72    MC0             0              0            0             0
Ethernet72    MC1             0              0            0             0
Ethernet72    MC2             0              0            0             0
Ethernet72    MC3             0              0            0             0
```

Ethernet72	MC4	0	0	0	0
Ethernet72	MC5	0	0	0	0
Ethernet72	MC6	0	0	0	0
Ethernet72	MC7	0	0	0	0
Ethernet72	MC8	0	0	0	0
Ethernet72	MC9	0	0	0	0

Note: Queue counters can be cleared by using the following command: sonic-clear queuecounters

show queue watermark

This command displays the user watermark or persistent-watermark for unicast or multicast queues (egress shared pool occupancy per queue) for all ports.

Usage
show queue {watermark | persistent-watermark} {multicast | unicast|all}

Parameters:

- watermark , the highest watermark after the last clean command.
- persistent-watermark , the highest watermark after system bring up.
- The 'all' designation refers to a specific queue type, it does not signify a merging of multicast and unicast.

Note: Both "user watermark" and "persistent watermark" can be cleared by the user.

Example: show for unitcast of watermark

```
admin@sonic:~$ show queue watermark unicast
Egress shared pool occupancy per unicast queue:
     Port   UC0   UC1   UC2   UC3   UC4   UC5   UC6   UC7   UC8   UC9
----------  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----
  Ethernet0     0     0     0     0     0     0     0     0     0     0
  Ethernet4   416     0     0     0     0     0     0     0     0     0
  Ethernet8   416     0     0     0     0     0     0     0     0     0
 Ethernet12   416     0     0     0     0     0     0     0     0     0
```

Example: show for multicast of watermark

```
admin@sonic:~$ show queue watermark multicast
Egress shared pool occupancy per multicast queue:
     Port    MC10    MC11    MC12    MC13    MC14    MC15    MC16    MC17    MC18    MC19
-----------  ------  ------  ------  ------  ------  ------  ------  ------  ------  ------
  Ethernet0       0       0       0       0       0       0       0       0       0       0
  Ethernet4     416       0       0       0       0       0       0       0       0       0
  Ethernet8     416       0       0       0       0       0       0       0       0       0
 Ethernet12     416       0       0       0       0       0       0       0       0       0
 Ethernet16     416       0       0       0       0       0       0       0       0       0
```

Example: show for unicast of persistent-watermark

```
admin@sonic:~$ show queue persistent-watermark unicast
Egress shared pool occupancy per unicast queue:
     Port    UC0    UC1    UC2    UC3    UC4    UC5    UC6    UC7    UC8    UC9
-----------  -----  -----  -----  -----  -----  -----  -----  -----  -----  -----
  Ethernet0      0      0      0      0      0      0      0      0      0      0
  Ethernet4    416      0      0      0      0      0      0      0      0      0
  Ethernet8    416      0      0      0      0      0      0      0      0      0
```

Example: show for multicast of persistent-watermark

```
admin@sonic:~$ show queue persistent-watermark multicast
Egress shared pool occupancy per multicast queue:
     Port    MC10    MC11    MC12    MC13    MC14    MC15    MC16    MC17    MC18    MC19
-----------  ------  ------  ------  ------  ------  ------  ------  ------  ------  ------
  Ethernet0       0       0       0       0       0       0       0       0       0       0
  Ethernet4       0       0       0       0       0       0       0       0       0       0
  Ethernet8       0       0       0       0       0       0       0       0       0       0
```

show priority-group watermark

This command displays the user watermark or persistent-watermark for the Ingress "headroom" or "shared pool occupancy" per priority-group for all ports.

Usage
show priority-group {watermark | persistent-watermark} {headroom | shared}

Parameters:

- watermark , the highest watermark after the last clean command.
- persistent-watermark , the highest watermark after system bring up.
- headroom , the max size of headroom has been used.
- shared , the max size has been used in shared pool.

Note: Both "user watermark" and "persistent watermark" can be cleared by the user.

Example

```
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
```

Example (Ingress headroom per PG)

```
admin@sonic:~$ show priority-group watermark headroom
Ingress headroom 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
```

Example (Ingress shared pool occupancy per PG)

```
admin@sonic:~$ show priority-group persistent-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
```

Example (Ingress headroom per PG)

```
admin@sonic:~$ show priority-group persistent-watermark headroom
Ingress headroom 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
```

Queue and Priority-Group Clear Commands

sonic-clear queuecounters

This command will clear the packet and byte counters for all queues of all ports.

Usage

```
sonic-clear queuecounters
```

Example

```
admin@sonic:~$ sonic-clear queuecounters
Clear and update saved counters for Ethernet0
Clear and update saved counters for Ethernet1
Clear and update saved counters for Ethernet2
Clear and update saved counters for Ethernet3
```

sonic-clear queue watermark

This command will clear the user watermark or persistent-watermark for unicast or multicast queues (egress shared pool occupancy per queue) for all ports.

The 'all' designation refers to a specific queue type, it does not signify a merging of multicast and unicast.

Usage
sonic-clear queue {watermark | persistent-watermark} {unicast | multicast|all}

Example: clear unitcast of user watermark
admin@sonic:~$ sudo sonic-clear queue watermark unicast

Example: clear multicast of user watermark
admin@sonic:~$ sudo sonic-clear queue watermark multicast

Example: clear unicast of persistent-watermark
admin@sonic:~$ sudo sonic-clear queue persistent-watermark unicast

Example: clear multicast of persistent-watermark
admin@sonic:~$ sudo sonic-clear queue persistent-watermark multicast

sonic-clear priority-group watermark

This command will clear the user watermark or persistent-watermark for the Ingress "headroom" or "shared pool occupancy" per priority-group for all ports.

Usage

sonic-clear priority-group {watermark | persistent-watermark} {headroom | shared}

Parameters:

- watermark , the highest watermark after the last clean command.
- persistent-watermark , the highest watermark after system bring up.
- headroom , the max size of headroom has been used.
- shared , the max size has been used in shared pool.

Example: clear headroom of user watermark
admin@sonic:~$ sudo sonic-clear priority-group watermark headroom

Example: clear shared pool occupancy of user watermark
admin@sonic:~$ sudo sonic-clear priority-group watermark shared

Example: clear headroom of persistent-watermark
admin@sonic:~$ sudo sonic-clear priority-group persistent-watermark headroom

Example: clear shared pool occupancy of persistent-watermark
admin@sonic:~$ sudo sonic-clear priority-group persistent-watermark shared

44 SNMP

Table of Contents

SNMP Show commands

show runningconfiguration snmp

This command displays the global SNMP configuration that includes the location, contact, and community settings.

Usage
show runningconfiguration snmp

Example

```
admin@sonic:~$ show runningconfiguration snmp
Location
------------
Emerald City
SNMP_CONTACT    SNMP_CONTACT_EMAIL
--------------  --------------------
joe             joe@contoso.com
Community String    Community Type
------------------  ----------------
Jack                RW
```

show runningconfiguration snmp location

This command displays the SNMP location setting.

Usage
show runningconfiguration snmp location [--json]

Parameters:

- json: Display the output in JSON format.

Example
admin@sonic:~$ show runningconfiguration snmp location Location Emerald City

Example with json format
admin@sonic:~$ show runningconfiguration snmp location --json {'Location': 'Emerald City'}

show runningconfiguration snmp contact

This command displays the SNMP contact setting.

Usage
show runningconfiguration snmp contact [--json]

Parameters:

- json: Display the output in JSON format.

Example
admin@sonic:~$ show runningconfiguration snmp contact Contact Contact Email --------- --------------- joe joe@contoso.com

Example with json format
admin@sonic:~$ show runningconfiguration snmp contact --json {'joe': 'joe@contoso.com'}

show runningconfiguration snmp community

This command displays the SNMP community setting.

Usage
show runningconfiguration snmp community [--json]

Parameters:

- json: Display the output in JSON format.

Example
admin@sonic:~$ show runningconfiguration snmp community Community String   Community Type ---------------- ---------------- Jack   RW

Example with json format
admin@sonic:~$ show runningconfiguration snmp community --json {'Jack': {'TYPE': 'RW'}}

show snmp snmpagentaddress

This command displays the SNMP agent address setting.

Usage
show snmp snmpagentaddress

Example
admin@sonic:~$ show snmpagentaddress ListenIP   ListenPort   ListenVrf ---------- ------------ ----------- 10.0.0.60

SNMP Config commands

config snmp location modify

This command is used to modify the SNMP location.

Usage
config snmp location modify <location>

Parameters:

- <location>: SNMP location, default value is "public".

Example
admin@as7326-56x:~$ sudo config snmp location modify USA

config snmp location del

This command is used to restore the SNMP location.

Usage
config snmp location del <location>

Parameters:

- <location>: SNMP location, default value is "public".

Example
admin@as7326-56x:~$ sudo config snmp location del USA

config snmp contact add

This command is used to add the SNMP contact.

Usage

config snmp contact add <contact_name> <contact_email>

Parameters:

- <contact_name>: SNMP contact.
- <contact_email>: SNMP contact email.

Example
admin@sonic:~$ sudo config snmp contact add joe joe@contoso.com

config snmp contact modify

This command is used to modify the SNMP contact.

Usage
config snmp contact modify <contact> <contact_email>

Parameters:

- <contact>: SNMP contact.
- <contact_email>: SNMP contact email.

Example
admin@sonic:~$ sudo config snmp contact modify test test@contoso.com

config snmp contact del

This command is used to delete the SNMP contact.

Usage
config snmp contact del <contact>

Parameters:

- <contact>: SNMP contact.

Example
admin@sonic:~$ sudo config snmp contact del test

config snmp community add

This command is used to add the SNMP community.

Usage
config snmp community add <snmp_community> <access_type>

Parameters:

- <snmp_community>: SNMP community.
- <access_type>: one of the following:
    - RO : Read-only community.
    - RW : Read-write community.

Example
admin@sonic:~$ sudo config snmp community add testcomm ro

config snmp community replace

This command is used to replace the SNMP community.

Usage
config snmp community replace <current_community_string> <new_community_string>

Parameters:

- <current_community_string>: current SNMP community.
- <new_community_string>: new SNMP community.

Example
admin@sonic:~$ sudo config snmp community replace testcomm newtestcomm

config snmp community del

This command is used to delete the SNMP community.

Usage
config snmp community del <snmp_community>

Parameters:

- <snmp_community>: SNMP community.

Example
admin@sonic:~$ sudo config snmp community del newtestcomm

config snmpagentaddress add

This command is used to add the SNMP agent address.

Usage
config snmpagentaddress add <agent_address> [-p|--port <port>] [-v|--vrf <vrf_name>]

Parameters:

- <agent_address>: IP address of SNMP agent.
- <port>: Port number of SNMP agent. Default value is 161.
- <vrf_name>: VRF name. Indicates that the SNMP agent is part of the VRF.

Example
admin@as7326-56x:~$ sudo config snmpagentaddress add 10.0.0.60

config snmpagentaddress del

This command is used to delete the SNMP agent address.

Usage
config snmpagentaddress del <agent_address> [-p|--port <port>] [-v|--vrf <vrf_name>]

Parameters:

- <agent_address>: IP address of SNMP agent.
- <port>: Port number of SNMP agent. Default value is 161.
- <vrf_name>: VRF name. Indicates that the SNMP agent is part of the VRF.

Example
admin@as7326-56x:~$ sudo config snmpagentaddress del 10.0.0.60

45 SNMP Traps

Table of Contents

SNMP Trap Show Commands

show snmptrap

This command displays the configured SNMP trap server IP addresses.

Usage
show snmptrap

Example
admin@sonic:~$ show snmptrap Version TrapReceiverIP Port VRF Community --------- ---------- ------ ----- ---------- 2 31.31.31.31 456 mgmt public

SNMP Trap Config Commands

config snmptrap modify

This command configures the trap server IP address and some options for the traps.

Usage
config snmptrap modify <snmp version> [-p <port>] [-v <vrf name>] [-c <community>] <trap server ip>

Parameters:

- <snmp version>: SNMP version. Each SNMP version can be configured with one trap server IP address.
    - 1

    - 2
    - 3
- <port>: the port to receive the SNMP traps. (default: 162)
- <vrf name>: VRF name; using this VRF name, the SNMP agent sends the trap through the <vrf name> domain. The option can be one of following VRF types:
    - mgmt, the keyword to specify management VRF
    - none , the keyword to clear the VRF specified before
    - <name> , specifies the name of one data VRF
- <community>
- <trap server ip>: The server IP address that receives the trap

Note:

- The configuration is stored in snmpd.conf ,
- The SNMP service is restarted to take the configuration effect.

Example
admin@sonic:~$ sudo config snmptrap modify 2 -p 456 -v mgmt 21.21.21.21 trap2sink 21.21.21.21:456%mgmt public

In this example, a user configures a trap server address (21.21.21.21) for SNMP version 2, changes the port (456), and specifies the management VRF domain. This configuration is stored in /etc/snmp/snmpd.conf inside of the SNMP docker.

In the output information, the "%mgmt" would not be present if the "-v" option is not specified.

In the case of SNMPv1, "trapsink" will be updated, and in the case of v2, "trap2sink" will be updated.

config snmpinform del

This command deletes the trap server configuration of the specified SNMP version. This configuration is removed from snmpd.conf and the SNMP service restarted to make this configuration effective in the SNMP agent.

Usage

config snmpinform del <snmp_version>

Parameters:

<snmp version>, the version to be deleted.

Example
admin@sonic:~$ sudo config snmpinform del 2

45.1 SNMP inform

Table of Contents

SNMP Inform show commands

show snmpinform

This command displays the configured SNMP trap server IP address.

Usage
show snmpinform

Example

```
admin@sonic:~$ show snmpinform
Version  TrapReceiverIP     Port  VRF    Community
---------  ----------------  ------  -----  -----------
      2  31.31.31.31         456  mgmt   public
```

SNMP Inform Config Commands

config snmpinform modify

This command configures the IP address of the inform server and some options for the inform.

Usage
config snmptrap modify <snmp version> [-p <port>] [-v <vrf name>] [-c <community>] <inform server ip>

Parameters：

- < snmp version > ： SNMP version。SNMPv2 and SNMPv3 version can be configured with one inform server IP address.
  - 2
  - 3
- <port>：the port to receive the SNMP inform. (default: 162)
- <vrf名称>：VRF name; using this VRF name, the SNMP agent sends the trap through the <vrf name> domain. The option can be one of following VRF types:
  - mgmt，the keyword to specify management VRF
  - none ， the keyword to clear the VRF specified before
  - <name>， specifies the name of one data VRF
- <community>
  - default value public
  - When configuring the SNMPv3 version, the username should be SNMPv3

•<inform server ip>: The server IP address that receives the inform

Note:

- The configuration is stored in snmpd.conf ,
- The SNMP service is restarted to take the configuration effect.

Example
admin@sonic:~$ sudo config snmpinform modify 2 -p 456 -v mgmt 21.21.21.21 informsink 21.21.21.21:456%mgmt public

In this example, a user configures a trap server address (21.21.21.21) for SNMP version 2, changes the port (456), and specifies the management VRF domain. This configuration is stored in /etc/snmp/snmpd.conf inside of the SNMP docker.

In the output information, the "%mgmt" would not be present if the "-v" option is not specified.

In the case of SNMPv1, "trapsink" will be updated, in the case of v2, "trap2sink" will be updated, and in the case of v3, "trapsess" will be updated.

Example
admin@sonic:~$ sudo config snmpinform modify 3 -p 456 21.21.21.21 -c myuser The configuration file/etc/snmp/snmpd.conf will generate the following configuration trapsess -Ci -v 3 -l authPriv -e 0x80001f888069061b0e86e4b66700000000 21.21.21.21:456 -u myuser

In this example, a user configures a inform server address (21.21.21.21) for SNMP version 3, changes the port (456), specifies the management VRF domain, and set the SNMPv3 user. This configuration is stored in /etc/snmp/snmpd.conf inside of the SNMP docker.

In the output information, the "%mgmt" would not be present if the "-v" option is not specified.

In the case of SNMPv2, "trap2sink" will be updated, and in the case of v3, "trapsess" will be updated.

config snmpinform del

This command deletes the trap server configuration for the specified SNMP version.

This configuration will be removed from snmpd.conf and the SNMP service will restart for this configuration to take effect in the SNMP agent.

Usage
config snmpinform del <snmp_version>

参数:

<snmp version>，the version to be deleted.

Example
admin@sonic:~$ sudo config snmpinform del 2

46 Software Installation and Management

Table of Contents

The SONiC software can be installed by two methods; using the "sonic_installer" tool or "ONIE Installer".

SONiC Installer

This is a command line tool available as part of the SONiC software; If the device is already running the SONiC software, this tool can be used to install an alternate image in the partition. This tool has the facility to install an alternate image, list the available images, and set the next reboot image. This command requires elevated (root) privileges to run.

sonic-installer list

This command displays information about currently installed images. It displays a list of installed images, the currently running image, and the image set to be loaded at the next reboot.

Usage:
sonic-installer list

Example:
admin@tor:~$ sudo sonic-installer list Current: SONiC_20220819_084543_202111_184 Next: SONiC_20220819_084543_202111_184 Available: SONiC_20220819_084543_ec202111_184 SONiC_20220526_081320_ec202111_117

This output can be obtained without root privileges by running the show boot command.

sonic-installer install

This command is used to install a new image in the alternate image partition. This command takes a path to an installable SONiC image or URL and installs the image.

Usage:
sonic-installer install [OPTIONS] <image_file_path>

Options:

- -y, --yes, When prompted 'yes/no', select 'yes' directly
- -f, --force, Forces installation of an image of a type that differs from that of the currently running image
- --skip-platform-check, Force installation of an image of a type which is not of the same platform
- --skip_migration，Do not migrate current configuration to the newly installed image
- --skip-package-migration，Do not migrate current packages to the newly installed image
- --skip-setup-swap， Skip setup temporary SWAP memory used for installation
- --swap-mem-size <INTEGER> , SWAP memory space size [default: (1024MiB)] NOTE: this argument is mutually exclusive with arguments: skip_setup_swap

- --total-mem-threshold <INTEGER> ,If system total memory is lower than threshold, setup SWAP memory [default:(2048 MiB)] NOTE: this argument is mutually exclusive with arguments:skip_setup_swap
- --available-mem-threshold <INTEGER> , If system available memory is lower than threhold, setup SWAP memory [default:(1200 MiB)] NOTE: this argument is mutually exclusive with arguments: skip_setup_swap

Note

- By default, the current configuration will be migrated to the newly installed image. The option "--skip_migration" can be applied to omit the migration of configuration.
- If a kernel panic has ever occurred on the running of the current image, there will be dmesg files in "/sys/fs/pstore/", which can be used for debugging. It is strongly recommended to have a backup before installing a new image. Also, remember to note down the current image version so the dmesg files can be correlated to the correct image version.
- The format of files in the "/sys/fs/pstore/" may not be compatible with all Linux kernel versions, which could result in error logs that read "pstore: crypto comp decompress failed, ret = -22!" when the system boots. These files will be deleted after the first boot with the freshly loaded image to prevent them from showing harmless error logs that can confuse users.

Example:
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
```

sonic-installer set-default

This command is used to change the image that can be loaded by default in all the subsequent reboots.

Usage:
sonic-installer set-default <image_name>

Example:
admin@sonic:~$ sudo sonic-installer set-default SONiC-OS-HEAD.XXXX

sonic-installer set-nex-boot

This command is used to change the image that can be loaded in the next reboot only. Note that following the next reboot, it will always fall back to the current image.

Usage:
sonic-installer set-next-boot <image_name>

Example:
admin@sonic:~$ sudo sonic-installer set-next-boot SONiC-OS-HEAD.XXXX

sonic-installer remove

This command is used to remove the unused SONiC image from the disk. Note that it's not allowed to remove the currently running image.

Usage:
sonic-installer remove [y|-yes] <image_name>

Example:
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

sonic-installer cleanup

This command removes all unused images from the device, leaving only the currently active image and the image that will be booted next (if different). If there are no images that can be removed, the command will output "No image(s) to remove".

Usage:
sonic-installer cleanup [y|-yes]

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

sonic_installer binary_version (not supported)

This command is used to get the version from the local binary image file.

sonic_installer rollback_docker (not supported)

This command is used to rollback the docker image to a previous version.

sonic_installer upgrade_docker (not supported)

This command is used to upgrade a docker image from a local binary or URL.

47 Startup & Running Configuration

Table of Contents

Startup Configuration

show startupconfiguration bgp

This command is used to display the startup configuration for the BGP module.

Usage
show startupconfiguration bgp

Example
admin@sonic:~$ show startupconfiguration bgp Routing-Stack is: frr ! ! template: bgpd/bgpd.conf.j2 !

```
!
! ========== Managed by sonic-cfggen DO NOT edit manually! ====================
! generated by templates/quagga/bgpd.conf.j2 with config DB data
! file: bgpd.conf
!
!
! template: common/daemons.common.conf.j2
!
hostname as5812-54x
password zebra
enable password zebra
!
log syslog informational
log facility local4
!
! end of template: common/daemons.common.conf.j2!
agentx
!
!
!
! template: bgpd/bgpd.main.conf.j2
!
! bgp multiple-instance
!
! BGP configuration
!
! TSA configuration
!
ip prefix-list PL_LoopbackV4 permit 10.1.0.32/32
!
ipv6 prefix-list PL_LoopbackV6 permit fc00:1::/64
!
!
!
```

```
router bgp 65100
!
bgp log-neighbor-changes
no bgp default ipv4-unicast
!
bgp bestpath as-path multipath-relax
!
bgp graceful-restart restart-time 240
bgp graceful-restart
bgp graceful-restart preserve-fw-state
...
```

Running Configuration

This sub-section explains the show commands for displaying the running configuration for the following modules.

1. BGP
2. Interfaces
3. NTP
4. SNMP
5. ALL
6. ACL
7. Ports
8. Syslog

show runningconfiguration bgp

This command displays the running configuration of the BGP module.

Usage
show runningconfiguration bgp

Example
admin@sonic:~$ show runningconfiguration bgp Building configuration... Current configuration: ! frr version 7.2.1-sonic frr defaults traditional hostname as5812-54x log syslog informational log facility local4 agentx no service integrated-vtysh-config ! enable password zebra password zebra ! ip route 0.0.0.0/0 10.250.0.1 200 ! router bgp 65100 bgp router-id 10.1.0.32 bgp log-neighbor-changes no bgp default ipv4-unicast bgp graceful-restart restart-time 240 bgp graceful-restart bgp graceful-restart preserve-fw-state bgp bestpath as-path multipath-relax neighbor PEER_V4 peer-group

...

show runningconfiguration interfaces

This command displays the running configuration for the interfaces.

Usage
show runningconfiguration interfaces

Example
admin@sonic:~$ show runningconfiguration interfaces { "Ethernet0": {}, "Ethernet1": {}, "Ethernet2": {}, "Ethernet3": {}, "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": {},
        "Ethernet0| 10.0.0.0/31": {},
        "Ethernet0|FC00::1/126": {},
        "Ethernet1| 10.0.0.2/31": {},
        "Ethernet1|FC00::5/126": {},
        "Ethernet2| 10.0.0.4/31": {},

...
```

show runningconfiguration ntp

This command displays the running configuration of the NTP module.

Usage
show runningconfiguration ntp

Example

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

show runningconfiguration snmp

This command displays the running configuration of the SNMP module.

Usage
show runningconfiguration snmp

Example

```
admin@sonic:~$ show runningconfiguration snmp
################################################################################
# Managed by sonic-config-engine
################################################################################
#
# EXAMPLE.conf:
#   An example configuration file for configuring the Net-SNMP agent ('snmpd')
#   See the 'snmpd.conf(5)' man page for details
#
#  Some entries are deliberately commented out, and will need to be explicitly activated
#
################################################################################
#
#  AGENT BEHAVIOUR
#
#  Listen for connections on all ip addresses, including eth0, ipv4 lo
#
```

```
agentAddress udp:161
agentAddress udp6:161
##############################################################################
#
#  ACCESS CONTROL
#
                                #  system + hrSystem groups only
view   systemonly  included   .1.3.6.1.2.1.1
view   systemonly  included   .1.3.6.1.2.1.25.1
                                #  Default access to basic system info
rocommunity public
rocommunity6 public
##############################################################################
#
#  SYSTEM INFORMATION
#
#  Note that setting these values here, results in the corresponding MIB objects being 'read-only'
#  See snmpd.conf(5) for more details
sysLocation    public
sysContact     Azure Cloud Switch vteam <linuxnetdev@microsoft.com>
                                # Application + End-to-End layers
sysServices    72
...
```

show runningconfiguration all

This command displays the entire running configuration.

Usage
show runningconfiguration all

Example

```
admin@sonic:~$ show runningconfiguration all
{
        "ACL_TABLE": {
        "DATAACL": {
                "policy_desc": "DATAACL",
                "ports": [
                        "Ethernet16",
                        "Ethernet0",
                        "Ethernet17",
                        "Ethernet1",
                        "Ethernet18",
                        "Ethernet2",
                        "Ethernet19",
                        "Ethernet3",
                        "Ethernet20",
                        "Ethernet4",
                        "Ethernet21",
                        "Ethernet5",
                        "Ethernet22",
                        "Ethernet6",
                        "Ethernet23",
                        "Ethernet7",
                        "Ethernet24",
                        "Ethernet8",
                        "Ethernet25",
                        "Ethernet9",
                        "Ethernet26",
                        "Ethernet10",
                        "Ethernet27",
                        "Ethernet11",
                        "Ethernet28",
                        "Ethernet12",
```

```
                "Ethernet29",
                "Ethernet13",
                "Ethernet30",
                "Ethernet14",
                "Ethernet31",
                "Ethernet15"
            ],
            "stage": "ingress",
            "type": "L3"
        },
        "EVERFLOW": {
            "policy_desc": "EVERFLOW",
            "ports": [
                "Ethernet10",
                "Ethernet9",
                "Ethernet16",
                "Ethernet15",
                "Ethernet14",
                "Ethernet13",
                "Ethernet12",
                "Ethernet11",
                "Ethernet18",
                "Ethernet17",
                "Ethernet2",
                "Ethernet1",
                "Ethernet0",
                "Ethernet6",
                "Ethernet5",
                "Ethernet4",
                "Ethernet3",
                "Ethernet8",
                "Ethernet7",
                "Ethernet21",
                "Ethernet22",
```

```
                    "Ethernet19",
                    "Ethernet20",
                    "Ethernet25",
                    "Ethernet26",
                    "Ethernet23",
                    "Ethernet24",
                    "Ethernet27",
                    "Ethernet28",
                    "Ethernet30",
                    "Ethernet29",
                    "Ethernet31"
                ],
                "stage": "ingress",
                "type": "MIRROR"
        },
...
```

show runningconfiguration acl

This command displays the running configuration of the ACLs.

Usage
show runningconfiguration acl

Example

root@sonic:~# show runningconfiguration acl
{
"TEST1|DEFAULT_RULE": {
"ETHER_TYPE": "2048",
"PACKET_ACTION": "DROP",

```
        "PRIORITY": "1"
        },
        "TEST1|RULE_1": {
        "PACKET_ACTION": "FORWARD",
        "PRIORITY": "9999",
        "SRC_IP": "20.0.0.2/32"
        }
}
```

show runningconfiguration ports

This command displays the running configuration of the Ports.

Usage
show runningconfiguration ports [<portname>]

Example

admin@sonic:~$ show runningconfiguration ports
{
"Ethernet0": {
"admin_status": "up",
"alias": "tenGigE1",
"description": "ARISTA01T2:Ethernet1",
"index": "1",
"lanes": "13",
"mtu": "9100",
"pfc_asym": "off",
"speed": "10000"
},
"Ethernet1": {

```
        "admin_status": "up",
        "alias": "tenGigE2",
        "description": "ARISTA02T2:Ethernet1",
        "index": "2",
        "lanes": "14",
        "mtu": "9100",
        "pfc_asym": "off",
        "speed": "10000"
        },
        "Ethernet2": {
...

admin@sonic:~$ show runningconfiguration ports Ethernet0
{
        "Ethernet0": {
        "index": "1",
        "lanes": "13",
        "description": "ARISTA01T2:Ethernet1",
        "admin_status": "up",
        "mtu": "9100",
        "alias": "tenGigE1",
        "pfc_asym": "off",
        "speed": "10000"
        }
}
```

show runningconfiguration syslog

This command displays the running configuration of the Syslog module.

Usage
show runningconfiguration syslog

Example
admin@sonic:~$ show runningconfiguration syslog Syslog Servers [10.250.1.44]

Note

- For all "show startupconfiguration" and "show runningconfiguration" commands, only the partial output is shown here. In the realtime, all the configuration information is displayed.

48 Syslog

Table of Contents

Syslog Configuration Commands

The config syslog command is used to add or remove the configured syslog servers.

config syslog add

This command is used to add a new syslog server to the Syslog server list. Note that more than one syslog server can be added to the list.

Usage
config syslog add <ipv4-address | ipv6-address> [--source <ipv4-address | ipv6-address>] [--port <number>] [--vrf {default | mgmt}]

Parameters:

- 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)
- source(OPTIONAL) : IP address of specific source IP, the source IP must exist in default vrf or mgmt vrf.
- port (OPTIONAL), specifies the UDP port of the collector.
    - valid range is from 0 to 65535. (default is 6343)
- vrf (OPTINAL), specifies the VRF of the collector. (default is default)
    - default , connects using the default VRF.
    - mgmt , connects using the mgmt VRF. If the mgmt VRF doesn't be created yet, the default VRF will be used to conntect to server.

The following example shows how to add a remote syslog server with the ip address 1.1.1.1.

Example
admin@sonic:~$ sudo config syslog add 1.1.1.1 --source 192.168.8.231 Running command: systemctl reset-failed rsyslog-config rsyslog Running command: systemctl restart rsyslog-config

config syslog delete

This command is used to delete a configured syslog server.

Usage
config syslog del <ipv4-address | ipv6-address>

Parameters:

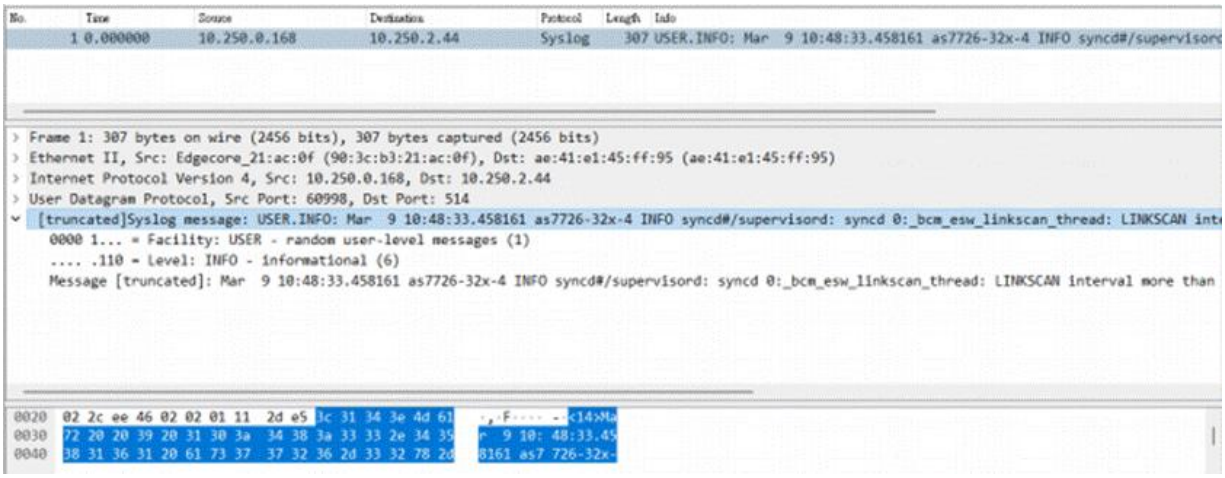
- ipv4-address : IP address of the collector in dotted decimal format for IPv4
- ipv6-address : x:x:x:x::x format for IPv6 address of the collector (where :: notation specifies successive hexadecimal fields of zeros)

The following example shows how to delete a remote syslog server with the ip address 1.1.1.1.

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

Note

- The format of the syslog messages sent to configured syslog servers is defined in RFC3164. The following packet opened in Wireshark is an example. At the header of the syslog message, the facility and severity levels are encoded and placed between angle brackets ("<" and ">").



49 Subport

Subport Show commands

show subinterfaces status

This command display the Subport configuration and status.

Usage
show subinterfaces status

Example

```
admin@sonic:~# show subinterfaces status

  Sub port interface    Speed    MTU    Vlan    Admin    Parent admin                 Type

--------------------  -------  -----  ------  -------  --------------  --------------------

        Ethernet4.10     100G   9100      10       up              up  802.1q-encapsulation

      Ethernet4.4094     100G   9100    4094       up              up  802.1q-encapsulation
```

Subport Configuration commands

A subport interface is added (or removed) when it's configured with IP address ("config interface ip") or bound on a VRF ("config interface vrf"), If user does not specify the <vrf name>, the L3 configuration on subport interface is bound on default VRF.

User should be careful in configuring sequence of "config interface vrf" and "config interface ip". (please refer example.)

config interface ip add/remove

Configuring IP address on subport is the same as config interface ip add/remove command.

This command will automatically add (or remove) subport interface if the subport interface does not exist (or already existed).

The VLAN ID in subport interface name specifies the 802.1q Vlan tagging. The ingress and egress packets of subport interface should be tagged with the VLAN ID. For example, for sub port interface Ethernet4.20, Vlan 20 is used for 802.1q Vlan tagging.

Usage
config interface ip {add|remove} <sub_port_interface_name> <ip_addr>

Parameters

- sub_port_interface_name: specify subport to add (or remove) subport interface

Example
admin@sonic:~# sudo config interface ip add Ethernet4.20 192.169.1.1/24 admin@sonic:~# sudo config interface ip remove Ethernet4.20 192.169.1.1/24

50 System State

Table of Contents

Processes

This command is used to determine the CPU utilization. It also lists the active processes along with their

corresponding process ID and other relevant parameters.

This sub-section explains the various "processes" specific data that includes the following.

- cpu Show processes CPU info
- memory Show processes memory info
- summary Show processes info

The "show processes" commands provide a wrapper over Linux's "top" command.

The "show process cpu" command sorts the processes being displayed by cpu-utilization, whereas "show process memory" does it for processes' memory-utilization.

show processes cpu

This command displays the current CPU usage by process. This command uses Linux's "top -bn 1 -o %CPU" command to display the output.

Usage
show processes cpu

Tip : Users can pipe the output to "head" to display only the "n" number of lines (e.g., show processes cpu | head -n 10).

Example
admin@sonic:~$ show processes cpu top - 23:50:08 up 1:18, 1 user, load average: 0.25, 0.29, 0.25

Tip : Advanced users can view individual processes using variations of the ps command (e.g., ps -ax | grep <process name>).

show processes memory

This command displays the current memory usage by processes. This command uses Linux's "top -bn 1 -o %MEM" command to display the output.

Usage
show processes memory

Note:

- the pipe option can be used using " | head -n" to display only the "n" number of lines

Example

```
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
```

show processes summary

This command displays the current summary information about all the processes.

Usage
show processes summary

Example
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

Services & Memory

These commands are used to know the services that are running and the memory that is currently utilized.

show services

This command displays the state of all the SONiC processes running inside a docker container. This helps to identify the status of SONiC's critical processes.

Usage
show services

Example

```
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
...
```

show system-memory

This command displays the system-wide memory utilization information – just a wrapper over the Linux native "free" command.

Usage
show system-memory

Example
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

show mmu (Not Supported)

This command displays the virtual address to physical address translation status of the Memory Management Unit (MMU).

Usage
show mmu

Example
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
---------  --------------------------------
```

show line (Not Supported)

This command displays the serial port or a virtual network connection status. This command is used only when SONiC is used as a console switch. This command is not applicable when SONiC used as a regular switch.

Note: This command is not working. It crashes as follows. A bug ticket is opened for this issue.

Usage
show line

Example
admin@sonic:~$ show line

System-Health

System health monitor is intended to monitor both critical services/processes and peripheral device status and leverage system log, system status LED to and CLI command output to indicate the system status.

show system-health detail

This command displays the system-health detail information.

Usage
show system-health detail

Example

```
admin@wedge100bf-32x-1:~$ sudo show system-health detail
System status summary
  System status LED
  Services:
    Status: OK
  Hardware:
    Status: Not OK
    Reasons: Invalid temperature data for PSU 2, temperature=N/A, threshold=N/A
             PSU 1 is out of power
System services and devices monitor list
Name                    Status    Type
----------------------  --------  ----------
wedge100bf-32x-1          OK       System
rsyslog                   OK       Process
root-overlay              OK       Filesystem
var-log                   OK       Filesystem
routeCheck                OK       Program
diskCheck                 OK       Program
container_checker         OK       Program
vnetRouteCheck            OK       Program
container_memory_telemetry  OK       Program
telemetry:telemetry       OK       Process
telemetry:dialout         OK       Process
snmp:snmpd                OK       Process
snmp:snmp-subagent        OK       Process
sflow:sflowmgrd           OK       Process
lldp:lldpd                OK       Process
```

```
lldp:lldp-syncd          OK      Process
lldp:lldpmgrd            OK      Process
nat:natmgrd              OK      Process
nat:natsyncd             OK      Process
syncd:syncd              OK      Process
teamd:teammgrd           OK      Process
teamd:teamsyncd          OK      Process
teamd:tlm_teamd          OK      Process
p4rt:p4rt                OK      Process
swss:orchagent           OK      Process
swss:portsyncd           OK      Process
swss:neighsyncd          OK      Process
swss:fdbsyncd            OK      Process
swss:vlanmgrd            OK      Process
swss:intfmgrd            OK      Process
swss:portmgrd            OK      Process
swss:buffermgrd          OK      Process
swss:vrfmgrd             OK      Process
swss:nbrmgrd             OK      Process
swss:vxlanmgrd           OK      Process
swss:coppmgrd            OK      Process
swss:tunnelmgrd          OK      Process
swss:esmgrd              OK      Process
bgp:zebra                OK      Process
bgp:staticd              OK      Process
bgp:bgpd                 OK      Process
bgp:fpmsyncd             OK      Process
bgp:essyncd              OK      Process
bgp:bgpcfgd              OK      Process
database:redis           OK      Process
PSU 1                    Not OK  PSU
PSU 2                    Not OK  PSU
counter-rotating-fan-1   OK      Fan
counter-rotating-fan-2   OK      Fan
```

```
counter-rotating-fan-3     OK       Fan
counter-rotating-fan-4     OK       Fan
counter-rotating-fan-5     OK       Fan
System services and devices ignore list
Name    Status    Type
------  --------  ------
```

show system-health monitor-list

This command displays system-health monitored services and devices name list.

Usage
show system-health monitor-list

Example

```
admin@wedge100bf-32x-1:~$ sudo show system-health monitor-list
System services and devices monitor list
Name                    Status    Type
----------------------  --------  ----------
wedge100bf-32x-1          OK       System
rsyslog                   OK       Process
root-overlay              OK       Filesystem
var-log                   OK       Filesystem
routeCheck                OK       Program
diskCheck                 OK       Program
container_checker         OK       Program
vnetRouteCheck            OK       Program
container_memory_telemetry  OK       Program
telemetry:telemetry       OK       Process
telemetry:dialout         OK       Process
```

```
snmp:snmpd              OK      Process
snmp:snmp-subagent      OK      Process
sflow:sflowmgrd         OK      Process
lldp:lldpd              OK      Process
lldp:lldp-syncd         OK      Process
lldp:lldpmgrd           OK      Process
nat:natmgrd             OK      Process
nat:natsyncd            OK      Process
syncd:syncd             OK      Process
teamd:teammgrd          OK      Process
teamd:teamsyncd         OK      Process
teamd:tlm_teamd         OK      Process
p4rt:p4rt               OK      Process
swss:orchagent          OK      Process
swss:portsyncd          OK      Process
swss:neighsyncd         OK      Process
swss:fdbsyncd           OK      Process
swss:vlanmgrd           OK      Process
swss:intfmgrd           OK      Process
swss:portmgrd           OK      Process
swss:buffermgrd         OK      Process
swss:vrfmgrd            OK      Process
swss:nbrmgrd            OK      Process
swss:vxlanmgrd          OK      Process
swss:coppmgrd           OK      Process
swss:tunnelmgrd         OK      Process
swss:esmgrd             OK      Process
bgp:zebra               OK      Process
bgp:staticd             OK      Process
bgp:bgpd                OK      Process
bgp:fpmsyncd            OK      Process
bgp:essyncd             OK      Process
bgp:bgpcfgd             OK      Process
database:redis          OK      Process
```

PSU 1	Not OK	PSU
PSU 2	Not OK	PSU
counter-rotating-fan-1	OK	Fan
counter-rotating-fan-2	OK	Fan
counter-rotating-fan-3	OK	Fan
counter-rotating-fan-4	OK	Fan
counter-rotating-fan-5	OK	Fan

show system-health summary

This command displays system-health summary information.

Usage
show system-health summary

Example
admin@wedge100bf-32x-1:~$ sudo show system-health summary System status summary System status LED Services: Status: OK Hardware: Status: Not OK Reasons: Invalid temperature data for PSU 2, temperature=N/A, threshold=N/A PSU 1 is out of power

51 Troubleshooting

Table of Contents

Collect techsupport information

show techsupport

In field service, there is limited time to gather information for troubleshooting and debugging. The command gathers show techsupport relevant information about the state of the device; information as diverse as syslog entries, database state, routing-stack state, etc. It then compresses the information into an archive file. This archived file can then be sent to the SONiC development team for examination.

Usage
show techsupport [--since=<time_specifier>] show techsupport [--nolog]

Options:

- --since Collect logs and core files since a given date.
- --silent Run techsupport in silent mode.
- --nolog Collect system information without syslog to reduce the archive file size.

Note

- The archive file is stored in /var/dump/<DEVICE_HOST_NAME>_YYYYMMDD_HHMMSS.tar.gz
- The location and name of the archive file will be displayed at the end of the execution of the command "show techsupport "

This command can generate a large dump file after the SONiC system has been running for a long time and there are exhaustive system resources. When the log files are specified for a certain period (by using the " –since" option) or are not been included (by using the " –no log" option), the dump file size can be reduced to MB level and the time to collect the data is also reduced relatively.

Example
admin@sonic:~$ show techsupport --since=yesterday # Will collect syslog and core files for the last 24 hours admin@sonic:~$ show techsupport --since='hour ago' # Will collect syslog and core files for the last one hour admin@sonic:~$ show techsupport --nolog # Will not collect syslog and core files

Usage of "logger"

Use the 'logger' command to add a marker to make it simple to find associated Syslog entries for a reported issue.

If there is a way to reproduce an issue by a specific procedure, it would be very helpful to execute a logger command to add a special mark into the syslog before and after reproducing the issue.

For example, execute the first logger command before recreating the issue, and then execute the second command after recreating the issue as shown below. Using this marker, you can grep the syslog to know which part of the syslog is related to the reported issue. The related syslog content will be the messages between "===== test start=====" and "===== test finish=====".

```
logger ===== test start=====
logger ===== test finish=====
```

Example demonstration

Examples of collecting device information and log files, and sending them to a remote host using the "show techsupport" command.

It is known that a large number of log files will be generated if the device has been running for a long time. Therefore, it will consume more time to process those files into an archive file.

Example 1: Collect the device information along with the log files

Step 1: Execute the show techsupport command with "--since" option.

Example
admin@as5835-54x-3:~$ show techsupport --since='hour ago' main mkdir: created directory '/var/dump/sonic_dump_as5835-54x_20210129_071517' '/var/dump/sonic_dump_as5835-54x_20210129_071517/generate_dump' -> '/usr/bin/generate_dump' sonic_dump_as5835-54x_20210129_071517/ sonic_dump_as5835-54x_20210129_071517/generate_dump mkdir: created directory '/var/dump/sonic_dump_as5835-54x_20210129_071517/proc' ... (skipped) ... /var/dump/sonic_dump_as5835-54x_20210129_071517.tar.gz

Step 2: Use the scp command to copy the archive file from the local device (File generated from step 1) to a remote site.

Example
admin@as5835-54x:~$ sudo scp /var/dump/sonic_dump_as5835-54x_20210129_071517.tar.gz sonic@10.250.2.44:/home /sonic/tmp_dennis/ sonic@10.250.2.44's password: sonic_dump_as5835-54x_20210129_071517.tar.gz 100% 3111KB 86.4MB/s 00:00

Example 2: Collect the device information and log files separately

Step 1: Execute the show techsupport command with "--no log" option to collect the device information.

Example
admin@as5835-54x-3:~$ show techsupport --nolog main mkdir: created directory '/var/dump/sonic_dump_as5835-54x-3_20210129_082320' '/var/dump/sonic_dump_as5835-54x-3_20210129_082320/generate_dump' -> '/usr/bin/generate_dump' sonic_dump_as5835-54x-3_20210129_082320/ sonic_dump_as5835-54x-3_20210129_082320/generate_dump mkdir: created directory '/var/dump/sonic_dump_as5835-54x-3_20210129_082320/proc' ... (skipped) ... /var/dump/sonic_dump_as5835-54x-3_20210129_082320.tar.gz

Step 2: Use the scp command to copy the archive file from the local device to a remote site.

Example
admin@as5835-54x-3:~$ sudo scp /var/dump/sonic_dump_as5835-54x-3_20210129_082320.tar.gz sonic@10.250.2.44: /home/sonic/tmp_dennis/ sonic@10.250.2.44's password: sonic_dump_as5835-54x-3_20210129_082320.tar.g 100% 2007KB 81.7MB/s 00:00

Step 3: Use the scp to copy the log (ex:syslog) file from the local device to a remote site.

Example
admin@as5835-54x-3:~$ sudo scp /var/log/syslog* sonic@10.250.2.44:/home/sonic/tmp_dennis/sonic_log/ sonic@10.250.2.44's password: syslog 100% 20KB 11.4MB/s 00:00

```
syslog.1 100% 2056KB 79.5MB/s 00:00
syslog.2.gz 100% 162KB 58.4MB/s 00:00
syslog.3.gz 100% 160KB 59.7MB/s 00:00
syslog.4.gz 100% 170KB 65.7MB/s 00:00
...
(skipped)
...
syslog.4.gz 100% 170KB 65.7MB/s 00:00
```

52 TFTP

53 VLAN

Table of Contents

VLAN Show Commands

show vlan brief

This command displays brief information about all the VLANs configured on 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 un tagged mode, and the DHCP Helper Address.

Usage
show vlan brief

Example
admin@sonic:~$ show vlan brief +-----------+----------------+-----------+---------------+------------+--------------+------------- +------------+

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

show vlan brief --mtu

This command is used to display the VLAN ID, VLAN MTU, list of VLAN member ports and mtu of member ports.

Example
admin@sonic:~$ show vlan brief -- mtu +----------+-----------+-----------+----------- + | VLAN ID | VLAN MTU | Ports | Port MTU | +===========+============+============+============+ | 100 | 1500 | Ethernet0 | 1500 | | | | Ethernet4 | 1500 |

show vlan config

This command displays all the VLAN configuration.

Usage
show vlan config

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

show vlan brief --mac

Example
admin@sonic:~$ show vlan brief --mac +-----------+---------------+-------------------+ | VLAN ID | Ports | VLAN MAC | +============+================+====================+ | 200 | Ethernet64 | 80:a2:35:88:88:89 | +-----------+---------------+-------------------+

VLAN Config Commands

This sub-section explains how to configure a VLAN and its member ports.

config vlan add/del

This command is used to add or delete a VLAN.

Usage
config vlan (add | del) <vlan_id>

Example (Create the VLAN "Vlan100" if it does not already exist)
admin@sonic:~$ sudo config vlan add 100

config vlan member add/del

This command is used to add or delete a member port to/from an already created VLAN.

Usage
config vlan member add/del [-u|--untagged] <vlan_id> <member_portname>

Note :

- Adding the -u or --un tagged flag will set the port member in "untagged" mode.
- It is not allowed to add an Ethernet port / port channel with a L3 configuration to a VLAN.
- An Ethernet port / port channel could only be added to one VLAN in un tagged mode.

Example (Add Ethernet0 as member of the vlan 100)
admin@sonic:~$ sudo config vlan member add 100 Ethernet0

Example (Add Ethernet4 as member of the vlan 100)
admin@sonic:~$ sudo config vlan member add 100 Ethernet4

config vlan mtu

This command is used to config vlan mtu. (default mtu of vlan is 9100)

Usage
config vlan mtu <vlan_id> <mtu>

Example
admin@sonic:~$ sudo config vlan mtu 100 1500

Note:

- The update of vlan mtu would not change the mtu of port.
- User needs to handle the port mtu when changing vlan mtu which is different from port MTU.
- sag interface and vrrp interface is created from vlan interface. The mtu of sag interface and vrrp interface would also changed as the same value as vlan mtu if v lan mtu is changed.
- The VLAN MTU refers to the data length at the L3 layer, not the total length of the entire packet. For packets with the same VLAN MTU, whether they are tagged (TAG) or untagged (non-TAG), the data length at the L3 layer can be different.

config vlan mac_address

Example
admin@sonic:~$ sudo config vlan add 200 admin@sonic:~$ sudo config vlan member add 200 -u Ethernet64 admin@sonic:~$ sudo config interface ip add Vlan200 200.1.1.200/24 admin@sonic:~$ sudo config vlan mac_address 200 80:a2:35:88:88:89 admin@sonic:~$ sudo ifconfig Vlan200 Vlan200: flags=4099<UP,BROADCAST,MULTICAST> mtu 9100 inet 200.1.1.200 netmask 255.255.255.0 broadcast 200.1.1.255

```
ether 80:a2:35:88:88:89  txqueuelen 1000  (Ethernet)
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
```

54 VLAN Stacking

Table of Contents

VLAN Stacking Show Commands

show vlan-stacking

This command displays the information about all the VLAN stacking rule configured on the device.

Usage
show vlan-stacking

Example
admin@sonic:~$ show vlan-stacking Interface Stage Match VLAN Action Apply VLAN ---------- ------- ---------- -------- ---------- Ethernet0 egress 200 pop Ethernet0 ingress 100 push 200 Ethernet4 egress 200 swap 100 Ethernet4 ingress 100 swap 200

VLAN Stacking Config Commands

This sub-section explains how to add(or delete) a VLAN stacking rule to(or from) the specified interface.

config vlan-stacking add

This command is used to add a VLAN stacking rule to interface.

Usage
config vlan-stacking add <interface_name> <stage> <match_vlan> <action> <apply_vlan>

Parameter:

<interface_name>: The name of physical interface or PortChannel, e.g. "Ethernet0" or "PortChannel0001".

<stage> : The traffic direction of the packet, e.g. "ingress" or "egress".

<match_vlan> : The VLAN ID on the packet which expected to match the rule(The range is from 1 to 4094).

<action> : The action applied to the packet when it matched the rule, e.g. "push", "pop" or "swap".

push: insert an <apply_vlan> (or SVLAN, outer VLAN) to the frame

pop: remove the <match_vlan> (or outer VLAN) from the frame

swap: replace the <match_vlan> (matched outer VLAN) with <apply_vlan>

<apply_vlan> : The VLAN ID applied to the packet according to the action field(The range is from 1 to 4094).

Example: Add vlan id 200, SVLAN, when ingress packet's vlan id is matched 100 on Ethernet0

Example
admin@sonic:~$ sudo config vlan-stacking add Ethernet0 ingress 100 push 200

config vlan-stacking del

This command is used to delete a VLAN stacking rule from interface.

Usage
config vlan-stacking del <interface_name> <stage> <match_vlan>

Parameter:

<interface_name>: The name of physical interface or PortChannel, e.g. "Ethernet0" or "PortChannel0001".

<stage> : The traffic direction of the packet, e.g. "ingress" or "egress".

<match_vlan> : The VLAN ID on the packet which expected to match the rule(The range is from 1 to 4094).

Example: Delete the configuration applied to egress packet which matched vlan id 200 on Ethernet0.

Example
admin@sonic:~$ sudo config vlan-stacking del Ethernet0 egress 200

Caveat

Do not support on DCS8500-128D, AS9746-128D, AS9817-64OC, AS9736-64D.

55 VRF Configuration

Table of Contents

VRF Show Commands

show vrf

This command displays all VRFs configured on the system along with interface binding to the VRF. If vrf-name is also provided as part of the command, when the VRF is created it will display all interfaces binding to the VRF. If the VRF is not created, nothing will be displayed.

Usage
show vrf [<vrf_name>]

Example
admin@sonic:~$ show vrf VRF Interfaces ------- ------------ Vrf-red Vlan100 Loopback11 Vrf-blue Loopback100 Loopback102

Note: You may refer to Interfaces for binding a VRF and interface.

VRF Config Commands

config vrf add

This command creates a VRF in the SONiC system with the provided VRF name.

Note: The vrf-name should always start with the keyword "Vrf".

Usage
config vrf add <vrf-name>

config vrf del

This command deletes the VRF with the name vrf-name .

Usage
config vrf del <vrf-name>

config vrf add_vrf_vni_map

This command creates VRF-VNI mapping in the SONiC system.

Note: The show command is in the VxLAN CLI guide.

Usage
config vrf add_vrf_vni_map <vrf-name> <vni>

Example
config vrf add Vrf1

config vxlan add vtep 10.1.0.32 config vxlan evpn_nvo add evpnnvo vtep config vrf add_vrf_vni_map Vrf1 20000

config vrf del_vrf_vni_map

This command deletes VRF-VNI mapping from the SONiC system.

Usage
config vrf del_vrf_vni_map <vrf-name>

56 VRF Route Leaking

The CLI configuration for VRF route leaking uses the vtysh command to configure static and dynamic route leaks.

For dynamic route leaking, BGP is used as an example.

Static VRF Route Leaking

The following command creates a static route that leaks the next hop into a specified VRF.

Usage
ip route <A.B.C.D/M> <A.B.C.D> nexthop-vrf <vrf-name>

Example
admin@sonic:~# vtysh sonic# configure sonic(config)# vrf Vrf1 sonic(config-vrf)# ip route 2.2.2.2/32 10.0.0.59 nexthop-vrf Vrf2 sonic(config-vrf)# end sonic# exit admin@sonic:~# admin@sonic:~# show ip route vrf Vrf1 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 route, r - rejected route VRF Vrf1: S>* 2.2.2.2/32 [1/0] via 10.0.0.59, PortChannel0002(vrf Vrf2), 01:34:15 C>* 10.0.0.56/31 is directly connected, PortChannel0001, 01:40:04

Dynamic VRF Route Leaking

Basic Configuration

The following command configures a dynamic VRF route leak that automatically imports routes between VRFs. In this example, the routes in the default VRF are imported to Vrf1.

Usage
import vrf <vrf-name>

Note:

- import vrf <vrf-name> is shortcut syntax for specifying automatic leaking from vrf-name to the current VRF. In the other words, you do not need to consider that the underlying mechanism relies on the BGP constructs of Route Distinguisher (RD) andRoute Targets (RTs), because they are automatically derived when you enable route leaking.

Example
admin@sonic:~# vtysh sonic# configure sonic(config)# router bgp 65200 vrf Vrf1 sonic(config-router)# address-family ipv4 unicast sonic(config-router-af)# import vrf default sonic(config-router-af)# end sonic# exit admin@sonic:~# admin@sonic:~# show ip route vrf Vrf1 193.11.248.128 Routing entry for 193.11.248.128/25 Known via "bgp", distance 200, metric 0, vrf Vrf1, best Last update 00:03:47 ago * 10.0.0.59, via PortChannel0002(vrf default) * 10.0.0.61, via PortChannel0003(vrf default) * 10.0.0.63, via PortChannel0004(vrf default)

Combine with route-map and prefix-list

You can also decide to select certain prefixes from being imported. The match rule must be configured in a route map.

Usage
import vrf route-map <name of route-map>

Note: Our test environment is a t0 topology, so the default VRF will get 6440 routes from peers.

Example
admin@sonic:~# vtysh sonic# configure sonic(config)# ip prefix-list test_vrf_route_leak seq 5 deny 193.11.248.0/25 sonic(config)# ip prefix-list test_vrf_route_leak seq 10 permit 193.11.240.128/25 sonic(config)# route-map VRF_ROUTE_LEAK permit 5 sonic(config-route-map)# match ip address prefix-list test_vrf_route_leak sonic(config-route-map)# exit sonic(config)# router bgp 65200 vrf Vrf1 sonic(config-router)# address-family ipv4 unicast sonic(config-router-af)# import vrf route-map VRF_ROUTE_LEAK sonic(config-router-af)# import vrf default sonic(config-router-af)# end

57 VxLAN (includes EVPN and EVPN-MH)

Table of Contents

VxLAN Show Commands

show vxlan tunnel

This command displays brief information about VxLANs configured in the device. It displays VxLAN tunnel name, source IP address, destination IP address and VLAN VNI tunnel mappings.

Usage

show vxlan tunnel

Example
admin@sonic:~$ show vxlan tunnel vxlan tunnel name source ip destination ip tunnel map name tunnel map mapping(vni -> vlan) ---------- ---------- ---------- ---------- ---------- vtep 1.1.1.1 map_3000_Vlan30 3000 -> Vlan30

show vxlan name <vxlanname>

This command displays brief information for a specified VxLAN tunnel. It displays VxLAN tunnel name, source IP address, destination IP address and VLAN VNI tunnel mappings.

Usage
show vxlan name <vxlanname>

Example
admin@sonic:~$ show vxlan name vtep vxlan tunnel name source ip destination ip tunnel map name tunnel map mapping(vni -> vlan) ---------- ---------- ---------- ---------- ---------- vtep 1.1.1.1 map_3000_Vlan30 3000 -> Vlan30

show vxlan interface

This command displays brief VTEP information.

Usage
show vxlan interface

Example

```
admin@sonic:~$ show vxlan interface
VTEP Information:
        VTEP Name : vtep, SIP  : 1.1.1.1
        NVO Name  : nvo,  VTEP : vtep
        Source interface  : Loopback0
```

show vxlan vlanvnimap

This command displays all the VLAN VNI mappings.

Usage
show vxlan vlanvnimap

Example

```
admin@sonic:~$ show vxlan vlanvnimap
+--------+-------+
| VLAN   | VNI   |
+========+=======+
| Vlan30 | 3000  |
+--------+-------+
Total count : 1
```

show vxlan vrfvnimap

This command displays all the VRF VNI mappings.

Note: The config commands are in the VRF CLI guide.

Usage
show vxlan vrfvnimap

Example

```
admin@sonic:~$ show vxlan vrfvnimap
+-------+-------+
| VRF   |   VNI |
+=======+=======+
| Vrf-1 |   104 |
+-------+-------+
Total count : 1
```

show vxlan remote_mac <remoteip/esi/all>

This command displays all MACs learnt from a specified remote VTEP IP, from a specified ESI, or from all of the remote VTEP IPs for all VNIs.

Usage
show vxlan remote_mac <remoteip/esi/all>

Example

```
admin@sonic:~$ show vxlan remotemac 2.2.2.2
+---------+-------------------+-------------+-------+-------+---------+
| VLAN    | MAC               | RemoteVTEP  | ESI   |   VNI | Type    |
+=========+===================+=============+=======+=======+=========+
| Vlan1000 | 00:12:34:56:78:90 | 2.2.2.2     |       |   100 | dynamic |
+---------+-------------------+-------------+-------+-------+---------+
Total count : 1
admin@sonic:~$ show vxlan remotemac 03:00:11:22:33:44:55:00:00:a8
+---------+-------------------+-------------+-----------------------------+-------+---------+
| VLAN    | MAC               | RemoteVTEP  | ESI                         |   VNI | Type    |
+=========+===================+=============+=============================+=======+=========+
| Vlan1000 | 00:55:66:77:88:AA |             | 03:00:11:22:33:44:55:00:00:a8 |   100 | dynamic |
+---------+-------------------+-------------+-----------------------------+-------+---------+
Total count : 1
```

```
admin@sonic:~$ show vxlan remotemac all
+---------+-----------------+------------+--------------------------+------+--------+
| VLAN    | MAC             | RemoteVTEP | ESI                      |  VNI | Type   |
+=========+=================+============+==========================+======+========+
| Vlan1000 | 00:12:34:56:78:90 | 2.2.2.2    |                          |  100 | dynamic |
+---------+-----------------+------------+--------------------------+------+--------+
| Vlan1000 | 00:55:66:77:88:AA |            | 03:00:11:22:33:44:55:00:00:a8 |  100 | dynamic |
+---------+-----------------+------------+--------------------------+------+--------+
Total count : 2
```

show vxlan remote_vni <remoteip/all>

This command displays all the VNIs learnt from the specified remote VTEP, or all the VNIs learnt from all of the remote VTEPs.

Usage
show vxlan remote_vni <remoteip/all>

Example
admin@sonic:~$ show vxlan remote_vni 3.3.3.3 +---------+-------------+-------+ | VLAN | RemoteVTEP | VNI | +=========+=============+=======+ | Vlan101 | 3.3.3.3 | 1001 | +---------+-------------+-------+ Total count : 1

show vxlan remotevtep

This command displays all remote VTEPs (a.k.a. VxLAN tunnels) learnt by EVPN/VxLAN.

Usage
show vxlan remotevtep

Example
admin@sonic:~$ show vxlan remotevtep +-------------+-------------+-------------------+--------------+ | SIP | DIP | Creation Source | OperStatus | +==============+==============+====================+==============+ | 11.11.11.11 | 22.22.22.22 | EVPN | oper_up | +-------------+-------------+-------------------+--------------+ Total count : 1

show vxlan evpn es

This command display all Ethernet Segments. The 'status' field indicates the operation status of the corresponding PortChannel interface.

Usage
show vxlan evpn es

Example
admin@sonic:~$ show vxlan evpn es Type: L local, R remote, N non-DF +-----------------------------+--------+-----------------+----------+-------------+ | ESI | Type | ES Interface | status | VTEPS | +================================+========+=================+==========+=============+ | 03:44:38:39:ab:cd:01:00:00:01 | LRN | PortChannel0001 | down | 1.1.1.1 | | | | | | 2.2.2.2 | | | | | | 3.3.3.3 | | | | | | 4.4.4.4 |

```
|                           |      |              |         | 5.5.5.5    |
+---------------------------+------+--------------+---------+------------+
| 03:44:38:39:ab:cd:01:00:00:02 | L    | PortChannel0002 | up      |            |
+---------------------------+------+--------------+---------+------------+
| 03:44:38:39:ab:cd:01:00:00:03 | RN   |              |         | 172.0.0.24 |
|                           |      |              |         | 172.0.0.25 |
|                           |      |              |         | 172.0.0.26 |
+---------------------------+------+--------------+---------+------------+
Total count : 3
```

show neigh-suppress

This command display neighbor suppression status.

Usage
show neigh-suppress { all | vlan <vlan-id> }

Example

```
root@sonic:/home/admin# show neigh-suppress all
+---------+-----------+--------------------+
| VLAN    | STATUS    | ASSOCIATED_NETDEV  |
+=========+===========+====================+
| Vlan500 | Configured | vtep-500          |
+---------+-----------+--------------------+
| Vlan600 | Configured | vtep-600          |
+---------+-----------+--------------------+
Total count : 2

root@sonic:/home/admin#
```

VxLAN Configuration Commands

config vxlan add <vtepname> <src_ipv4>

This command is for VTEP Source IP configuration. The vtepname is a string, and src_ipv4 is an IPV4 address in dotted notation A.B.C.D .

Usage
config vxlan add <vtepname> <src_ipv4>

Example
sudo config vxlan add vtep 1.1.1.1

config vxlan evpn_nvo add <nvoname> <vtepname>

This command is for NVO configuration.

Usage
config vxlan evpn_nvo add <nvoname> <vtepname>

Example
sudo config vxlan evpn_nvo add nvo vtep

config vxlan map add <vtepname> <vlanid> <vnid>

This command creates VLAN-VNI mapping on the VTEP with name vtepname .

Usage
config vxlan map add <vtepname> <vlanid> <vnid>

Example
sudo config vxlan map add vtep 30 3000

config vxlan evpn_es add <portchannelname> <esid> [<sysmac>]

This command creates an Ethernet Segment on specified PortChannel interface.

Usage
config vxlan evpn_es add <protchannelname> <esid> [<sysmac>]

Example
#type 0 sudo config vxlan evpn_es add PortChannel0001 00:11:22:33:44:55:66:77:88:99 #type 3 sudo config vxlan evpn_es add PortChannel0001 168 00:11:22:33:ab:cd

config vxlan del <vtepname>

This command deletes a VTEP with name vtepname .

Usage
config vxlan del <vtepname>

Example
sudo config vxlan del vtep

config vxlan evpn_nvo del <nvoname>

This command deletes NVO with name nvoname .

Usage
config vxlan evpn_nvo del <nvoname>

Example
sudo config vxlan evpn_nvo del nvo

config vxlan map del <vtepname> <vlanid> <vnid>

This command deletes specific VLAN-VNI mapping on the VTEP with name vtepname .

Usage
config vxlan map del <vtepname> <vlanid> <vnid>

Example
sudo config vxlan map del vtep 30 3000

config vxlan evpn_es del <portchannelname>

This command deletes the Ethernet Segment on specified PortChannel interface.

Usage
config vxlan evpn_es del <protchannelname>

Example
sudo config vxlan evpn_es del PortChannel0001

config neigh-suppress vlan

This command will suppress both ARP & ND flooding over the tunnel when Vlan is extended.

Usage
config neigh-suppress vlan <vlan-id> <"on"/"off">

Note：vlan-id represents the VLAN

ID and on/off is enabled or disabled. By default ARP/ND suppression is disabled.

Example
config neigh-suppress vlan 600 on

58 Warm Reboot

Warm Reboot Configuration Commands

warm-reboot

This command initiates a warm reboot of the device. The command does not require setting a warm restart configuration, it sets up everything needed to perform a warm reboot. This command requires root privilege.

Usage
warm-reboot \[-h|-?|-v|-f|-r|-k|-x|-c <control plane assistant IP list>|-s\]

Parameters:

- -h,-? : get this help
- -v : turn on verbose mode
- -f : force execution
- -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.

Example
admin@sonic:~$ sudo warm-reboot -v Tue Oct 22 23:20:53 UTC 2019 Pausing orchagent ... Tue Oct 22 23:20:53 UTC 2019 Stopping radv ... Tue Oct 22 23:20:54 UTC 2019 Stopping bgp ... Tue Oct 22 23:20:54 UTC 2019 Stopped bgp ... Tue Oct 22 23:20:57 UTC 2019 Initialize pre-shutdown ... Tue Oct 22 23:20:58 UTC 2019 Requesting pre-shutdown ... Tue Oct 22 23:20:58 UTC 2019 Waiting for pre-shutdown ... Tue Oct 22 23:20:59 UTC 2019 Pre-shutdown succeeded ... Tue Oct 22 23:20:59 UTC 2019 Backing up database ... Tue Oct 22 23:21:00 UTC 2019 Stopping teamd ... Tue Oct 22 23:21:00 UTC 2019 Stopped teamd ... Tue Oct 22 23:21:00 UTC 2019 Stopping syncd ... Tue Oct 22 23:21:11 UTC 2019 Stopped syncd ... Tue Oct 22 23:21:11 UTC 2019 Stopping all remaining containers ... Tue Oct 22 23:21:13 UTC 2019 Stopped all remaining containers ... Tue Oct 22 23:21:15 UTC 2019 Rebooting with /sbin/kexec -e to SONiC-OS-20191021.01 ...

59 Warm Restart

Table of Contents

Besides a device-level warm reboot, SONiC also provides a docker-based warm restart. This feature is currently upported by the following dockers: BGP, teamD, and SWSS. A user can manage to restart a particular docker with no interruption on packet forwarding and no effect on other services. This helps to reduce operational costs as well as development efforts. For example, to fix a bug in the BGP routing stack, only the BGP docker image needs to be built, tested, and upgraded.

To achieve uninterrupted packet forwarding during the restarting stage and database reconciliation at the post starting stage, warm restart enables dockers with adjacency state machine to facilitate standardized protocols.

For example, a BGP restarting switch must have BGP "Graceful Restart" enabled, and its BGP neighbors must be "Graceful Restart Helper Capable", as specified in IETF RFC4724.

Before executing a warm restart for the BGP docker, the following BGP commands should be enabled:

```
bgp graceful-restart
bgp graceful-restart preserve-fw-state
```

In the current SONiC release, the above two commands are enabled by default.

You should be aware that during a warm restart, certain BGP fast convergence features and black hole avoidance features should either be disabled or set to a lower preference to avoid conflicts with the BGP graceful restart.

For example, BGP BFD could be disabled via:

```
no neighbor <A.B.C.D|X:X::X:X|WORD> bfd
```

otherwise, the fast failure detection would cause packet drop during the warm reboot.

Another commonly deployed blackhole avoidance feature: dynamic route priority adjustment, could be disabled to avoid large routes churn during BGP restart. Use the following command.

```
no bgp max-med on-peerup
```

Warm Restart Show Commands

show warm_restart config

This command displays all the configuration related to a warm restart.

Usage
show warm_restart config

Example
admin@sonic:~$ show warm_restart config name enable timer_name timer_duration

show warm_restart state

This command displays the warm restart state.

Usage
show warm_restart state

Example
admin@sonic:~$ show warm_restart state name restore_count state orchagent 0 vlanmgrd 0 bgp 1 reconciled portsyncd 0 teammgrd 1 neighsyncd 0 teamsyncd 1 syncd 0 natsyncd 0

Warm Restart Config Commands

This sub-section explains the various configurations related to the warm restart feature. The following parameters can be configured using this command.

1. bgp_timer
2. disable
3. enable
4. neighsyncd_timer
5. teamsyncd_timer

Each of these sub-commands are explained in the following section.

Users can use an optional parameter -s to use the unix domain socket for communicating with the RedisDB which will be faster when compared to using the default network sockets. All these commands have the following option.

Options: -s, --redis-unix-socket-path TEXT unix socket path for redis connection.

config warm_restart bgp_timer (Not Supported)

This command is used to set the BGP timer value for warm restart of the BGP service. bgp_timer holds the time interval utilized by fpm syncd during warm-restart episodes. During this interval, fpmsyncd will recover all the routing states previously pushed to AppDB, as well as all new states coming from zebra/bgpd. Upon expiration of this timer, fpmsyncd will execute the reconciliation logic to eliminate all the stale entries from AppDB. This timer should match the BGP-GR restart-timer configured within the elected routing- stack.

Usage
config warm_restart [-s|--redis-unix-socket-path <socket_path>] bgp_timer <seconds>

Parameters:

seconds: Range from 1 to 3600

Example
admin@sonic:~$ sudo config warm_restart bgp_timer 1000

config warm_restart enable/disable

This command is used to enable or disable the warm restart for a particular service that supports warm reboot. The following four services support warm reboot. When a user restarts the particular service using systemctl restart <service_name> , this configured value will be checked for whether it is enabled or disabled. If this configuration is enabled for that service, it will perform awarm reboot for that service. Otherwise, it will do a cold restart of the service.

Usage
config warm_restart [-s|--redis-unix-socket-path <socket_path>] enable [<module_name>]

Parameters:

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

Example (Set warm_restart as "enable" for the "system" service)
admin@sonic:~$ sudo config warm_restart enable

Example (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

Example (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

config warm_restart neighsyncd_timer (Not Supported)

This command is used to set the neighsyncd_timer value for a warm restart of the swss service. The neighsyncd_timer is the timer used for swss (neighsyncd) service during the warm restart. The timer is started after the neighborTable is restored to internal data structures.

Then, neighborsyncd 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 Valid value is 1-9999. 0 is invalid.

Usage
config warm_restart [-s|--redis-unix-socket-path <socket_path>] neighsyncd_timer <seconds>

Parameters:

- seconds: Range from 1 to 9999

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

config warm_restart bgp_timer (Not Supported)

This command is used to set the bgp_timer value for a warm restart of the bgp service. The bgp_timer is the timer used for the bgp ser vice during the warm restart. The 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 1-9999. 0 is invalid.

Usage

config warm_restart [-s|--redis-unix-socket-path <socket_path>] bgp_timer <seconds>

Parameters:

- seconds: Range from 1 to 9999

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

config warm_restart teamsyncd_timer (Not Supported)

This command is used to set the teamsyncd_timer value for a warm restart of the teamd service. The teamsyncd_timer holds the time interval utilized by teamsyncd during warm-restart episodes. 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: 1-9999. 0 is invalid.

Usage
config warm_restart teamsyncd_timer <seconds>

Parameters:

- seconds: Range from 1 to 9999

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

60 Watermark

Watermark Show Commands

show watermark telemetry interval

This command displays the configured interval for the telemetry.

Usage
show watermark telemetry interval

Example
admin@sonic:~$ show watermark telemetry interval Telemetry interval 120 second(s)

Watermark Config Commands

config watermark telemetry interval

This command is used to configure the interval for telemetry. The default interval is 120 seconds. There is no regulation on the valid range of values; it leverages the Linux timer.

Usage
config watermark telemetry interval <value>

Example

```
admin@sonic:~$ sudo config watermark telemetry interval 999
```

61 WRED & ECN

Table of Contents

This section explains all the Explicit Congestion Notification (ECN) show commands and ECN configuration

options that are supported in SONiC.

WRED & ECN Show Commands

show wred

This command is used to display the WRED profile.

Usage
show wred [<profile_name>]

Parameters:

<profile_name>: Profile name.

Example
admin@sonic:~$ show wred Profile: ecn_prof Color Mode Min Threshold Max Threshold Drop Probability ------- ------ --------------- --------------- ------------------ Green ECN 100 10000 25 Yellow ECN 200 20000 50 Red ECN 400 40000 75

show interface wred

This command is used to display the WRED configuration for all interfaces or a given interface.

Usage
show interface wred <interface_name>

Parameters:

<interface_name>: Physical interface name. For example: "Ethernet0".

Example
admin@as9516-32d-2:~$ show interface wred Ethernet0 Queue: 0 ECN/WRED: ecn_prof2 Color Mode Min Threshold Max Threshold Drop Probability Green ECN 5000 10000 100 Yellow ECN Red ECN

WRED & ECN Configuration Commands

config wred add

This command is used to create a WRED profile.

Usage
config wred add <profile> --mode={ecn|wred} {--gmin <gmin> --gmax <gmax> --gdrop <gdrop>} [--ymin <ymin> --ymax <ymax> --ydrop <ydrop>] [--rmin <rmin> --rmax <rmax> --rdrop <rdrop>]

Note: On mellano switchs, the command distinguishes between ecn and wred through mode, and other parameters are shared.

Parameters:

- <profile_name>: Profile name.
- mode: ECN or WRED mode.
    - ecn: Enable ECN marking.
    - wred : Enable WRED dropping.

- <gmin>: Minimum threshold in bytes to start WRED dropping or ECN marking for green packet.
- <gmax>: Maximum threshold in bytes for WRED dropping or ECN marking for green packet.
- <gdrop>: Maximum dropping or marking probability for green packet. Minimum: 0. Maximum: 100.
- <ymin>: Minimum threshold in bytes to start WRED dropping or ECN marking for yellow packet.
- <ymax>: Maximum threshold in bytes for WRED dropping or ECN marking for yellow packet.
- <ydrop>: Maximum dropping or marking probability for yellow packet. Minimum: 0. Maximum: 100.
- <rmin>: Minimum threshold in bytes to start WRED dropping or ECN marking for red packet.
- <rmax>: Maximum threshold in bytes for WRED dropping or ECN marking for red packet.
- <rdrop>: Maximum dropping or marking probability for red packet. Minimum: 0. Maximum: 100.

Note:

The devices using the Broadcom ASIC, the maximum drop probability supports one of [0~10, 25, 50, 75, 100] in hardware.

- If the user configuration value is from 0 to 10, takes the same value as hardware configuration.
- If the user configuration value is from 10 to 24, takes 10 as hardware configuration.
- If the user configuration value is from 25 to 49, takes 25 as hardware configuration.
- If the user configuration value is from 50 to 74, takes 50 as hardware configuration.
- If the user configuration value is from 75 to 99, takes 75 as hardware configuration.
- If user configuration value exceeds 100, takes 100 is used for hardware configuration.

The following table shows the maximum threshold per switch.

Switch	Maximum Threshold (bytes)
AS5835-54X AS7326-56X AS7726-32X	67,108,608
AS9746-32D AS9736-64D	133,168,898
AS9746-128d	158,220,288

Example
sudo config wred add ecn_profile --mode ecn --gmin 5000 --gmax 10000 --gdrop 100

config wred update

This command is used to modify an existing WRED profile.

Usage
config wred update <profile> [--mode={ecn|wred}] [--gmin <gmin> --gmax <gmax> --gdrop <gdrop>] [--ymin <ymin> --ymax <ymax> --ydrop <ydrop>] [--rmin <rmin> --rmax <rmax> --rdrop <rdrop>] [--no-green] [--no-yellow] [--no-red]

Parameters:

- <profile_name>: Profile name.
- mode: ECN or WRED mode.
    - ecn: Enable ECN marking.
    - wred : Enable WRED dropping.
- <gmin>: Minimum threshold in bytes to start WRED dropping or ECN marking for green packet.
- <gmax>: Maximum threshold in bytes for WRED dropping or ECN marking for green packet.
- <gdrop>: Maximum dropping or marking probability for green packet. Minimum: 0. Maximum: 100.
- <ymin>: Minimum threshold in bytes to start WRED dropping or ECN marking for yellow packet.
- <ymax>: Maximum threshold in bytes for WRED dropping or ECN marking for yellow packet.
- <ydrop>: Maximum dropping or marking probability for yellow packet. Minimum: 0. Maximum: 100.
- <rmin>: Minimum threshold in bytes to start WRED dropping or ECN marking for red packet.
- <rmax>: Maximum threshold in bytes for WRED dropping or ECN marking for red packet.
- <rdrop>: Maximum dropping or marking probability for red packet. Minimum: 0. Maximum: 100.
- no-green: Remove the green setting from the profile.
- no-yellow : Remove the yellow setting from the profile.
- no-red : Remove the red setting from the profile.

Note:

The devices using the Broadcom ASIC, the maximum drop probability supports one of [0~10, 25, 50, 75, 100] in hardware.

- If the user configuration value is from 0 to 10, takes the same value as hardware configuration.

- If the user configuration value is from 10 to 24, takes 10 as hardware configuration.
- If the user configuration value is from 25 to 49, takes 25 as hardware configuration.
- If the user configuration value is from 50 to 74, takes 50 as hardware configuration.
- If the user configuration value is from 75 to 99, takes 75 as hardware configuration.
- If user configuration value exceeds 100, takes 100 is used for hardware configuration.

Example
sudo config wred update ecn_profile --mode ecn --gmin 10000 --gmax 20000 --gdrop 50

The following example shows how to remove the yellow setting from an existing profile.

Example
sudo config wred update ecn_profile --no-yellow

config wred del

This command is used to delete a WRED profile.

Usage
config wred del <profile>

Parameters:

<profile_name>: Profile name.

Example
sudo config wred del ecn_profile

config interface wred bind queue

This command is used to configure the WRED thresholds on the specified queue.

Usage
config interface wred bind queue <interface_name> <queue> <profile_name>

Parameters:

<interface_name>: Physical interface name. For example: "Ethernet0".

<queue>: Queue. Minimum: 0. Maximum: 7.

<profile_name>: Profile name.

Example
sudo config interface wred bind queue Ethernet0 0 ecn_profile

config interface wred unbind queue

This command is used to reset the WRED thresholds on the specified queue.

Usage
config interface wred unbind queue <interface_name> <queue>

Parameters:

<interface_name>: Physical interface name. For example: "Ethernet0".

<queue>: Queue. Minimum: 0. Maximum: 7.

Example
sudo config interface wred unbind queue Ethernet0 0

ECN Show Commands

This sub-section contains the ECN show commands that are supported.

show ecn

Note

- this command can be replaced by "show wred" command.

This command displays all the WRED profiles that are configured in the device.

Usage
show ecn

Example: show the existed profile
admin@sonic:~$ show ecn Profile: AZURE_LOSSLESS ---------- ------- red_max_threshold 2097152 red_drop_probability 5 yellow_max_threshold 2097152 ecn ecn_all green_min_threshold 1048576 red_min_threshold 1048576 wred_yellow_enable true yellow_min_threshold 1048576 green_max_threshold 2097152 green_drop_probability 5 wred_green_enable true yellow_drop_probability 5

wred_red_enable true ---------- ------- Profile: wredprofileabcd ---------- --- red_max_threshold 100 ---------- ---

ECN Config Commands

This sub-section contains the configuration commands that can configure the WRED profiles.

config ecn

Note

- this command can be replaced by "config wred add" and "config wred update" commands.

This command configures the possible fields in a particular WRED profile that is specified using the "-profile <profilename>" argument. The list of the WRED profile fields that are configurable is listed below.

Usage(This configuration is only supported on Broadcom switches.)
config ecn -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>] [-v|--verbose]

Parameters:

- profile_name Profile name.
- red_threshold_max Set the red max threshold.
- red_threshold_min Set the red m in threshold.
- yellow_threshold_max Set the yellow max threshold.
- yellow_threshold_min Set the yellow min threshold.
- green_threshold_max Set the green max threshold.

- green_threshold_min Set the green min threshold.

Note

- The command can only be used to configure an existing WRED profile that is bound to a queue. It does not support creating a WRED profile and only limited fields can be configured.

Firstly, create a json file (here named ecn.json as an example) that includes a WRED profile (e.g.,

AZURE_LOSSLESS) and bind it to Ethernet0 queue 3 and Ethernet 4 queue4.

ecn.json

```
"WRED_PROFILE": {
        "AZURE_LOSSLESS": {
        "wred_green_enable": "true",
        "green_min_threshold": "1248",
        "green_max_threshold": "1872",
        "green_drop_probability": "25",
        "wred_yellow_enable": "true",
        "yellow_min_threshold": "1456",
        "yellow_max_threshold": "1872",
        "yellow_drop_probability": "50",
        "wred_red_enable": "true",
        "red_max_threshold": "2097152",
        "red_min_threshold": "2097152",
        "red_drop_probability": "75",
        "ecn": "ecn_all"
        }
},
"QUEUE": {
        "Ethernet0|3": {
                "wred_profile": "[WRED_PROFILE|AZURE_LOSSLESS]"
        },
        "Ethernet4|4": {
                "wred_profile": "[WRED_PROFILE|AZURE_LOSSLESS]"
        }
}
```

And then, use the sonic-cfggen command to load the json file that creates a WRED profile and applies it to queues.

Example
admin@sonic:~$ sudo sonic-cfggen -w -j ecn.json

The following example shows how to set a red max threshold 100 for the profile AZURE_LOSSLESS.

Example: Modify the red max threshold in profile 'AZURE_LOSSLESS'
admin@sonic:~$ sudo config ecn -profile AZURE_LOSSLESS -rmax 100

62 ZTP

Table of Contents

This section explains all the Zero Touch Provisioning (ZTP) commands that are supported in SONiC.

ZTP Show Commands

show ztp status

This command displays the current ZTP configuration of the switch. 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.

Usage
show ztp status show ztp status --verbose

Example
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.

Example

```
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
```

Description:

- ZTP AdminMode - Displays if the ZTP feature is administratively enabled or disabled. Possible values are True or False. This value is configurable using the config z tp enabled and config z tp disable commands.
- 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.
- Inactive: ZTP service is not running.
- 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 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.
    - (04m 12s) Discovering provisioning data

ZTP Configuration Commands

This sub-section explains the list of configuration options available for ZTP.

config ztp enable

Use this command to enable ZTP administrative mode.

Usage
config ztp enable

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

config ztp disable

Use this command to disable ZTP administrative mode. This command can also be used to abort a current ZTP session and load the

factory default switch configuration.

Usage

config ztp disable config ztp disable -y

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

config ztp run

Use this command to manually restart a new ZTP session. This command deletes the existing /etc/sonic/config_db.json file and starts the ZTP service. It also erases the previous ZTP session data. ZTP configuration is loaded on the switch and ZTP discovery is

performed.

Usage
config ztp run config ztp run -y

Example
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

63 Reloading Configuration

config reload

This command stops all services before clearing the configuration and restarts those services. The execution of the config reload takes some time since it restarts many services currently running on the device.

When users do “config reload”, the newly loaded config may or may not have a management IP address. If there is a management IP in the newly loaded config file, it might be different or identical to the previously defined value.

Usage
config reload [-y|--yes] [-l|--load-sysinfo] [<filename>] [-n|--no-service-restart] [-f|--force]

The Parameters are as below:

- " -y" or " –yes" : This forces the loading without prompting the user for confirmation. If the argument is not specified, it prompts the user to confirm whether the user wants to load this configuration file.
- " -n" or " --no-service-restart" : This clears and loads the configuration without restarting dependent services running on the device. One use case for this option is during boot time when the config-setup service loads the existing old configuration and no services are running on the device.
- " -f" or "–force": This option ignores the system sanity checks. By default, a list of sanity checks is performed and if one of the checks fails, the command will not execute. The checks include making sure the system status is not starting, all the essential services are up and swss is in a ready state.
- <filename> : Names of configuration file(s) to load, separated by comma with no spaces in between.

Example
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.

64 Linux Kernel Dump

Table of Contents

Linux Kernel Dump show commands

show kdump config

This command shows the configuration of Linux kernel dump.

Usage
show kdump config

Example
admin@sonic:~$ show kdump config Kdump administrative mode: Enabled Kdump operational mode: Ready after reboot Kdump memory reservation: 0M-2G:256M,2G-4G:320M,4G-8G:384M,8G-:448M Maximum number of Kdump files: 3

Field Description:

- "Kdump administrative mode" show the user configuration.
- "Kdump operational mode" show the current state.
- "Kdump memory reservation" show the reserved memory for the capture kernel.
- "Maximum number of Kdump files" indicate the the maximum files number will be kept in the system.

Note

- When Kdump is enabled through CLI for the fist time, a system reboot should be applied to make kdump take effect.
- From the output of "show kdump config", a hint "Ready after reboot" also show in the field: Kdump operational mode.
- "0M-2G:256M,2G-4G:320M,4G-8G:384M,8G-:448M" is the default value for the memory allocated for the capture kernel.

RAM size	Crash kernel parameter
<= 2GB	256 MB
<= 4GB	320 MB
<= 8GB	384 MB
> 8GB	448 MB

show kdump files

This command shows the Linux kernel core dump files and dmesg files which are generated by kernel dump tool.

Usage
show kdump files

Example

```
admin@sonic:~$ show kdump files
        Kernel core dump files                  Kernel dmesg files
---------------------------------------  ---------------------------------------
/var/crash/202212191136/kdump.202212191136  /var/crash/202212191136/dmesg.202212191136
/var/crash/202212191119/kdump.202212191119  /var/crash/202212191119/dmesg.202212191119
```

show kdump logging<file_name> <num_of_lines>

By default, this command will show the last 10 lines of latest dmesg file. This command can also accept a specific file name and number of lines as arguments.

Usage
show kdump logging

Example: showing the last 10 lines of latest dmesg file

```
admin@sonic:~$ show kdump logging
[  313.984453]  do_syscall_64+0x33/0x80
[  313.988444]  entry_SYSCALL_64_after_hwframe+0x44/0xa9
[  313.994092] RIP: 0033:0x7f82818b58f3
[  313.998089] Code: 8b 15 a1 25 0e 00 f7 d8 64 89 02 48 c7 c0 ff ff ff ff eb b7 0f 1f 00 64 8b 04 25 18 00 00
00 85 c0 75 14 b8 01 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 55 c3 0f 1f 40 00 48 83 ec 28 48 89 54 24 18
[  314.019077] RSP: 002b:00007ffdce0e0278 EFLAGS: 00000246 ORIG_RAX: 0000000000000001
[  314.027545] RAX: ffffffffffffffda RBX: 0000000000000002 RCX: 00007f82818b58f3
[  314.035514] RDX: 0000000000000002 RSI: 0000555e300c52f0 RDI: 0000000000000001
[  314.043491] RBP: 0000555e300c52f0 R08: 000000000000000a R09: 0000000000000001
[  314.051468] R10: 0000555e300b4180 R11: 0000000000000246 R12: 0000000000000002
[  314.059445] R13: 00007f82819996a0 R14: 0000000000000002 R15: 00007f8281994880
```

Example: specifying a file name and number of lines

```
admin@sonic:~$ show kdump logging dmesg.202212191119 -l 20
[  156.711753] Call Trace:
[  156.714498]  dump_stack+0x6b/0x83
[  156.718211]  panic+0x12d/0x303
[  156.721625]  ? printk+0x58/0x6f
[  156.725141]  sysrq_handle_crash+0x16/0x20
```

```
[ 156.729626]  __handle_sysrq.cold+0x43/0x113
[ 156.734304]  write_sysrq_trigger+0x24/0x40
[ 156.738885]  proc_reg_write+0x51/0x90
[ 156.742980]  vfs_write+0xc0/0x260
[ 156.746684]  ksys_write+0x5f/0xe0
[ 156.750395]  do_syscall_64+0x33/0x80
[ 156.754398]  entry_SYSCALL_64_after_hwframe+0x44/0xa9
[ 156.760047] RIP: 0033:0x7fa51a6918f3
[ 156.764045] Code: 8b 15 a1 25 0e 00 f7 d8 64 89 02 48 c7 c0 ff ff ff ff eb b7 0f 1f 00 64 8b 04 25 18 00
00 00 85 c0 75 14 b8 01 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 55 c3 0f 1f 40 00 48 83 ec 28 48 89 54 24 18
[ 156.785044] RSP: 002b:00007ffef637c018 EFLAGS: 00000246 ORIG_RAX: 0000000000000001
[ 156.793514] RAX: ffffffffffffffda RBX: 0000000000000002 RCX: 00007fa51a6918f3
[ 156.801491] RDX: 0000000000000002 RSI: 000055f5684cabb0 RDI: 0000000000000001
[ 156.809467] RBP: 000055f5684cabb0 R08: 000000000000000a R09: 0000000000000001
[ 156.817449] R10: 000055f5683c8a70 R11: 0000000000000246 R12: 0000000000000002
[ 156.825427] R13: 00007fa51a7756a0 R14: 0000000000000002 R15: 00007fa51a770880
```

Linux Kernel Dump config commands

config kdump

Administrative state of kdump is stored in ConfigDB.

The variable USE_KDUMP in the file /etc/default/kdump-tools is set to 0 to disable kdump, and set to 1 to enable kdump.

Since this command might require changing the kernel parameters to specify the amount of memory reserved for the capture kernel (the kernel parameters which are exported through /proc/cmdline), a reboot is necessary.

The command displays a message showing that kdump functionality will be either enabled or disabled following the next reboot.

```
Usage
```

```
admin@sonic:~$ sudo config kdump
Usage: config kdump [OPTIONS] COMMAND [ARGS]...
  Configure the KDUMP mechanism
Options:
  -h, -?, --help  Show this message and exit.
Commands:
  disable    Disable the KDUMP mechanism
  enable     Enable the KDUMP mechanism
  memory     Configure the memory for KDUMP mechanism
  num_dumps  Configure the maximum dump files of KDUMP mechanism.
```

Example

```
admin@sonic:~$ sudo config kdump enable
KDUMP configuration changes may require a reboot to take effect.
Save SONiC configuration using 'config save' before issuing the reboot command.
admin@sonic:~$ sudo config kdump disable
KDUMP configuration changes may require a reboot to take effect.
Save SONiC configuration using 'config save' before issuing the reboot command.
admin@sonic:~$ sudo config kdump num_dumps 2
admin@sonic:~$ sudo config kdump memory 512M
KDUMP configuration changes may require a reboot to take effect.
Save SONiC configuration using 'config save' before issuing the reboot command.
```

65 XSTP

Table of Contents

This section describes MSTP feature and commands which are supported in SONiC.

STP show commands

show spanning-tree

This command displays spanning tree information .

Usage
show spanning-tree

Example
admin@sonic:~$ show spanning-tree show spanning-tree Spanning Tree Information Spanning Tree Mode : RSTP Spanning Tree Enabled/Disabled : Enabled Instance : 0 VLANs Configured : 1-4094 Priority : 32768 Bridge Hello Time (sec.) : 2 Bridge Max. Age (sec.) : 20 Bridge Forward Delay (sec.) : 15 Root Hello Time (sec.) : 2 Root Max. Age (sec.) : 20 Root Forward Delay (sec.) : 15 Max. Hops : 20 Remaining Hops : 20 Designated Root : 32768.04F8F86AFA91 Current Root Port : 0 Current Root Cost : 0 Number of Topology Changes : 0 Last Topology Change Time (sec.): 1415 Transmission Limit : 3

```
Path Cost Method          : Long
---------------------------------------------------------------
Ethernet0 Information
---------------------------------------------------------------
 Admin Status             : Enabled
 Role                     : Designate
 State                    : Forwarding
 Admin Path Cost          : 0
 Oper Path Cost           : 400
 Priority                 : 128
 Designated Cost          : 0
 Designated Port          : 128.1
 Designated Root          : 32768.04F8F86AFA91
 Designated Bridge        : 32768.04F8F86AFA91
 Forward Transitions      : 2
 Admin Edge Port          : Auto
 Oper Edge Port           : Enabled
 Admin Link Type          : Auto
 Oper Link Type           : Point-to-point
 Loopback Detection Status      : Disabled
 Loopback Detection Release Mode  : Auto
 Loopback Detection Action      : Block
 Spanning-Tree Status     : Enabled
 Root Guard Status        : Disabled
 BPDU Guard Status        : Disabled
 BPDU Guard Auto Recovery       : Disabled
 BPDU Guard Auto Recovery Interval : 300
 BPDU Filter Status       : Disabled
 TC Propagate Stop        : Disabled
 ......
```

show spanning-tree brief

This command displays the brief information.

Usage
show spanning-tree brief

Example
admin@sonic:~$ show spanning-tree brief Spanning Tree Mode : RSTP Spanning Tree Enabled/Disabled : Enabled Designated Root : 32768.04F8F86AFA91 Current Root Port : 0 Current Root Cost : 0 Interface Pri Designated Designated Oper STP Role State Oper Bridge ID Port ID Cost Status Edge --------- --- ---------- ---------- -------- ------ ---- ----- ---- Ethernet0 128 32768.04F8F86AFA91 128.1 400 EN DESG FWD Yes Ethernet1 128 32768.04F8F86AFA91 128.2 400 EN DISB BLK No Ethernet2 128 32768.04F8F86AFA91 128.3 400 EN DISB BLK No Ethernet3 128 32768.04F8F86AFA91 128.4 400 EN DISB BLK No Ethernet4 128 32768.04F8F86AFA91 128.5 400 EN DESG FWD Yes .....

show spanning-tree interface

This command displays the information of specified interface.

Usage
show spanning-tree interface <interface_name>

Example
admin@sonic:~$ show spanning-tree interface Ethernet0 Ethernet0 Information ----------

```
Admin Status                  : Enabled
Role                        : Designate
State                       : Forwarding
Admin Path Cost               : 0
Oper Path Cost              : 400
Priority                    : 128
Designated Cost               : 0
Designated Port             : 128.1
Designated Root             : 32768.04F8F86AFA91
Designated Bridge            : 32768.04F8F86AFA91
Forward Transitions           : 2
Admin Edge Port             : Auto
Oper Edge Port              : Enabled
Admin Link Type             : Auto
Oper Link Type              : Point-to-point
Loopback Detection Status       : Disabled
Loopback Detection Release Mode  : Auto
Loopback Detection Action       : Block
Spanning-Tree Status          : Enabled
Root Guard Status           : Disabled
BPDU Guard Status             : Disabled
BPDU Guard Auto Recovery        : Disabled
BPDU Guard Auto Recovery Interval : 300
BPDU Filter Status            : Disabled
TC Propagate Stop             : Disabled
```

show spanning-tree mst instance

This command displays information of the specified MST instance.

Usage
show spanning-tree mst instance <instance_id>

Note: A port becomes a member of the MSTI instance if it is added to a VLAN that is mapped to that MSTI.

Example

```
admin@sonic:~$ show spanning-tree mst instance 1
Spanning Tree Information
--------------------------------------------------------------
 Spanning Tree Mode            : MSTP
 Spanning Tree Enabled/Disabled  : Enabled
 Instance                      : 1
 VLANs Configured              : 10
 Priority                      : 32768
 Bridge Hello Time (sec.)      : 2
 Bridge Max. Age (sec.)        : 20
 Bridge Forward Delay (sec.)   : 15
 Root Hello Time (sec.)        : 2
 Root Max. Age (sec.)          : 20
 Root Forward Delay (sec.)     : 15
 Max. Hops                     : 20
 Remaining Hops                : 20
 Designated Root               : 32768.1.04F8F86AFA91
 Current Root Port             : 0
 Current Root Cost             : 0
 Number of Topology Changes    : 0
 Last Topology Change Time (sec.): 64
 Transmission Limit            : 3
 Path Cost Method              : Long
--------------------------------------------------------------
Ethernet0 Information
--------------------------------------------------------------
 Admin Status                  : Enabled
 Role                          : Designate
 State                         : Forwarding
 External Admin Path Cost      : 0
 Internal Admin Path Cost      : 0
 External Oper Path Cost       : 400
 Internal Oper Path Cost       : 400
 Priority                      : 128
```

```
Designated Cost              : 0
Designated Port              : 128.1
Designated Root              : 32768.1.04F8F86AFA91
Designated Bridge            : 32768.1.04F8F86AFA91
Forward Transitions          : 1
Admin Edge Port              : Auto
Oper Edge Port               : Enabled
Admin Link Type              : Auto
Oper Link Type               : Point-to-point
Loopback Detection Status       : Disabled
Loopback Detection Release Mode  : Auto
Loopback Detection Action       : Block
Spanning-Tree Status         : Enabled
Root Guard Status            : Disabled
BPDU Guard Status            : Disabled
BPDU Guard Auto Recovery        : Disabled
BPDU Guard Auto Recovery Interval : 300
BPDU Filter Status           : Disabled
TC Propagate Stop            : Disabled
......
```

show spanning-tree mst brief

This command displays brief information of the specified MST instance.

Usage
show spanning-tree mst brief <instance_id>

Example
admin@sonic:~$ show spanning-tree mst brief 1 Spanning tree brief for instance 1 Spanning Tree Mode   : MSTP Spanning Tree Enabled/Disabled : Enabled Designated Root   : 32768.01.04F8F86AFA91

```
Current Root Port            : 0
Current Root Cost            : 0
Interface Pri Designated          Designated Oper    STP    Role State Oper
            Bridge ID          Port ID    Cost    Status          Edge
--------- --- -------------------- ---------- -------- ------ ---- ----- ----
Ethernet0 128 32768.01.04F8F86AFA91 128.1         400 EN     DESG FWD   Yes
```

show spanning-tree mst interface

This command displays the information of specified interface on a mst instance.

Usage
show spanning-tree mst interface <instance_id> <interface_name>

Example
admin@sonic:~$ show spanning-tree mst interface 1 Ethernet0 Ethernet0 Information -- Admin Status : Enabled Role : Designate State : Forwarding External Admin Path Cost : 0 Internal Admin Path Cost : 0 External Oper Path Cost : 400 Internal Oper Path Cost : 400 Priority : 128 Designated Cost : 0 Designated Port : 128.1 Designated Root : 32768.1.04F8F86AFA91 Designated Bridge : 32768.1.04F8F86AFA91 Forward Transitions : 1 Admin Edge Port : Auto Oper Edge Port : Enabled Admin Link Type : Auto

```
Oper Link Type                : Point-to-point
Loopback Detection Status     : Disabled
Loopback Detection Release Mode  : Auto
Loopback Detection Action     : Block
Spanning-Tree Status          : Enabled
Root Guard Status             : Disabled
BPDU Guard Status             : Disabled
BPDU Guard Auto Recovery      : Disabled
BPDU Guard Auto Recovery Interval : 300
BPDU Filter Status            : Disabled
TC Propagate Stop             : Disabled
```

show spanning-tree mst configuration

This command displays the configuration of the multiple spanning tree

Usage
show spanning-tree mst configuration

Example

```
admin@sonic:~$ show spanning-tree mst configuration
MSTP Configuration Information
-------------------------------------------------------------
 Configuration Name : 04 F8 F8 6A FA 91
 Revision Level     : 0
 Instance VLANs
-------------------------------------------------------------
    0    1-9,11-4094
    1    10
```

STP configuration commands

config spanning-tree

This command enables/disables the spanning tree mode for the device.

Usage
config spanning-tree enable {mstp | rstp | stp} config spanning-tree disable

option

- mstp: Multiple Spanning Tree (IEEE 802.1s)
- rstp: Rapid Spanning Tree Protocol (IEEE 802.1w)
- stp : Spanning Tree Protocol (IEEE 802.1D). This option uses RSTP set to STP forced compatibility mode. It uses RSTP for the internal state machine, but sends only 802.1D BPDUs.

Note:

- Only one mode can be enabled at any given time. That is, the configuration should be one of (mstp, rstp, stp) during enabling spanning tree.
- When switching the mode, eg stp to mstp, it will stop stp and then start mstp.
- Please exercise caution when switching between spanning tree modes. It is important to note that hanging modes will halt all spanning-tree instances from the previous mode and initiate a system restart in the new mode. This process may result in a temporary disruption of user traffic.
- When disabling spanning tree, spanning mode will be changed to default rstp.

Example
admin@sonic:~$ sudo config spanning-tree enable mstp

config spanning-tree forward_delay

This command allows configuring the forward delay time in seconds (default = 15), range 4-30 seconds.

Note:

2*(forward_delay-1) >= max_age >= 2*(hello_time +1).

The timer is used to control the timing of the various states in the spanning tree process.

Usage
config spanning-tree forward_delay <value>

Example

admin@sonic:~$ sudo config spanning-tree forward_delay 30

config spanning-tree hello

This command allow configuring the hello interval in seconds for transmission of bpdus (default = 2), range 1-10 seconds.

Note:

2*(forward_delay-1) >= max_age >= 2*(hello_time +1).

The timer is used to control the frequency of sending BPDUs in a network.

Usage
config spanning-tree hello <value>

Example
admin@sonic:~$ sudo config spanning-tree hello 10

config spanning-tree max_age

This command allows configuring the maximum time to listen for root bridge in seconds (default = 20), range 6-40 seconds.

Note:

2*(forward_delay-1) >= max_age >= 2*(hello_time +1).

The timer is used to determine the maximum duration during which a bridge can consider a received BPDU as valid.

Usage
config spanning-tree max_age <value>

Example

admin@sonic:~$ sudo config spanning-tree max_age 40

config spanning-tree priority

This command allows configuring the bridge priority in increments of 4096. The default is 32768 and range is 0-61440.

Note:

> The device with the highest priority, indicated by a lower numeric value, becomes the root bridge of the Spanning Tree.

Usage
config spanning-tree priority <value>

Example
admin@sonic:~$ sudo config spanning-tree priority 61440

config spanning-tree mst max_hops

This command allows configuring the maximum number of hops in the region before a BPDU is discarded. The default is 20 and range is 1-40.

Note:

> Each spanning tree instance within a region, including the internal spanning tree (IST) that interconnects these instances, employs a hop count to determine the maximum number of bridges that can forward a BPDU. As the BPDU is propagated, each bridge reduces the hop count by one. Once the hop count reaches zero, the bridge discards the BPDU.

Usage
config spanning-tree mst max_hops <value>

Example
admin@sonic:~$ sudo config spanning-tree mst max_hops 10

config spanning-tree mst name

This command allows configuring the name for the multiple spanning tree region in which this switch is located (default = mac address), max string length is 32.

Note:

The MST region name and revision number are utilized to identify a unique MST region. A bridge, such as this switch, can only be a part of one MST region, and all bridges within the same region must be configured with same MST instances.

Usage
config spanning-tree mst name <string>

Example
admin@sonic:~$ sudo config spanning-tree mst name testlab

config spanning-tree mst revision

This command allows configuring the revision number for this multiple spanning tree configuration of this switch. The default is 0 and range is 0-65535.

Note:

The MST region name and revision number are utilized to identify a unique MST region. A bridge, such as this switch, can only be a part of one MST region, and all bridges within the same region must be configured with same MST instances.

Usage

config spanning-tree mst revision <value>

Example
admin@sonic:~$ sudo config spanning-tree mst revision 1

config spanning-tree mst priority

This command allows configuring the priority of a spanning tree instance in increments of 4096. The default is

32768 and range is 0-61440.

Note:

- The device with the highest priority, indicated by a lower numeric value, becomes the root bridge of the Spanning Tree.
- MST priority is used in selecting the root bridge the specified instance. The device with the highest priority, indicated by a lower numeric value becomes the root bridge of the MSTI instance.

Usage
config spanning-tree mst priority <id> <value>

Example
admin@sonic:~$ sudo config spanning-tree mst priority 1 61440

config spanning-tree mst vlan add/del

This command allows configuring VLANs to a spanning tree instance, range 1-4094.

Note: The maximum number of MST instances allowed is 64.

Usage
config spanning-tree mst vlan {add|del} <id> <value>

Example
admin@sonic:~$ sudo config spanning-tree mst vlan add 1 10 admin@sonic:~$ sudo config spanning-tree mst vlan del 1 10

config spanning-tree interface

This command allows enabling or disabling of STP on an interface, by default STP will be enabled on the interface if global STP mode is configured.

Usage
config spanning-tree interface {enable|disable} <ifname>

Example
admin@sonic:~$ sudo config spanning-tree interface enable Ethernet0

config spanning-tree interface bpdu_filter

This command allow enabling or disabling of bpdu filter on an interface.

Usage
config spanning-tree interface bpdu_filter {enable|disable} <ifname>

Example
admin@sonic:~$ sudo config spanning-tree interface bpdu_filter enable Ethernet0

config spanning-tree interface root_guard

This command allow enabling or disabling of root guard on an interface.

Usage

config spanning-tree interface root_guard {enable|disable} <ifname>

Example
admin@sonic:~$ sudo config spanning-tree interface root_guard enable Ethernet0

config spanning-tree interface bpdu_guard

Below command allows enabling or disabling of bpdu guard on an interface.

Note: To reactivate a port that has been shut down due to a BPDU guard trigger, user can use the "config spanning-tree interface bpdu_guard disable <ifname>" command or specify "auto-recovery " value when enabling bpdu_guard.

Usage
config spanning-tree interface bpdu_guard {enable|disable} <ifname>

By default, BPDU guard will shutdown port, to take an action such as enabling the port after a specified timer has expired, the following command can be used with the auto-recovery option:

Usage
config spanning-tree interface bpdu_guard enable <ifname> [--auto-recovery <value>]

Example
admin@sonic:~$ sudo config spanning-tree interface bpdu_guard enable Ethernet0

config spanning-tree interface edge_port

Below command allows enabling, disabling, or automatically determining whether an interface is an edge port.

Usage
config spanning-tree interface edge_port {enable|disable|auto} <ifname>

Example
admin@sonic:~$ sudo config spanning-tree interface portfast enable Ethernet0

config spanning-tree interface priority

This command allows to configure the port level priority value in increments of 16 (default = 128), range 0-240.

Usage
config spanning-tree interface priority <ifname> <value>

Example
admin@sonic:~$ sudo config spanning-tree interface priority Ethernet0 240

config spanning-tree interface cost

This command allows to configure the port level cost value, range 1-200000000 (default value depend port type and speed).

Note: Default port cost on Ethernet and PortChannel port.

Port Type	Speed	Default Port Cost
Ethernet Port	10M (half-duplex)	2000000
	10M (full-duplex)	1000000
	100M (half-duplex)	200000
	100M (full-duplex)	100000
	1G (half-duplex)	20000
	1G (full-duplex)	10000
	10G (half-duplex)	2000
	10G (full-duplex)	1000

	25G (half-duplex)	800
	25G (full-duplex)	400
	40G (half-duplex)	500
	40G (full-duplex)	250
	100G (half-duplex)	200
	100G (full-duplex)	100
PortChannel Port	10M	500000
	100M	50000
	1G	5000
	10G	500
	25G	400
	40G	125
	100G	50

Usage
config spanning-tree interface cost <ifname> <value>

Example
admin@sonic:~$ sudo config spanning-tree interface cost Ethernet0 1000

config spanning-tree interface mst priority

This command allows to configure the port level priority value on a spanning instance, range 0-240 (default = 128).

Usage
config spanning-tree interface mst priority <ifname> <id> <value>

Example
admin@sonic:~$ sudo config spanning-tree interface mst priority Ethernet0 1 240

config spanning-tree interface mst cost

This command allows to configure the port level cost valueo n a spanning instance , range 1-200000000 (default value depend port type and speed).

Note: Default port cost on Ethernet and PortChannel port.

Port Type	Speed	Default Port Cost
Ethernet Port	10M (half-duplex)	2000000
	10M (full-duplex)	1000000
	100M (half-duplex)	200000
	100M (full-duplex)	100000
	1G (half-duplex)	20000
	1G (full-duplex)	10000
	10G (half-duplex)	2000
	10G (full-duplex)	1000
	25G (half-duplex)	800
	25G (full-duplex)	400
	40G (half-duplex)	500
	40G (full-duplex)	250
	100G (half-duplex)	200
	100G (full-duplex)	100
PortChannel Port	10M	500000

	100M	50000
	1G	5000
	10G	500
	25G	400
	40G	125
	100G	50

Usage
config spanning-tree interface mst cost <ifname> <id> <value>

Example
admin@sonic:~$ sudo config spanning-tree interface mst cost Ethernet0 1 1000

config spanning-tree interface loopback_detection

This command allow enabling or disabling loopback-detection on an interface.

Usage
config spanning-tree interface loopback_detection {enable|disable} <ifname>

Example
admin@sonic:~$ sudo config spanning-tree interface loopback_detection enable Ethernet0

config spanning-tree interface loopback_detection action

This command allow configuring the action of loopback_detection on an interface.

Note:

1. If the action is set to "block", the selected interface, which has been in discarding due to loopback detection, will release

detected loopback state under the following conditions:

- Configure to disable loopback-detection on the port, or
- The port receives any other BPDU excluding its own, or
- The port is link down and link up again, or
- The port stops receiving its own BPDU in a forward delay interval for non-edge port or migration time for auto edge port.

2. If the action is set to "shutdown," the selected interface, which has been shutdown due to loopback detection, will be

automatically reactivated under the following conditions:

- Configure to disable loopback-detection on the port, or
- After the shutdown interval time has expired.

Usage
config spanning-tree interface loopback_detection action {block|shutdown} <ifname> [--shutdown-interval <value>]

Example
admin@sonic:~$ sudo config spanning-tree interface loopback_detection action block Ethernet0 admin@sonic:~$ sudo config spanning-tree interface loopback_detection action shutdown Ethernet0 --shutdown-interval 90

config spanning-tree transmission_limit(next phase)

This command allows configuring the minimum interval between the transmission of consecutive RSTP/MSTP BPDUs. The default is 3 and range is 1-10.

Usage
config spanning-tree transmission_limit <count>

Example

admin@sonic:~$ sudo config transmission-limit 4

config spanning-tree pathcost method (next phase)

This command allows configuring the path cost method used for Rapid Spanning Tree and Multiple Spanning Tree

Usage
config spanning-tree pathcost method {long | short}

Example
admin@sonic:~$ sudo config spanning-tree pathcost method long

config spanning-treeinterface link_type(next phase)

Below command allows configuring the link type for Rapid Spanning Tree and Multiple Spanning Tree

Usage
config spanning-tree interface link-type {auto|point-to-point|shared} <ifname>

Example
admin@sonic:~$ sudo config spanning-tree interface link-type auto Ethernet0

config spanning-tree interface tc_prop_stop (next phase)

This command allows to stop the propagation of topology change notifications (TCN)

Usage
config spanning-tree interface tc-prop-stop {enable|disable} <ifname>

Example

admin@sonic:~$ sudo config spanning-tree interface tc-prop-stop enable Ethernet0

config spanning-tree interface protocol_migration (nextphase)

This command allows to re-check the appropriate BPDU format to send on the selected interface

Usage
config spanning-tree interface protocol_migration <ifname>

Example
admin@sonic:~$ sudo config spanning-tree interface protocol_migration Ethernet0

66 Hardware-Reset

Hardware Reset Commands

hardware-reset

This command is used to reset the devices through the CLI without performing a power cycle. The device gets reset immediately after the command is executed. This command requires root privilege.

Usage
hardware-reset [options]

Parameters

-h,-? : get this help

Example
admin@sonic:~$ sudo hardware-reset

67 Object Track

Table of Contents

Object Track Terminology

Tracked Object

- The object to be tracked in the object track session. It determines the tracked object status of a object traced session.
- If the tracked object meets the specific condition, the downlink interfaces will be shut down. Take the case when trackedobjects are ports or port channels as an example, the downlink interfaces are shut down when the link operation status of the ports or port channels in the tracked object list are all down.
- The first type of the tracked object can be physical ports or port channels such as Ethernet0,PortChannel0001.

- The second type of the tracked object can be BGP neighbors. If all BGP neighbors configured by the command are down, the downlink interfaces are shutdown.
- When both BGP neighbor tracked objects and physical ports/port channels tracked objects exists in the same session, the rule to determine the tracked object status is slightly different from the case that only has one type of tracked objects. The tracked object status is evaluated as up only when at least one BGP neighbor tracked object and one physical port/port channel are up at the same time.

Downlink Interfaces

- The downlink interfaces must to be shut down if all of the tracked objects are down.
- Down link Interfaces must be physical ports or port channels, such as Ethernet0,PortChannel0001.

Object Track Configuration Commands

config obj-track add

This command is used to create an object track session by the session_name.

- Can not create exist obj-track session.
- Add session_name check. Only allow a-z, A-Z, 0-9 and hyphen "-" for session_name. And hyphen can't be the first or the last one.
- The length of session_name must be in the range from 1 to 32 characters.
- User can create 30 sessions at most.

After creation:

- Tracked objects: None
- Downlink Ports: None
- Admin status: Disabled
- GuardTime: 180 seconds

Usage
config obj-track add <session-name>

Parameter:

<session-name>: The name of obj-track session.

Example
admin@sonic:~$ config obj-track add Session1

config obj-track del

This command is used to destroy an obj-track session by the session name.

Can not destroy non-exist obj-track session.

Usage
config obj-track del <session-name>

Parameter:

<session-name>: The name of obj-track session.

Example
admin@sonic:~$ config obj-track del Session1

config obj-track track-obj-type interface add

This command is used to add interfaces to tracked objects in the specified session.

- Can not add the interface that has been added to downlink in the specified session.
- Can not add tracked objects to a non-exist session.
- If all of the tracked interfaces configured by this command are down, the configured downlinks are shut down.

Usage
config obj-track track-obj-type interface add <session-name> <interface_name>

Parameter:

<session-name>: The name of obj-track session.

<interface_name>: The name of physical interface or PortChannel, e.g. "Ethernet0" or "PortChannel0001".

Example
admin@sonic:~$ config obj-track track-obj-type interface add Session1 Ethernet0 admin@sonic:~$ config obj-track track-obj-type interface add Session1 PortChannel0001

config obj-track track-obj-type interface del

This command is used to remove interfaces from the tracked objects in the specified obj-track session.

- Can not remove the interfaces that are not in the tracked objects in the specified session.
- Can not remove tracked objects from a non-exist session.

Usage
config obj-track track-obj-type interface del <session-name> <interface_name>

Parameter:

<session-name>: The name of obj-track session.

<interface_name>: The name of a physical interface or a port channel, e.g. "Ethernet0" or "PortChannel0001".

Example
admin@sonic:~$ config obj-track track-obj-type interface del Session1 Ethernet0 admin@sonic:~$ config obj-track track-obj-type interface del Session1 PortChannel0001

config obj-track track-obj-type bgp-neighbor ip add

This command is used to add BGP neighbors to tracked objects in the specified session.

- Can not add tracked objects to a non-exist session.
- If all of the tracked BGP neighbors configured by this command are down, the configured downlinks are shut down.

Usage
config obj-track track-obj-type bgp-neighbor ip add <session-name> <ip_addr>

Parameter:

<session-name>: The name of obj-track session.

<ip_addr>: The IPv4 address of the specified BGP neighbor.

Example
admin@sonic:~$ config obj-track track-obj-type bgp-neighbor ip add Session1 10.11.12.13

config obj-track track-obj-type bgp-neighbor ip del

This command is used to remove BGP neighbors from the tracked objects in the specified obj-track session.

- Can not remove the BGP neighbors that are not in the tracked objects in the specified session.
- Can not remove tracked objects from a non-exist session.

Usage
config obj-track track-obj-type bgp-neighbor ip del <session-name> <ip_addr>

Parameter:

<session-name>: The name of obj-track session.

<ip_addr>: The IPv4 address of the specified BGP neighbor.

Example
admin@sonic:~$ config obj-track track-obj-type bgp-neighbor ip del Session1 10.11.12.13

config obj-track track-obj-type bgp-neighbor ipv6add

This command is used to add BGP neighbors to tracked objects in the specified session.

- Can not add tracked objects to a non-exist session.
- If all of the tracked BGP neighbors configured by this command are down, the configured downlinks are shut down.

Usage
config obj-track track-obj-type bgp-neighbor ipv6 add <session-name> <ipv6_addr>

Parameter:

<session-name>: The name of obj-track session.

<ipv6_addr>: The IPv6 address of the specified BGP neighbor.

Example
admin@sonic:~$ config obj-track track-obj-type bgp-neighbor ipv6 add Session1 fc00:1::32

config obj-track track-obj-type bgp-neighbor ipv6 del

This command is used to remove BGP neighbors from the tracked objects in the specified obj-track session.

- Can not remove the BGP neighbors that are not in the tracked objects in the specified session.
- Can not remove tracked objects from a non-exist session.

Usage

config obj-track track-obj-type bgp-neighbor ipv6 del <session-name> <ipv6_addr>

Parameter:

<session-name>: The name of obj-track session.

<ipv6_addr>: The IPv6 address of the specified BGP neighbor.

Example
admin@sonic:~$ config obj-track track-obj-type bgp-neighbor ipv6 del Session1 fc00:1::32

config obj-track track-obj-type bgp-neighbor interface add

This command is used to add BGP-unnumbered neighbors to tracked objects in the specified session.

- Can not add the interface of the BGP-unnumbered neighbor that has been added to downlink in the specified session.
- Can not add tracked objects to a non-exist session.
- If all of the tracked BGP neighbors configured by this command are down, the configured downlinks are shut down.

Usage
config obj-track track-obj-type bgp-neighbor interface add <session-name> <interface_name>

Parameter:

<session-name>: The name of obj-track session.

<interface_name>: The name of physical interface or PortChannel, e.g. "Ethernet0" or "PortChannel0001", which is associated with the BGP-unnumbered neighbor.

Example
admin@sonic:~$ config obj-track track-obj-type bgp-neighbor interface add Session1 Ethernet1 admin@sonic:~$ config obj-track track-obj-type bgp-neighbor interface add Session1 PortChannel0002

config obj-track track-obj-type bgp-neighbor interface del

This command is used to remove BGP-unnumbered neighbors from the tracked objects in the specified obj-track session.

- Can not remove the BGP neighbors that are not in the tracked objects in the specified session.

- Can not remove BGP neighbors from a non-exist session.

Usage
config obj-track track-obj-type bgp-neighbor interface del <session-name> <interface_name>

Parameter:

<session-name>: The name of obj-track session.

<interface_name>: The name of physical interface or PortChannel, e.g. "Ethernet0" or "PortChannel0001", which is associated with the BGP-unnumbered neighbor.

Example
admin@sonic:~$ config obj-track track-obj-type bgp-neighbor interface del Session1 Ethernet1 admin@sonic:~$ config obj-track track-obj-type bgp-neighbor interface del Session1 PortChannel0002

config obj-track downlink interface add

This command is used to add interfaces to downlink to the specified obj-track session.

- Can not add the interface that has been added to the object tracked list in the specified session. Note that it includes the interface of the tracked object which is associated with BGP-unnumbered neighbors
- Can not add downlink interfaces to a non-exist session.
- If the tracked object status is evaluated as down, the downlink interfaces configured by the command are shut down.

Usage
config obj-track downlink interface add <session-name> <interface_name>

Parameter:

<session-name>: The name of obj-track session.

<interface_name>: The name of physical interface or PortChannel, e.g. "Ethernet0" or "PortChannel0001".

Example
admin@sonic:~$ config obj-track downlink interface add Session1 Ethernet1 admin@sonic:~$ config obj-track downlink interface add Session1 PortChannel0002

config obj-track downlink interface del

This command is used to remove the interfaces from the downlink interfaces in the specified obj-track session.

- Can not remove the interfaces that have not been added to the downlink interfaces in the specified session.
- Can not remove down links from a non-exist session.

Usage
config obj-track downlink interface del <session-name> <interface_name>

Parameter:

<session-name>: The name of obj-track session.

<interface_name>: The name of a physical interface or a port channel, e.g. "Ethernet0" or "PortChannel0001".

Example
admin@sonic:~$ config obj-track downlink interface del Session1 Ethernet1 admin@sonic:~$ config obj-track downlink interface del Session1 PortChannel0002

config obj-track admin

This command is used to enable/disable a obj-track session by the session_name.

- Can not set on non-exist obj-track session.

Usage
config obj-track admin <session-name> <admin-status>

Parameter:

<session-name>: The name of a obj-track session.

<admin-status>: The valid settings are enabled and disabled.

Example
admin@sonic:~$ config obj-track admin Session1 enabled admin@sonic:~$ config obj-track admin Session1 disabled

config obj-track guard-time

This command is used to configure the recover guard time by session_name.

- Can not set on non-exist obj-track session.
- The guard time should be in the range between 0 ~ 300 seconds.
- Guard time only takes effect when physical ports/port channels tracked objects exist in the same session. In other words, guard time will not take effect when only BGP neighbor tracked objects exist in the same session.

Usage
config obj-track guard-time <session-name> <guard_time>

Parameter:

<session-name>: The name of obj-track session

<guard-time>: The guard time in seconds(0~300 seconds, 60 seconds by default)

Example
admin@sonic:~$ config obj-track guard-time Session1 60

Object Track Show Commands

show obj-track

This command is used to show the obj-track session information.

Usage
show obj-track <session-name>

Parameter:

<session-name>: The name of obj-track session

Example
admin@sonic:~$ show obj-track Obj-Track Session Information: Name: Session1 Admin Status: enabled Track-obj-type: Interfaces: Ethernet0(up), PortChannel0001(down)

```
BGP nbrs: 10.11.12.13 (up), fc00:1::32(up)
BGP-unnumbered nbrs: Ethernet2(up), PortChannel0003(down)
Downlink:
Interfaces: Ethernet1(up), PortChannel0002(up)
GuardTime: 180 seconds
Operation Status:
Tracked Status: up
Oper Status: up
Obj-Track Session Information:
Name: Session2
Admin Status: enabled
Track-obj-type:
Interfaces: Ethernet2(down), PortChannel0003(down)
BGP nbrs: 10.11.12.13 (up), fc00:1::32(up)
BGP-unnumbered nbrs: Ethernet3(up), PortChannel0004(up)
Downlink:
Interfaces: Ethernet1(down), PortChannel0002(down)
GuardTime: 180 seconds
Operation Status:
Tracked Status: down
Oper Status: shutdown
```

Object Track Guidelines

Object Track uses the information from the tracked objects to determine the link status of the downlinks. If the condition from the tracked objects to shut down is matched, all the downlink interfaces are shut down. Otherwise, all the downlink interfaces are restored after the guard time expires.

General Use Case

1. The user must create an object track session first.
2. After the session is created, the user must add tracked objects and downlinks to that session.
3. Note that users must not add downlinks to tracked objects to prevent from recursive dependencies.
4. Then enable the object track session to monitor the tracked objects.

5. When the tracked objects meet the expected condition, all the downlinks are shut down. Otherwise, all the downlinks are restored after the guard time.

Port Track Use Case

1. The user must create an object track session that add port or port channels as tracked objects first
2. After the session is created, the user must add ports or port channels to the tracked object list and downlink interfaces to that session.
3. Note that users must not add downlink interfaces to the tracked object list to prevent from recursive dependencies.
4. Then enable the port track session to monitor the tracked interfaces.
5. When the interfaces in the object tracked list are all down, all the downlink interfaces are shut down. Otherwise, all the downlink interfaces are restored after the guard time.

Port Track Use Example

Create an object track session named as "PortTrack".

Example
admin@sonic:~$ config obj-track add PortTrack

Add tracked interfaces and downlinks.

Example
admin@sonic:~$ config obj-track track-obj-type interface add PortTrack Ethernet0 admin@sonic:~$ config obj-track track-obj-type interface add PortTrack PortChannel0001 admin@sonic:~$ config obj-track downlink interface add PortTrack Ethernet1 admin@sonic:~$ config obj-track downlink interface add PortTrack PortChannel0002

Enable the object track session "PortTrack".

Example
admin@sonic:~$ config obj-track admin PortTrack enabled

When Ethernet0 and PortChannel0001 are all down, the interfaces named as Ethernet1 and PortChannel0002 will be shut down.

When Ethernet0 or PortChannel0001 is up, the downlinks, Ethernet1 and PortChannel0002 will be restored after the guard time.

BGP Neighbor Track Use Case

1. The user must create an object track session that add BGP neighbors as tracked objects first.

2. After the session is created, the user must add BGP neighbors to the tracked object list and downlink interfaces to that session.

3. Note that users must not add downlink interfaces to the tracked object list to prevent from recursive dependencies.

4. Then enable the session to monitor the tracked BGP neighbors.

5. When the BGP neighbors in the object tracked list are all down, all the downlink interfaces are shut down. Otherwise, all the downlink interfaces are immediately restored. Note that the guard time configuration does not take effect when only BGP neighbor tracked objects exist.

Port Track and BGP Neighbor Track Use Case

1. The user must create an object track session first.

2. After the session is created, the user must add BGP neighbors, ports, or port channels to the tracked object list and downlink interfaces to that session.

3. Note that users must not add downlink interfaces to the tracked object list to prevent from recursive dependencies.

4. Then enable the session to monitor the tracked BGP neighbors.

5. When all the BGP neighbors in the object tracked list are down, or when all the interfaces in the object tracked list are down, all the downlink interfaces are shut down.

6. When at least one BGP neighbor in the tracked list is up and at least one interface in the tracked list is up, all the downlink interfaces are restored after the guard time.

Advanced Use Case

There are 2 group of ports. Port 1 ~ Port 2 are in the group 1. PortChannel1 ~ PortChannel2 are in the group 2.

The downlinks are Port3, PortChannel3.

Users want to shut down downlinks if group 1 or group 2 are down.

1. Create 2 object track sessions, session_1 and session_2.
2. Add group 1 ports to tracked objects to session_1.
3. Add downlinks to session_1.
4. Add group 2 ports to tracked objects to session_2.
5. Add downlinks to session_2.
6. Enable session_1 and session_2.

Users want to shut down downlinks if group 1 and group 2 are down.

Create 1 object track session, session_1.

1. Add group 1 ports to tracked objects session_1.
2. Add group 2 ports to tracked objects session_1.
3. Add downlinks to session_1.
4. Enable session_1.

Port-Channel

If the downlink port is a port-channel, there is something different on the way to shutdown a port-channel when it is shut down by object track and by admin-down command.

- shutdown port-channel by admin-down command(the command is executed by a user):
  - Only set admin-down to port-channel(shutdown at layer 3).
  - The tx/rx of member ports shall be disabled.
  - The physical link status may be up or down.
- shutdown port-channel by obj-track:
  - Set admin-down to port-channel.
  - The admin status of member ports shall be set to disabled.
  - The physical link status shall be down.

Caveat

Given a topology shown below.

Sonic Switch -------(Ethernet0)---------(BGP neighbor).

Configuration:

- The user tracks only one BGP unnumbered neighbor which is established via Ethernet0 by an object-track session. · The user adds Ethernet0 as the downlink interface in the same session. CLI will not forbid this operation.
- When the session is activated when BGP neighbor status is up, the tracked object status is evaluated as up. However, as long as the tracked BGP neighbor status is changed to down, the downlink interface Ethernet0 will be shut down. Ethernet0 will never be up so the BGP neighbor will never be present. Ethernet0 can only be up again until the session is disabled.

This is not a reasonable use case.

68 Port Protocol Down

Table of Contents

Port Protocol Down Show Commands

show protocol-down brief

This command is used to show protocol down brief information for each port.

Usage
show protocol-down brief [port]

Parameter:

port is the name of the interface like: Ethernet0, Ethernet1

The brief status of all ports will be displayed when 'port' is not specified.

Example output of "show protocol-down brief"
admin@sonic:~$ show protocol-down brief Interface ProtoDown Admin Effective Admin --------- --------- --------- ---------------- Ethernet0 False Up Up Ethernet4 True Down Down Ethernet8 True Up Down ...

Only the brief status of the specified port will be displayed when 'port' is specified.

Example output of "show protocol-down brief Ethernet0"
admin@sonic:~$ show protocol-down brief Ethernet0 Interface ProtoDown Admin Effective Admin --------- --------- --------- ----------

Ethernet0	False	Up	Up

show protocol-down status

This command is used to show protocol down status.

Usage
show protocol-down status [port]

Parameter:

port is the name of the interface like: Ethernet0, Ethernet1

The protocol down status of all ports will be displayed when 'port' is not specified.

Example output of "show protocol-down status"

```
admin@sonic:~$ show protocol-down status
Interface         EVPN       OBJTRK      PMS     STP  ProtoDown     Admin    Effective Admin
---------     ----------     --------    ------   ------  ---------  ---------   ----------------
Ethernet0         False       False      False    False      False        Up             Up
Ethernet4          True        True      False    False       True      Down           Down
Ethernet8          True       False      False    False       True        Up           Down
...
PortChannel101     False       False      False    True       True      Down           Down
```

Only the protocol down status of the specified port will be displayed when 'port' is specified.

Example output of "show protocol-down status Ethernet0"

```
admin@sonic:~$ show protocol-down status Ethernet0
Interface       EVPN       OBJTRK      PMS     STP    ProtoDown     Admin    Effective Admin
---------     --------     --------    ------   ------   ----------   --------   ----------------
Ethernet0       False       False      False    False       False        Up             Up
```

Interface Show Command

show interfaces status

This command is used to show interface status.

Usage
show interfaces status [port]

Parameter:

port is the name of the interface like: Ethernet0, Ethernet1

The interface status of all ports will be displayed when 'port' is not specified. Note that the fields "Porto Down" and "Eff Admin" are new added fields by this new design.

Example output of "show interfaces status"

```
admin@sonic:~$ show interfaces status
  Interface          Lanes      Speed    MTU    Oper FEC          Alias             Vlan      Oper
Admin    Proto Down   Eff Admin    Type    Asym PFC
-------------  ---------------  -------  -----  ----------  -------------  -----------  ------
-------  -----------  ---------  ------  ----------
Ethernet0        49,50,51,52     100G   9100       rs      Eth1(Port1)          trunk
down       up         True       down     N/A        off
Ethernet4        53,54,55,56     100G   9100       rs      Eth2(Port2)          trunk
up         up         False      up       N/A        off
...
Ethernet100    129,130,131,132     100G   9100       rs      Eth29(Port29)    PortChannel101
up         up         False      up       N/A        off
```

Only the interface status of the specified port will be displayed when 'port' is specified.

Example output of "show interfaces status Ethernet0"
admin@sonic:~$ show interfaces status Ethernet0 Interface Lanes Speed MTU Oper FEC Alias Vlan Oper Admin Proto Down Eff Admin Type Asym PFC ---------- ---------- ------- ----- ---------- ---------- ------ ------- ------- ---------- ---------- ------- ---------- Ethernet0 49,50,51,52 100G 9100 N/A Eth1(Port1) trunk down up True down N/A off

Port Protocol Down Guidelines

Protocol down is a state for each port. For the feature that has the functionality to shutdown a port under some certain conditions, the feature needs to set the protocol down state of its own feature. So each feature is responsible to maintain the protocol down state of its own feature on each port. The effective admin state of a port will be determined by the state of the protocol down and the admin state. In usual, the effective admin state is the same as admin state. The port protocol commands can be used to find outthe cause when the effective admin state is down.

Port Protocol Down Use Example

The effective admin state of a port might be changed by protocol down reasons managed by process/program. The following example demonstrates the procedures to configure object track settings and the effect on the protocol down status.

Setup an Object Track Session

Example commands to setup object track
admin@sonic:~$ config obj-track add PortTrack (1)

```
admin@sonic:~$ config obj-track track-obj-type interface add PortTrack Ethernet0 (2)
admin@sonic:~$ config obj-track downlink interface add PortTrack Ethernet4 (3)
admin@sonic:~$ config obj-track admin PortTrack enabled (4)
```

The description for above commands:

(1) Create a object tracked session named "PortTrack".

(2) Add a tracked object "Ethernet0", which is a port interface, into the session "PortTrack".

(3) Add a downlink interface "Ethernet4" into the session "PortTrack".

(4) Enable the object tracked session "PortTrack".

With the object-tracked settings shown above, the protocol down reason of the object track on Ethernet0 will be "True" when the port link operational status of Ethernet4 is down. The protocol down reason of the object track on Ethernet0 will be "False" when the portlink operational status of Ethernet4 is up.

Given that the Port Link Operation Status of Ethernet4 is Down

Here is the excerpted output of "show interface status". Note that the "Proto Down" of Ethernet0 is "True". The "Eff Admin"(Effective Admin) state is down, which is a resolved result according to "Admin" and Proto Down".

Example output of "show interfaces status"

```
admin@sonic:~$ show interfaces status
Interface         Lanes    Speed    MTU    Oper FEC       Alias    Vlan     Oper    Admin    Proto
Down    Eff Admin     Type    Asym PFC
-------------  -----------  -------  -----  ----------  ------------  ------  -------  ------
-----------  ---------  ------  ----------
Ethernet0     49,50,51,52    100G   9100       N/A   Eth1(Port1)   trunk     down     up
True       down      N/A       off
Ethernet4     53,54,55,56    100G   9100       N/A   Eth2(Port2)   trunk       up     up
False        up      N/A       off
```

```
...
```

Here is the output of "show protocol-down brief Ethernet0".

Example output of "show protocol-down brief Ethernet0"

```
admin@sonic:~$ show protocol-down brief Ethernet0
Interface    ProtoDown    Admin    Effective Admin
---------    --------- ---------    ---------------
Ethernet0        True       Up           Down
```

Here is the output of "show protocol-down status Ethernet0". Note that the "OBJTRK" field is true, which means the protocol down is set as True due to "OBJTRK" is true.

Example output of "show protocol-down status Ethernet0"

```
admin@sonic:~$ show protocol-down status Ethernet0
Interface       EVPN       OBJTRK     PMS     LAG    ProtoDown     Admin    Effective Admin
---------     -------     --------  -----  ------    ---------     ------    ---------------
Ethernet0       False       True    False    False       True        Up           Down
```

Given that the Port Link Operation Status of Ethernet4 is Changed from Down to Up

Here is the excerpted output of "show interface status". Note that the "Proto Down" of Ethernet0 is changed to "False". The "EffAdmin"(Effective Admin) state is changed to up. The port link operation status of Ethernet0 is also changed to up.

Example output of "show interfaces status"

```
admin@sonic:~$ show interfaces status
Interface          Lanes    Speed    MTU    Oper FEC        Alias    Vlan    Oper    Admin    Proto
Down    Eff Admin     Type    Asym PFC
-------------  -----------  -------  -----  ----------  -------------  ------  ------  -------
-----------  ---------  ------  ----------
Ethernet0      49,50,51,52    100G   9100       N/A    Eth1(Port1)   trunk      up      up
False          up      N/A       off
Ethernet4      53,54,55,56    100G   9100       N/A    Eth2(Port2)   trunk      up      up
False          up      N/A       off
...
```

Here is the output of "show protocol-down brief Ethernet0".

Example output of "show protocol-down brief Ethernet0"

```
admin@sonic:~$ show protocol-down brief Ethernet0
Interface    ProtoDown    Admin    Effective Admin
---------    ---------- ---------    ---------------
Ethernet0       False       Up              Up
```

Here is the output of "show protocol-down status Ethernet0". Note that the "OBJTRK" field is changed to false, which means the protocol down is set as false because EVPN, OBJTRK and PMS's protocol down statuses are false.

Example output of showprotocol-downstatusEthernet0

```
admin@sonic:~$ show protocol-down status Ethernet0
Interface       EVPN       OBJTRK      PMS      LAG    ProtoDown      Admin    Effective Admin
---------     -------     --------   ------   -------   ---------    --------    ---------------
Ethernet0       False       False    False     False       True         Up              Up
```

69 DHCP Snooping

Table of Contents

These commands are used to add or remove DHCP Snooping configuration.

DHCP Snooping show commands

show dhcp-snoop

This command is used to display dhcp snooping configuration

Usage
show dhcp-snoop

Example
admin@sonic:~# show dhcp-snoop DHCP Snooping Information IPv4 IPv6 ------- ------ disable N/A

show dhcp-snoop vlan

This command is used to display vlan for dhcp snooping

Usage
show dhcp-snoop vlan

Example
admin@sonic:~# show dhcp-snoop vlan Vlan Interface Name Status Vlan100 enable

show dhcp-snoop trust

This command is used to display trusted port for dhcp snooping

Usage
show dhcp-snoop trust

Example
admin@sonic:~# show dhcp-snoop trust Interface Name Status Ethernet0 enable

show dhcp-snoop bind

This command is used to display binding table for dhcp snooping

Usage
show dhcp-snoop bind

Example
admin@sonic:~# show dhcp-snoop bind Mac address IP address Interface Name Vlan Interface Name Lease Time Remain Time ---------- ---------- ---------- ---------- ---------- ---------- 00:11:22:33:44:55 10.10.100.1 Ethernet0 Vlan100 86400 86010

DHCP Snooping config commands

config dhcp snoop feature enable/disable

This command is used to enable/disable dhcp snooping feature

Usage
config feature state dhcp_snoop <enabled|disabled>

Example
admin@sonic:~# sudo config feature state dhcp_snoop enabled admin@sonic:~# sudo config feature state dhcp_snoop disabled

config dhcp snoop ipv4 enable/disable

This command is used to enable/disable ipv4 for DHCP snooping

Usage
config dhcp-snoop ipv4 <enabled|disabled>

Example
admin@sonic:~# sudo config dhcp-snoop ipv4 enable admin@sonic:~# sudo config dhcp-snoop ipv4 disable

config dhcp snoop trust vlan enable/disable

This command is used to enable/disable vlan for DHCP snooping

Usage
config dhcp-snoop vlan <enable|disable> <vlan-id>

Parameters:

vlan-id: Specifies the v lan id to enable/disable dhcp snooping

Example
admin@sonic:~# sudo config dhcp-snoop vlan enable 100 admin@sonic:~# sudo config dhcp-snoop vlan disable 100

config dhcp snoop trust port add/del

This command is used to add/del trust port for DHCP snooping

Usage
config dhcp-snoop trusted <add|del> <port-name>

Parameters:

port-name: Specifies Ethernet or PortChannel to add/del as trust port for dhcp snooping

Example
admin@sonic:~# sudo config dhcp-snoop trusted add Ethernet0 admin@sonic:~# sudo config dhcp-snoop trusted del Ethernet0 admin@sonic:~# sudo config dhcp-snoop trusted add PortChannel1 admin@sonic:~# sudo config dhcp-snoop trusted del PortChannel1

70 IGMP Snooping

Table of Contents

IGMP Snooping Configuration Commands

This sub-section of commands is used to configure IGMP Snooping.

config igmp snooping

This command is used to enable/disable IGMP Snooping.

Usage
config igmp snooping (enable|disable)

Example
admin@sonic:~$ sudo config igmp snooping enable admin@sonic:~$ sudo config igmp snooping disable

config igmp snooping mrouter-port-expire-time

This command is used to set the mrouter port expire time.

Usage
config igmp snooping mrouter-port-expire-time <1-65535>

Example
admin@sonic:~$ sudo config igmp snooping mrouter-port-expire-time 300

The expire time is in seconds. The default value is 300 seconds.

config igmp snooping mrouter-port-forward-mode

This command is used to set the multicast forward mode for the mrouter port. If the mode is set to 'dynamic', the IP multicast stream won’t be forwarded to mrouter ports unless this mrouter port has group joined. If the mode is set to 'forward', all the IP multicast stream will be forwarded to mrouter ports. By default, the mode is set to 'forward'.

Usage
config igmp snooping mrouter-port-forward-mode (dynamic|forward)

Example
admin@sonic:~$ sudo config igmp snooping mrouter-port-forward-mode dynamic

The default value is 'forward'.

config igmp snooping querier

This command is used to enable or disable the Querier function.

Usage
config igmp snooping querier (enabled|disabled)

Example
admin@sonic:~$ sudo config igmp snooping querier enabled admin@sonic:~$ sudo config igmp snooping querier disabled

config igmp snooping version

This command is used to set the IGMP version.

Usage
config igmp snooping version <1-3>

Example
admin@sonic:~$ sudo config igmp snooping version 2

The default value is 2.

config igmp snooping vlan

This command is used to enable/disable IGMP Snooping on a VLAN.

Usage
config igmp snooping vlan (enable|disable) <vid>

Example
admin@sonic:~$ sudo config igmp snooping vlan enable 100 admin@sonic:~$ sudo config igmp snooping vlan disable 100

The default value is 'enable'.

config igmp snooping vlan immediate-leave

This command is used to enable or disable the Immediate Leave function on a VLAN.

Usage
config igmp snooping vlan immediate-leave (enabled|disabled) <vid>

Example
admin@sonic:~$ sudo config igmp snooping vlan immediate-leave enabled 100 admin@sonic:~$ sudo config igmp snooping vlan immediate-leave disabled 100

The default value is 'disable'.

config igmp snooping vlan last-member-query-count

This command is used to set the Last Member Query Count for a VLAN.

Usage
config igmp snooping vlan last-member-query-count <vid> <count>

Example
admin@sonic:~$ sudo config igmp snooping vlan last-member-query-count 100 2

The default value is 2.

config igmp snooping vlan last-member-query-interval

This command is used to set the Last Member Query Interval for a VLAN.

Usage
config igmp snooping vlan last-member-query-interval <vid> <interval>

The interval is in seconds. The default value is 1 second.

Example
admin@sonic:~$ sudo config igmp snooping vlan last-member-query-interval 100 1

The default value is 1 second.

config igmp snooping vlan mrouter-port

This command is used to set the IGMP Snooping Multicast Router Port for a VLAN.

Usage
config igmp snooping vlan mrouter-port (add|remove) <vid> <port>

Example
admin@sonic:~$ sudo config igmp snooping vlan mrouter-port add 100 Ethernet0 admin@sonic:~$ sudo config igmp snooping vlan mrouter-port remove 100 Ethernet0

config igmp snooping vlan query-interval

This command is used to set the IGMP Query Interval for a VLAN. The Query Interval should be greater than the Query Response Interval.

Usage
config igmp snooping vlan query-interval <vid> <interval>

Example
admin@sonic:~$ sudo config igmp snooping vlan query-interval 100 10

Please note loaded setting will be lost after system reboot. To preserve setting, run `config save`.

config igmp snooping vlan query-response-interval

This command is used to set the IGMP Query Response Interval for a VLAN.

Usage
config igmp snooping vlan query-response-interval <vid> <interval>

The interval is in seconds. The default value is 10 seconds.

Example
admin@sonic:~$ sudo config igmp snooping vlan query-response-interval 100 10

config igmp snooping vlan static-group

This command is used to add or remove a static group for a VLAN.

Usage
config igmp snooping vlan static-group (add|remove) <vid> <ip_addr> <port>

Example
admin@sonic:~$ sudo config igmp snooping vlan static-group add 100 224.1.1.1 Ethernet0 admin@sonic:~$ sudo config igmp snooping vlan static-group remove 100 224.1.1.1 Ethernet0

config igmp snooping vlan version

This command is used to set the IGMP version for a VLAN.

Usage

config igmp snooping vlan version <vid> <1-3>

Example
admin@sonic:~$ sudo config igmp snooping vlan version 100 2

The default value is 2.

sonic-clear igmp snooping dynamic groups

This command is used to clear the dynamic groups.

Usage
sonic-clear igmp snooping dynamic groups

Example
admin@sonic:~$ sudo sonic-clear igmp snooping dynamic groups

sonic-clear igmp snooping statistics

This command is used to clear the statistics of IGMP Snooping packets.

Usage
sonic-clear igmp snooping statistics <interface_name>

Example
admin@sonic:~$ sudo sonic-clear igmp snooping statistics Ethernet0

IGMP Snooping Show Commands

This sub-section lists all the possible show commands for the IGMP Snooping available in the device. Following example gives the list of possible shows on IGMP Snooping. Subsequent pages explain each of these commands in detail.

Example

```
admin@sonic:~$ show igmp snooping -?
Show IGMP Snooping information
Options:
  -?, -h, --help  Show this message and exit.
Commands:
  groups      Show IGMP Snooping groups information
  mrouter     Show IGMP Snooping mrouter information
  querier     Show IGMP Snooping querier information
  statistics  Show IGMP Snooping statistics
  vlan        Show IGMP Snooping vlan information
```

show igmp snooping

This command is used to display IGMP Snooping information.

Usage

```
show igmp snooping
```

Example

```
admin@sonic:~$ show igmp snooping
 IGMP Snooping                 : Disabled
 Router Port Expire Time       : 300 s
 Router Port Mode              : Forward
 Version                       : 2
 Querier                       : Enabled
 VLAN 1:
 -------
```

```
IGMP Snooping                  : Disabled
IGMP Snooping Running Status   : Inactive
Version                        : Using global Version (2)
Immediate Leave                : Disabled
Last Member Query Interval     : 10 (unit: 1/10s)
Last Member Query Count        : 2
Query Interval                 : 125
Query Response Interval        : 100 (unit: 1/10s)
VLAN Static Group    Port
---- --------------- -----------
1    225.1.1.1       Ethernet  6
```

show igmp snooping groups

This command is used to display IGMP Snooping Groups information.

Usage
show igmp snooping groups [vid]

Example

```
admin@sonic:~$ show igmp snooping groups
Bridge Multicast Forwarding Entry Count:1
Flag: R - Router port, M - Group member port
      H - Host counts (number of hosts joined to group on this port).
      P - Port counts (number of forwarding ports).
 Uptime: Group elapsed time; Expire: Group remain time.
VLAN Group         Source         Port         Up time     Expire Count
---- ---------------- ---------------- ------------- ----------- ------ --------
  1 224.1.1.1      *                    00:00:00:03          1(P)
                        Ethernet 1(M)                    0(H)
                        Ethernet 2(M) 00:00:00:03 00:03      3(H)
                        Ethernet 1(R)
  2 224.1.1.2      *                    00:03                1(P)
                        Ethernet 1(R)
```

```
admin@sonic:~$ show igmp snooping groups 1
Bridge Multicast Forwarding Entry Count:1
Flag: R - Router port, M - Group member port
    H - Host counts (number of hosts joined to group on this port).
    P - Port counts (number of forwarding ports).
 Uptime: Group elapsed time; Expire: Group remain time.
VLAN Group         Source         Port         Up time     Expire Count
---- --------------- --------------- ------------ ----------- ------ --------
  1 224.1.1.1      *                          00:00:00:03          1(P)
                        Ethernet 1(M)                     0(H)
                        Ethernet 2(M) 00:00:00:03 00:03      3(H)
                        Ethernet 1(R)
```

show igmp snooping mrouter

This command is used to display IGMP Snooping Multicast Router Port information.

Usage
show igmp snooping mrouter [vid]

Example
admin@sonic:~$ show igmp snooping mrouter VLAN M'cast Router Port Type Expire ---- ------------------ ------- -------- 1 Ethernet 1 Static 2 Ethernet 2 Dynamic 00:00:03 admin@sonic:~$ show igmp snooping mrouter 1 VLAN M'cast Router Port Type Expire ---- ------------------ ------- -------- 1 Ethernet 1 Static ````

show igmp snooping querier status

This command is used to display IGMP Snooping Querier status information.

Usage
show igmp snooping querier status

Example
admin@sonic:~$ show igmp snooping querier status VLAN 1 Other Querier : None Other Querier Expire : 0(m):0(s) Other Querier Uptime : 0(h):0(m):0(s) Self Querier : None Self Querier Expire : 0(m):0(s) Self Querier Uptime : 0(h):0(m):0(s) General Query Received : 0 General Query Sent : 0 Specific Query Received : 0 Specific Query Sent : 0

show igmp snooping statistics

This command is used to display IGMP Snooping Statistics information. The statistics only count the packet that is handled by the IGMP Snooping supported interfaces.

Usage
show igmp snooping statistics (input|output) <interface name>

Example
admin@sonic:~$ show igmp snooping statistics input Input Statistics: Interface Report Leave G Query G(-S)-S Query Drop Join Succ Group

```
---------- -------- -------- -------- ------------ -------- --------- ------
Ethernet 1 0       0       0       0           0       0       0
VLAN     1 0       0       0       0           0       0       0
admin@sonic:~$ show igmp snooping statistics output
Output Statistics:
Interface   Report   Leave    G Query  G(-S)-S Query Drop     Group
----------- -------- -------- -------- ------------ -------- ------
Ethernet 1  0       0       0       0           0       0
Ethernet 2  0       0       0       0           0       0
```

show igmp snooping vlan

This command is used to display IGMP Snooping VLAN information.

Usage
show igmp snooping vlan <vid>

Example

```
admin@sonic:~$ show igmp snooping vlan 1
 VLAN 1:
 --------
 IGMP Snooping                  : Disabled
 IGMP Snooping Running Status       : Inactive
 Version                        : Using global version (2)
 Immediate Leave                : Disabled
 Last Member Query Interval         : 10 (unit: 1/10s)
 Last Member Query Count            : 2
 Query Interval                 : 125
 Query Response Interval            : 100 (unit: 1/10s)
 VLAN Static Group    Port
 ---- --------------- -----------
 1    225.1.1.1       Ethernet  6
```

71 Policy-Based Routing (PBR)

Table of Contents

PBR Config Commands

config pbr {add|del} map <pbr-map-name> <sequence-number> {permit|deny}

This command add or delete a pbr map rule entry.

Usage

config pbr {add|del} map <pbr-map-name> <sequence-number> {permit|deny}

Example
admin@sonic:~$ sudo config pbr add map pmap1 10 permit admin@sonic:~$ sudo config pbr del map pmap1 10 permit

config pbr map <pbr-map-name> <sequence-number> match {add|del}

This command add or delete the match attributes of a pbr map rule entry.

Usage
config pbr map <pbr-map-name> <sequence-number> match {add|del} --src_ip <ipv4/v6> --dst_ip <ipv4/v6> -- src_port <0-65535> --dst_port <0-65535> --ip_proto <0-255>

Example
admin@sonic:~$ sudo config pbr map pmap1 10 match add --src_ip 1.1.1.1

config pbr map <pbr-map-name> <sequence-number> action {add|del}

This command add or delete the action attributes of a pbr map rule entry.

Note: There is no action for 'deny' type

Usage
config pbr map <pbr-map-name> <sequence-number> action {add|del} --nexthop <ipv4/v6> --dscp <0-63>

Example
admin@sonic:~$ sudo config pbr map pmap1 10 action add --nexthop 192.169.2.2

config interface pbr bind/unbind

This command bind or unbind the packet incoming interface with pbr map, supporting Vlan, Ethernet, and PortChannel interface binding PBR.

Usage
config interface pbr bind <interface_name> <pbr-map-name> config interface pbr unbind <interface_name>

Example
admin@sonic:~$ sudo config interface pbr bind Ethernet1 pmap1 admin@sonic:~$ sudo config interface pbr unbind Ethernet1

PBR Show Commands

show pbr map

This command shows which set of next-hops are active.

Usage
show pbr map [<pbr-map-name>]

Example
admin@sonic:~$ show pbr m + +------------+--------+---------------+--------------------+ | Map | Sequence | Type | Match | Action set | +=======+============+========+===============+====================+ | pmap1 | 10 | permit | src_ip:1.1.1.1 | nexthop:192.169.2.2 | +-------+------------+--------+---------------+--------------------+ | pmap1 | 20 | permit | src_ip:2.2.2.2 | nexthop:192.169.3.2 | +-------+------------+--------+---------------+--------------------+

show pbr interface

This command shows the interface bound with pbr

Usage
show pbr interface [<interface_name>] [--detail]

Example
admin@sonic:~$ show pbr interface Interface Map ---------- ----- Ethernet1 pmap1 Ethernet2 pmap1 admin@sonic:~$ show pbr interface --detail Interface Map Seq Status ---------- ----- ----- -------- Ethernet1 pmap1 10 Inactive Ethernet1 pmap1 20 Inactive Ethernet2 pmap1 10 Inactive

Ethernet2 pmap1 20 Inactive

72 VRRP

Virtual router redundancy protocol is as known backup router mechanism to prevent traffic broken suddenly while a router with some problems. The election happen between these routers , which takes part in VRRP group. Highest priority routers as master is responsible for forwarding traffic, another as backup.

VRRP interface command

Use config interface vrrp command to create or delete VRRP interface.

Note

The VRRP interface name always starts with "Vrrp" and combines with the group ID and v4 or v6.

VRRP interface needs to designate a parent interface name, for instance, you want to create a VRRP interface on Vlan1000, you need to type Vlan1000 as the last parameter

Use config interface vrrp ip command to set or remove IPv4/IPv6 address on VRRP interface.

Note

This command automatically derives the virtual MAC address from the VRRP interface name and IP address

Example
admin@sonic:~$ config interface vrrp add Vrrp5-v4 Vlan1000
admin@sonic:~$ config interface vrrp ip add Vrrp5-v4 10.0.2.16/24
admin@sonic:~$ config interface vrrp ip del Vrrp5-v4
admin@sonic:~$ config interface vrrp add Vrrp5-v6 Vlan1000
admin@sonic:~$ config interface vrrp ipv6 add Vrrp5-v6 2001:db8::370:7334/64
admin@sonic:~$ config interface vrrp ipv6 del Vrrp5-v6

VRRP group command

Configure VRRP group through FRR command. Note that Vlan1000 is parent interface.

Example
admin@sonic:~$ vtysh
sonic# configure
sonic(config)# interface Vlan1000
sonic(config-if)# vrrp 5 version 3
sonic(config-if)# vrrp 5 ip 10.0.2.16
sonic(config-if)# vrrp 5 ipv6 2001:0db8::0370:7334
sonic(config-if)# no vrrp 5

VRRP show command

Use show vrrp command to display all of VRRP status.

Use show vrrp interface command to display VRRP group associated the interface.

Use show vrrp summary command to display the brief information.

Example

```
admin@sonic:~$ show vrrp
 Virtual Router ID               5
 Protocol Version                3
 Autoconfigured                  No
 Shutdown                        No
 Interface                       eth0
 VRRP interface (v4)             None
 VRRP interface (v6)             None
 Primary IP (v4)
 Primary IP (v6)                 ::
 Virtual MAC (v4)                00:00:5e:00:01:05
 Virtual MAC (v6)                00:00:5e:00:02:05
 Status (v4)                     Initialize
 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)   0 ms
 Master Advertisement Interval (v6)   0 ms
 Advertisements Tx (v4)          0
 Advertisements Tx (v6)          0
 Advertisements Rx (v4)          0
 Advertisements Rx (v6)          0
 Gratuitous ARP Tx (v4)          0
 Neigh. Adverts Tx (v6)          0
 State transitions (v4)          0
 State transitions (v6)          0
 Skew Time (v4)                  0 ms
```

```
Skew Time (v6)                  0 ms
Master Down Interval (v4)       0 ms
Master Down Interval (v6)       0 ms
IPv4 Addresses                  0
IPv6 Addresses                  0
admin@sonic:~$ show vrrp interface Vlan1000
Virtual Router ID               5
Protocol Version                3
Autoconfigured                  No
Shutdown                        No
Interface                       Vlan1000
VRRP interface (v4)             None
VRRP interface (v6)             None
Primary IP (v4)
Primary IP (v6)                 ::
Virtual MAC (v4)                00:00:5e:00:01:05
Virtual MAC (v6)                00:00:5e:00:02:05
Status (v4)                     Initialize
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)  0 ms
Master Advertisement Interval (v6)  0 ms
Advertisements Tx (v4)          0
Advertisements Tx (v6)          0
 Advertisements Rx (v4)         0
Advertisements Rx (v6)          0
Gratuitous ARP Tx (v4)          0
Neigh. Adverts Tx (v6)          0
State transitions (v4)          0
```

```
State transitions (v6)            0
Skew Time (v4)                    0 ms
Skew Time (v6)                    0 ms
Master Down Interval (v4)         0 ms
Master Down Interval (v6)         0 ms
IPv4 Addresses                    0
IPv6 Addresses                    0
admin@sonic:~$ show vrrp summary
 Interface   VRID   Priority   IPv4   IPv6   State (v4)   State (v6)
 ---------------------------------------------------------------------
 Vlan1000    5      100        0      0      Backup       Backup
```

73 Isolation-myself

During the convergence of the routing protocol, some Layer 3 traffic may have the same ingress and egress interfaces, resulting in a temporary loop. By enabling the "isolation-myself" function, Layer 3 forwarding traffic with the same ingress and egress interfaces will be discarded at the egress interface, thereby preventing loops.

Isolation-myself Show Commands

show isolation-myself all

This command is used to display isolation-myself configuration.

Example

```
root@sonic:/home/admin# show isolation-myself all
+----------------+---------+
| Interface Name  | Status  |
+=================+=========+
| Ethernet0       | disable |
```

```
+----------------+---------+
| Ethernet1      | disable |
+----------------+---------+
| Ethernet2      | disable |
+----------------+---------+
| Ethernet3      | disable |
+----------------+---------+
| Ethernet4      | disable |
+----------------+---------+
| Ethernet5      | disable |
+----------------+---------+
| Ethernet6      | disable |
+----------------+---------+
```

show isolation-myself interface <interface_name>

This command is used to display isolation-myself configuration for a specified port.

Example

```
root@sonic:/home/admin# show isolation-myself interface Ethernet7
+----------------+---------+
| Interface Name  | Status  |
+=================+=========+
| Ethernet7      | enable  |
+----------------+---------+
```

Isolation-myself Config Commands

config interface isolation-myself enable <interface_name>

config interface isolation-myself disable <interface_name>

The default port does not have isolation-myself, and only supports Ethernet interface configuration.

Example
root@sonic:/home/admin# config interface isolation-myself enable Ethernet6 root@sonic:/home/admin# config interface isolation-myself disable Ethernet6

74 Static DNS

Table of Contents

Static DNS display command

show dns nameserver

This command is used to display static DNS configuration

Example
admin@sonic:~$ show dns nameserver Nameserver --- 172.21.170.178

Static DNS configuration command

config dns nameserver add

This command is used to add static DNS configuration

Example

admin@sonic:~$ sudo config dns nameserver add 172.21.170.178
admin@sonic:~$ sudo config dns nameserver add 172.21.170.177
admin@sonic:~$ sudo config dns nameserver add 2001::1
admin@sonic:~$ sudo config dns nameserver add 2001::2
Usage: config dns nameserver add [OPTIONS] <ip_address>
Try "config dns nameserver add -h" for help.
 	
Error: The maximum number (3) of nameservers exceeded.
 	
admin@sonic:~$ show dns nameserver
  Nameserver
-------------- 	
172.21.170.177
172.21.170.178
  2001::1

config dns nameserver del

This command is used to delete static DNS configuration

Example
admin@sonic:~$ sudo config dns del 172.21.170.178

75 Hash

Table of Contents

This section explains the various show and configuration commands available for user.

Hash Show Commands

This subsection explains how to display switch hash configuration.

show switch-hash global

This command displays switch hash global configuration.

Usage
show switch-hash global

Options:

-j, --json Display in JSON format

Example
root@sonic:/home/admin# show switch-hash global +----------+-------------------------------------+ | Hash | Configuration | +==========+=====================================+ | ECMP | +--------------+-------------+--------+ |

```
|         | | Hash Field   | Algorithm   | Seed   | |
|         | |--------------+-------------+--------| |
|         | | IP_PROTOCOL  | CRC_32HI    | 10     | |
|         | | DST_IP       |             |        | |
|         | | SRC_IP       |             |        | |
|         | | L4_DST_PORT  |             |        | |
|         | | L4_SRC_PORT  |             |        | |
|         | +--------------+-------------+--------+ |
+-----------+-------------------------------------+
| LAG       | +--------------+-------------+--------+ |
|         | | Hash Field   | Algorithm   | Seed   | |
|         | |--------------+-------------+--------| |
|         | | IP_PROTOCOL  | CRC_32HI    | 10     | |
|         | | DST_IP       |             |        | |
|         | | SRC_IP       |             |        | |
|         | | L4_DST_PORT  |             |        | |
|         | | L4_SRC_PORT  |             |        | |
|         | +--------------+-------------+--------+ |
+-----------+-------------------------------------+
| SYMMETRIC | +---------+                         |
|         | | State   |                           |
|         | |---------|                         |
|         | | disable |                           |
|         | +---------+                           |
+-----------+-------------------------------------+
root@sonic:/home/admin#
```

Hash Config Commands

This subsection explains how to configure switch hash.

config switch-hash global ecmp/lag hash

This command is used to manage switch hash global configuration.

Usage
config switch-hash global ecmp-hash <hash_field_list> config switch-hash global lag-hash <hash_field_list>

Parameters:

hash_field_list: hash fields for hashing packets going through ECMP/LAG. Range: IN_PORT, VLAN_ID, IP_PROTOCOL, DST_IP, SRC_IP, L4_DST_PORT, L4_SRC_PORT, IPV6_FLOW_LABEL. One or more of these can be used, and multiple fields should be separated by spaces.

Example
root@sonic:/home/admin# config switch-hash global ecmp-hash IN_PORT VLAN_ID IP_PROTOCOL DST_IP SRC_IP L4_DST_PORT L4_SRC_PORT IPV6_FLOW_LABEL

config switch-hash global ecmp/lag hash algorithm

This command is used to manage switch hash algorithm global configuration.

Usage
config switch-hash global ecmp-hash-algorithm <hash_algorithm> config switch-hash global lag-hash-algorithm <hash_algorithm>

Parameters:

hash_algorithm: hash algorithm for hashing packets going through ECMP/LAG.Range: CRC, XOR, CRC_32LO, CRC_32HI, CRC_CCITT, CRC_XOR. One of these must be used.

Example
config switch-hash global ecmp-hash-algorithm CRC config switch-hash global lag-hash-algorithm CRC

config switch-hash global ecmp/lag hash seed

This command is used to manage switch hash seed global configuration.

Usage
config switch-hash global ecmp-hash-seed <hash_seed> config switch-hash global lag-hash-seed <hash_seed>

Parameters:

hash_seed: hash seed for hashing packets going through ECMP/LAG. Range:0-4294967295, default:10.

Example
config switch-hash global ecmp-hash-seed 100 config switch-hash global lag-hash-seed 200

config switch-hash global symmetric

This command is used to manage switch symmetric hash configuration.

Usage

config switch-hash global symmetric <enable/disable>

Parameters:

<enable/disable>: Used to enable or disable symmetric hash. Default value: disable.

Example
config switch-hash global symmetric enable

76 Routing Security

Table of Contents

Routing Security show commands

show route-table vrf <vrf_name>

This command is used to display the routing information installed in all VRFs or a specified VRF.

Usage
show route-table vrf <vrf_name>

Parameter:

- <vrf_name>: VRF name. For example: "Vrf1".

Note:

- The displayed installed routing information does not include the routing information of the default VRF.

Example

```
admin@sonic:~$ show route-table vrf
VRF    Simply alert    IPV4 Max Route limit    IPV6 Max Route limit    Installed Routes     Installed Routes NUM
-----  --------------  ----------------------  ----------------------  -----------------  ----------------------
Vrf1   Disabled                                                        128.1.1.0/24                    2
                                                                       128.1.1.4


admin@sonic:~$ show route-table vrf Vrf1
VRF    Simply alert    IPV4 Max Route limit    IPV6 Max Route limit    Installed Routes     Installed Routes NUM
-----  --------------  ----------------------  ----------------------  -----------------  ----------------------
Vrf1   Disabled                                                        128.1.1.0/24                    2
                                                                       128.1.1.4
```

show route-table ip <vrf_name>

This command is used to display the IPv4 routing information installed in all VRFs or a specified VRF.

Usage
show route-table ip <vrf_name>

Parameter:

- <vrf_name>: VRF name. For example: "Vrf1".

Example
admin@sonic:~$ show route-table ip VRF Simply alert IPV4 Max Route limit Installed Routes Installed Routes NUM ----- ------------ ---------------------- ----------------- ---------------------- Vrf1 Disabled 128.1.1.0/24 2 128.1.1.4 admin@sonic:~$ show route-table ip Vrf1 VRF Simply alert IPV4 Max Route limit Installed Routes Installed Routes NUM ----- ------------ ---------------------- ----------------- ---------------------- Vrf1 Disabled 128.1.1.0/24 2 128.1.1.4

show route-table ipv6 <vrf_name>

This command is used to display the IPv6 routing information installed in all VRFs or a specified VRF.

Usage
show route-table ipv6 <vrf_name>

Parameter:

- <vrf_name>: VRF name. For example: "Vrf1".

Example
admin@sonic:~$ show route-table ipv6 VRF Simply alert IPV6 Max Route limit Installed Routes Installed Routes NUM ----- ------------ ---------------------- ----------------- ---------------------- Vrf1 Disabled 2018::/64 2 2018::7 admin@sonic:~$ show route-table ipv6 Vrf1

VRF	Simply alert	IPV6 Max Route limit	Installed Routes	Installed Routes NUM
Vrf1	Disabled	2018::/64	2	
		2018::7		

Routing Security config commands

config vrf simply-alert set/unset <vrf_name>

This command configures whether to only issue a warning message when the maximum number of routes in a VRF exceeds the configured route limit. If only a warning message is issued, new routes can continue to be added to the VRF. If not, once the configured route limit is reached, no new routes will be added to the VRF.

Usage
config vrf simply-alert set/unset <vrf_name>

Parameter:

- <vrf_name>: VRF name. For example: "Vrf1".

Note:

- The default VRF does not support configuring these values.

Example

```
admin@sonic:~$ sudo config vrf simply-alert set Vrf1
admin@sonic:~$ show route-table ip Vrf1
VRF    Simply alert    IPV4 Max Route limit    Installed Routes      Installed Routes NUM
-----  --------------  ----------------------  ------------------  ----------------------
Vrf1   Enabled                          128.1.1.0/24                      2
                                  128.1.1.4
```

config vrf route-table-limit <ip_version (ip, ipv6)> <vrf_name> NUMBER

This command configures the maximum number of routes for the VRF.。

Usage
config vrf route-table-limit <ip_version (ip, ipv6)> <vrf_name> NUMBER

Parameter:

- <ip_version>: You can choose to configure IPv4 and/or IPv6
- <vrf_name>: VRF name. For example: "Vrf1".
- NUMBER : The maximum number of routes for a VRF.

Note:

- The maximum number of IPv4 and IPv6 routes in a VRF are separate.
- The default VRF does not support configuring these values.

Example

```
admin@sonic:~$ sudo config vrf route-table-limit ip Vrf1 6
admin@sonic:~$ show route-table ip Vrf1
admin@sonic:~$ show route-table vrf
VRF    Simply alert    IPV4 Max Route limit    IPV6 Max Route limit    Installed Routes      Installed Routes
NUM
-----  --------------  ----------------------  ----------------------  ------------------  ----------------------
Vrf1   Enabled         6                                 128.1.1.0/24                      2
                                                 128.1.1.4
```

```
admin@sonic:~$ show route-table ip Vrf1
VRF    Simply alert    IPV4 Max Route limit    Installed Routes      Installed Routes NUM
-----  --------------  ----------------------  ------------------  ----------------------
Vrf1   Enabled         6                       128.1.1.0/24                        2
                                               128.1.1.4

admin@sonic:~$ sudo config vrf route-table-limit ipv6 Vrf1 6
admin@sonic:~$ show route-table ipv6 Vrf1
admin@sonic:~$ show route-table ipv6 Vrf1
VRF    Simply alert    IPV6 Max Route limit    Installed Routes      Installed Routes NUM
-----  --------------  ----------------------  ------------------  ----------------------
Vrf1   Enabled         6                       2018::/64                           2
                                               2018::7
```

77 Fine-grained ECMP

Table of Contents

Show Commands

show fgnhg group

This command displays fine-grained ECMP group configurations.

Usage
show fgnhg group [OPTIONS] [<fgnhg_group_name>| "all"]

Parameter:

fgnhg_group_name: name of the fgnhg group

Example
root@sonic:/home/admin# show fgnhg group +------------+-------------+------------------+ | Group Name | Match Mode | Hash Bucket Size | +==============+===============+====================+ | fg21 | route-based | 64 | +------------+-------------+------------------+ | fg22 | nexthop-based | 64 | +------------+-------------+------------------+

show fgnhg active-hops

This command displays the effective next hop for routes by prefix.

Usage
show fgnhg active-hops [OPTIONS] [NHG]

Parameter:

NHG: Only route-based fine-grained ECMP group can query the active next hop for the group.

Example
root@sonic:/home/admin# show fgnhg active-hops +----------------+-------------------+ | FG_NHG_PREFIX | Active Next Hops | +================+===================+ | 55.0.0.0/24 | 10.10.1.1 | | | 10.10.2.1 | | | 10.10.3.1 | +----------------+-------------------+ | 44.0.0.0/24 | 10.10.1.1 | | | 10.10.2.1 | | | 10.10.3.1 | | | 10.10.4.1 | +----------------+-------------------+ root@sonic:/home/admin#

show fgnhg hash-view

This command displays the next hop hash view for routes by prefix.

Usage
show fgnhg hash-view [OPTIONS] [NHG]

Parameter:

NHG: Only route-based fine-grained ECMP group can query the next hop hash view for the group.

Example

```
root@sonic:/home/admin# show fgnhg hash-view
+----------------+-----------+---------------+
| FG_NHG_PREFIX  | Next Hop  | Hash buckets  |
+================+===========+===============+
| 55.0.0.0/24    | 10.10.1.1 | 0             |
|                |           | 2             |
|                |           | 4             |
|                |           | 6             |
|                |           | 8             |
|                |           | 10            |
|                |           | 12            |
|                |           | 14            |
|                |           | 16            |
|                |           | 18            |
|                |           | 20            |
|                |           | 22            |
|                |           | 24            |
|                |           | 26            |
|                |           | 28            |
|                |           | 30            |
+----------------+-----------+---------------+
| 55.0.0.0/24    | 10.10.2.1 | 1             |
|                |           | 3             |
|                |           | 5             |
|                |           | 7             |
|                |           | 9             |
|                |           | 11            |
|                |           | 13            |
|                |           | 15            |
```

```
|               |           | 17          |
|               |           | 19          |
|               |           | 21          |
|               |           | 23          |
|               |           | 25          |
|               |           | 27          |
|               |           | 29          |
|               |           | 31          |
+---------------+-----------+-------------+
| 55.0.0.0/24   | 10.10.3.1 | 32          |
|               |           | 33          |
|               |           | 34          |
|               |           | 35          |
|               |           | 36          |
|               |           | 37          |
|               |           | 38          |
|               |           | 39          |
|               |           | 40          |
|               |           | 41          |
|               |           | 42          |
|               |           | 43          |
|               |           | 44          |
|               |           | 45          |
|               |           | 46          |
|               |           | 47          |
|               |           | 48          |
|               |           | 49          |
|               |           | 50          |
|               |           | 51          |
|               |           | 52          |
|               |           | 53          |
|               |           | 54          |
|               |           | 55          |
|               |           | 56          |
|               |           | 57          |
|               |           | 58          |
```

```
|             |          | 59          |
|             |          | 60          |
|             |          | 61          |
|             |          | 62          |
|             |          | 63          |
+---------------+-----------+---------------+
| 44.0.0.0/24    | 10.10.1.1  | 0           |
|             |          | 1           |
|             |          | 2           |
|             |          | 3           |
|             |          | 4           |
|             |          | 5           |
|             |          | 6           |
|             |          | 7           |
|             |          | 8           |
|             |          | 9           |
|             |          | 10          |
|             |          | 11          |
|             |          | 12          |
|             |          | 13          |
|             |          | 14          |
|             |          | 15          |
+---------------+-----------+---------------+
| 44.0.0.0/24    | 10.10.2.1  | 16          |
|             |          | 17          |
|             |          | 18          |
|             |          | 19          |
|             |          | 20          |
|             |          | 21          |
|             |          | 22          |
|             |          | 23          |
|             |          | 24          |
|             |          | 25          |
|             |          | 26          |
|             |          | 27          |
|             |          | 28          |
```

```
|               |           | 29            |
|               |           | 30            |
|               |           | 31            |
+---------------+-----------+---------------+
| 44.0.0.0/24   | 10.10.3.1 | 32            |
|               |           | 33            |
|               |           | 34            |
|               |           | 35            |
|               |           | 36            |
|               |           | 37            |
|               |           | 38            |
|               |           | 39            |
|               |           | 40            |
|               |           | 41            |
|               |           | 42            |
|               |           | 43            |
|               |           | 44            |
|               |           | 45            |
|               |           | 46            |
|               |           | 47            |
+---------------+-----------+---------------+
| 44.0.0.0/24   | 10.10.4.1 | 48            |
|               |           | 49            |
|               |           | 50            |
|               |           | 51            |
|               |           | 52            |
|               |           | 53            |
|               |           | 54            |
|               |           | 55            |
|               |           | 56            |
|               |           | 57            |
|               |           | 58            |
|               |           | 59            |
|               |           | 60            |
|               |           | 61            |
|               |           | 62            |
```

```
|              |          | 63          |
+--------------+----------+-------------+
```

Config Commands

config fgnhg group

This command is used to create or delete a fine-grained ECMP group.

Usage
config fgnhg add [OPTIONS] <fgnhg_group_name> type <type_value> size <size_value> match-mode <match-mode-value> config fgnhg del [OPTIONS] FGNHG_GROUP_NAME

Parameter:

fgnhg_group_name/FGNHG_GROUP_NAME: Name of fine-grained ECMP group.

type_value：Only the "static" type is supported.

size_value：Only 64 is supported.

match-mode-value："route-based" or "nexthop-based"

Note：

- Does not support directly updating the match-mode of an existing group; the old group must be deleted and then recreated.
- The group can only be deleted after all members and prefixes in the group have been removed.

Example

```
root@sonic:/home/admin# config fgnhg add fg21 type static size 64 match-mode route-based

root@sonic:/home/admin# config fgnhg del fg21
```

config fgnhg member

This command is used to add or delete members from a fine-grained ECMP group.

Usage
config fgnhg member add [OPTIONS] FGNHG_GROUP_NAME NEXTHOP_IP <bank_number> [nexthop_intf] config fgnhg member del [OPTIONS] FGNHG_GROUP_NAME NEXTHOP_IP

Parameter:

FGNHG_GROUP_NAME: Name of fine-grained ECMP group.

NEXTHOP_IP: The next-hop IPv4/IPv6 address of the member.

bank_number: Start from 0 and be added in sequential order. Members in the same bank share the same state. When a member fails or recovers, flow redistribution occurs among members in the same bank.

nexthop_intf： The local interface name for the next hop. Support Ethernet and PortChannel interface name.

Note:

- If the group has already been configured with a prefix, then no more members can be added to the group. You need to remove the prefix configuration before changing the group members.
- A member can only be configured for one group. If you need to update the group that a member belongs to, you need to delete the old group member and then add the member to the new group.

Example
root@sonic:/home/admin# config fgnhg member add fg21 10.10.1.1 0 Ethernet448

root@sonic:/home/admin# config fgnhg member del fg21 10.10.1.1

config fgnhg prefix

This command is used to add or delete prefixes in the route-based mode of a fine-grained ECMP group.

Usage
config fgnhg prefix add [OPTIONS] FGNHG_GROUP_NAME PREFIX config fgnhg prefix del [OPTIONS] FGNHG_GROUP_NAME PREFIX

Parameter：

FGNHG_GROUP_NAME：Name of fine-grained ECMP group.

PREFIX：IPv4/IPv6 network segment used to match ECMP routes.

Note：

- Members must be added to the group first before configuring route prefixes.
- A prefix can only be configured for one group. If you need to update the group that a prefix belongs to, you need to delete the old prefix and then add the prefix to the new group.

Example
root@sonic:/home/admin# config fgnhg prefix add fg21 44.0.0.0/24 root@sonic:/home/admin# config fgnhg prefix del fg21 44.0.0.0/24

78 Monitor Link

Monitor Link Group show commands

show monitor-link group

This command displays monitor link group configurations.

Usage
show monitor-link group

Example
root@sonic:/home/admin# show monitor-link group ------- Monitor Link Configuration -------

```
Group ID            : 1
Downlink Up Delay   : 0
Uplink Interface    : Ethernet512
Downlink Interface  : Ethernet513

Interface    Type      Oper Status    Shutdown Reason
-----------  --------  -------------  ----------------
Ethernet512  uplink    up
Ethernet513  downlink  up
```

Monitor Link Group config commands

config monitor-link group member add

This command is used to add uplink or downlink port to the specified monitor link group.

Usage
config monitor-link group member add <group_id> <types (downlink or uplink)> <interface_name>

Example
root@sonic:/home/admin# config monitor-link group member add 1 uplink Ethernet512 root@sonic:/home/admin# config monitor-link group member add 1 downlink Ethernet513

config monitor-link group member delete

This command is used to delete uplink or downlink port from the specified monitor link group.

Usage
config monitor-link group member del <group_id> <types (downlink or uplink)> <interface_name>

Example
root@sonic:/home/admin# config monitor-link group member del 1 downlink Ethernet513

config monitor-link group downlink-up-delay set

This command is used to configure downlink up delay for the specified monitor link group.

Usage
config monitor-link group downlink-up-delay set <group_id> <downlink_up_delay>

Example
root@sonic:/home/admin# config monitor-link group downlink-up-delay set 1 10

config monitor-link group downlink-up-delay unset

This command is used to delete downlink up delay for the specified monitor link group.

Usage
config monitor-link group downlink-up-delay unset <group_id>

Example
root@sonic:/home/admin# config monitor-link group downlink-up-delay unset 1

79 Platform Component Firmware

80 Latency Distribution Histogram（LDH）

Table of Contents

LDH show commands

show ldh counter <ldh-name>

This command is used to display ldh statistics .

Usage
Usage: show ldh counter [OPTIONS] <ldh-name> Show ldh counter information

Example
root@sonic:/home/admin# show ldh counter LDH0 Last cached time was 2025-06-16 02:12:02.367406 RANGE TIME PACKETS --- --- 0-1(ns) 0 2-1000(ns) 0 1001-10000(ns) 0 10001-60000(ns) 0

sonic-clear ldhcounters

This command is used to clear ldh statistics.

Usage
Usage: sonic-clear ldhcounters [OPTIONS] Clear ldh counters

Example
root@sonic:/home/admin# sonic-clear ldhcounters Clear saved counters

LDH config commands

config ldh timerange add <ldh-name> <time-range>

This command is used to configure the time range for LDH.

Usage
Usage: config ldh timerange add [OPTIONS] <ldh-name> <time-range> config LDH timerange information

Example
root@sonic:/home/admin# sudo config ldh timerange add LDH0 0-1,2-1000,1001-10000,10001-60000

config ldh srcport add <ldh-name> <src-port>

This command is used to configure the source port of LDH.

Usage
Usage: config ldh srcport add [OPTIONS] <ldh-name> <src-port> config LDH srcport information

Example
root@sonic:/home/admin# sudo config ldh srcport add LDH0 Ethernet8,Ethernet16,Ethernet24

config ldh dstport add <ldh-name> <dst-port>

This command is used to configure the destination port of LDH.

Usage
Usage: config ldh dstport add [OPTIONS] <ldh-name> <dst-port> config LDH srcport information

Example
root@sonic:/home/admin# sudo config ldh dstport add LDH0 Ethernet8,Ethernet24,Ethernet32

config ldh set state <ldh-name> <mode>

This command is used to enable or disable LDH.

Usage
Usage: config ldh set state [OPTIONS] <ldh-name> <mode>

Example
root@sonic:/home/admin# sudo config ldh set state LDH0 enable root@sonic:/home/admin# sudo config ldh set state LDH0 disable

config ldh del <ldh-name>

This command is used to delete the created LDH.

Usage
Usage: config ldh del [OPTIONS] <ldh-name>

Example
root@sonic:/home/admin# sudo config ldh del LDH0

81 AR

Adaptive Routing show commands

show ar config

This command displays the AR configuration information.

Usage
show ar config

Example
admin@sonic:~$ show ar config AR state: enabled AR Port ---------- Ethernet92 Ethernet116 Ethernet140

Adaptive Routing config commands

config ar enabled
config ar disabled

This command is used to enable or disable the AR feature。

Usage
config ar enabled **config ar disabled**

Example
admin@sonic:~$ sudo config ar enabled

config ar port enabled <interface_name>
config ar port disabled <interface_name>

This command is used to enable or disable the AR feature on an interface。

Usage
config ar port enabled <interface_name> **config ar port disabled <interface_name>**

Note:

- The AR feature configuration will take effect only after restarting swss. Make sure to save the configuration before restarting swss；
- To enable the AR feature on an interface, the AR feature must also be enabled globally。

Example
admin@sonic:~$ sudo config ar port enabled Ethernet116

Further Information

Web www.naddod.com

Email For order requirements: **sales@naddod.com**
For other information: **info@naddod.com**
For cooperation: **agency@naddod.com**
For technical support: **tech@naddod.com**
For customer service: **support@naddod.com**

Disclaimer

1. We are committed to continuous product improvement and feature upgrades, and the contents contained in this manual are subject to change without notice.
2. Nothing herein should be construed as constituting an additional warranty.
3. NADDOD assumes no responsibility for the use or reliability of equipment or software not provided by NADDOD.