###### Access CLI interface

***Objective:***

This test case verifies that the node with SAOS 10.x is reachable from the network for IP management, and to open the CLI for manual CLI-based configuration of SAOS 10.x box.

***Procedure:***

 Login to system through console port. Provision a static IP or check if any DHCP IP has been assigned to local management interface mgmtbr0.

#disable DHCP

dhcp-client client mgmtbr0 admin-enable false

#setup static IP for mgmtbr0

oc-if:interfaces interface mgmtbr0 ipv4 address address x.x.x.x config ip x.x.x.x prefix-length 20

#Setup static route to default gateway

rib vrf default ipv4 10.0.0.0/8 next-hop x.x.x.x description "default gw"

* Display the IP interfaces.

show ip interfaces brief

* Login to UI using the management IP you checked in the previous step:

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

* + Replace x.x.x.x with IP address of the node.
  + username: diag password: ciena123
  + ~~a “-p 830” parameter for port 830 is only needed for SAOS 10.2 or earlier.~~
  + You will be logged in to the CLI
  + You can now access the configuration interface with typing
    - config

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### ZTP

***Objective:***

Objective is to install SAOS 10.x with ZTP process. Network based ZTP process is useful when we want to ensure the same version of software is automatically installed on multiple nodes in the network. ZTP only allowed over VLAN 127, and untagged is not supported.

***Procedure:***

* Ensure you have DHCP environment setup is been done with either of
  + Option 66/67 to provide tftp server and filename of Command File
  + Option 125 to provide URL of Command Fil
* Ensure that the image you want to download is located on an HTTP/TFTP server
* Verify that the command file is located at the TFTP server and the config file is supplied
* Start the node if it is the first time it is being powered up
* Once the device boots up, Login to UI container using the management IP you checked in the previous step (default login/passwd displayed below):

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

username: diag password: ciena123

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Verify Manual network-based installation

***Objective:***

Objective is to install SAOS 10.x on a system, using the manual network-based installation.

***Procedure:***

* Login to system console port.
* When ONIE comes up it will try to find the resource for ZTP. If you want to specify the location of the installer file manually, which is different from what it might fetch from network installer, you should stop it:

ONIE:/ # onie-discovery-stop

* Then proceed with the manual installation from the installer file from http, tftp or ftp server.

ONIE:/ # onie-nos-install <http://x.x.x.x/installer.bin> ONIE:/ # onie-nos-install tftp://x.x.x.x/installer.bin ONIE:/ # onie-nos-install ftp://x.x.x.x/installer.bin

Replace x.x.x.x with IP address or the URL of where the image is residing. Here is an example:

ONIE:/ # onie-nos-install <http://x.x.x.x/valimar-> snapshot/17-12-00-0141/meta-onie-installer-dnx/meta\_01-00- 00-0181-core.bin

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Verify USB-based installation of SAOS 10.x

***Objective:***

Objective is to install SAOS 10.x on a system using USB-based method.

***Procedure:***

* Ensure that the format of your USB stick is FAT32 formatted.
* Ensure that the image you want is on the USB stick
* Ensure that the image is named “**onie-installer**”. This is important. Currently, the load name cannot be named anything else.
* Start the node if it is the first time it is being powered up, or follow the following steps otherwise
* Login to UI container using the management IP you checked in the previous step:

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

username: diag password: ciena123

When ONIE comes up it will try to find the resource for ZTP. Wait for the installation to complete from here.

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Verify System Power Cycle will maintain the configuration

***Objective:***

To verify that SAOS 10.x on sytem maintains configuration and operation following a disruption to power.

***Procedure:***

* Login to UI container using the management IP you checked in the previous step:

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

username: diag password: ciena123

* Then issue the reboot command below or power cycle the node.
  + system restart
* Once powered up verify that device can be reachable by management network, and login is re-enabled.
* Login to the box and confirm configuration is still in place.

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### SNMP v3 Trap Configuration

***Objective:***

The objective of this section is to configure SNMP v3 Trap on the SAOS cli.

***SNMPv3 Trap:***

* + - * Same as the SNMP GET parameters but additional fields are added to specify the Trap target IP.

***Procedure:***

snmp usm local user cienaNoAuthNoPrivUser exit

exit exit exit

snmp usm local user cienaAuthNoPrivUser auth md5 key 63:69:65:6e:61:41:75:74:68:4b:65:79 snmp usm local user cienaAuthPrivUser auth md5 key 63:69:65:6e:61:41:75:74:68:4b:65:79 snmp usm local user cienaAuthPrivUser priv des key 63:69:65:6e:61:50:72:69:76:4b:65:79

snmp vacm group cienaV3Group access "" usm no-auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaV3Group access "" usm auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaV3Group access "" usm auth-priv context-match exact notify-view cienaAll snmp vacm group cienaV3Group member cienaNoAuthNoPrivUser security-model usm

snmp vacm group cienaV3Group member cienaAuthNoPrivUser security-model usm snmp vacm group cienaV3Group member cienaAuthPrivUser security-model usm snmp target TestTarget2 target-params TestUsmNoAuthNoPriv udp ip 10.176.137.38 snmp target TestTarget2 tag TestTag

snmp target TestTarget3 target-params TestUsmAuthNoPriv udp ip 10.176.137.38 snmp target TestTarget3 tag TestTag

snmp target TestTarget4 target-params TestUsmAuthPriv udp ip 10.176.137.38 snmp target TestTarget4 tag TestTag

snmp target-params TestUsmNoAuthNoPriv usm security-level no-auth-no-priv user-name cienaNoAuthNoPrivUser

snmp target-params TestUsmAuthNoPriv usm security-level auth-no-priv user-name cienaAuthNoPrivUser

snmp target-params TestUsmAuthPriv usm security-level auth-priv user-name cienaAuthPrivUser snmp vacm view cienaAll include internet

snmp notify Test-NOTIFY tag TestTag type trap

***Output:***

* show snmp

+

SNMP NOTIFY +

| Notification Name | Notification Tag | Notification Type |

+ + + +

| Test-NOTIFY | TestTag | trap |

+ + +

+

+

SNMP USM +

| User Name | Type | Auth Protocol | Priv Protocol | Engine ID |

+ + + + + +

| cienaNoAuthNoPrivUser | local | | | 80:00:05:23:01:0A:78:67:F8:00:00 |

| cienaAuthNoPrivUser | local | md5 | | 80:00:05:23:01:0A:78:67:F8:00:00 |

| cienaAuthPrivUser | local | md5 | des | 80:00:05:23:01:0A:78:67:F8:00:00 |

+ + +

+

+ + +

SNMP TARGET-PARAMS +

| Target Param Name | Security Name | User Name | Security Model | Security Level |

+ + + + + +

| TestUsmNoAuthNoPriv | | cienaNoAuthNoPrivUser | usm | no-auth-no-priv |

| TestUsmAuthNoPriv | | cienaAuthNoPrivUser | usm | auth-no-priv |

| TestUsmAuthPriv | | cienaAuthPrivUser | usm | auth-priv |

+ + +

+

+ + +

SNMP TARGET +

| Target Name | IP Address | Param Name | Tags | UDP Port | Retry Count | Timeout | Prefix Length |

+ + + + + + + + +

| TestTarget2 | 10.176.137.38 | TestUsmNoAuthNoPriv | TestTag | 162 | 3 | 1500 | 32 |

| TestTarget3 | 10.176.137.38 | TestUsmAuthNoPriv | TestTag | 162 | 3 | 1500 | 32 |

| TestTarget4 | 10.176.137.38 | TestUsmAuthPriv | TestTag | 162 | 3 | 1500 | 32 |

+ + +

+ SNMP VACM VIEW +

+ + + + + +

| Viewtree Name | Subtree | Type |

+ + + +

| cienaAll | internet | include |

+ + + +

+ SNMP VACM GROUP MEMBER +

| Group Name | Security Model | Security Name |

+ + + +

| cienaV3Group | usm | cienaNoAuthNoPrivUser |

| cienaV3Group | usm | cienaAuthNoPrivUser |

| cienaV3Group | usm | cienaAuthPrivUser |

+ + +

+

+

SNMP VACM GROUP ACCESS +

| Group Name | Context | Context Match | Security Model | Security Level | Read View | Notify View |

+ + + + + + + +

| cienaV3Group | | exact | usm | no-auth-no-priv | | cienaAll |

| cienaV3Group | | exact | usm | auth-no-priv | | cienaAll |

| cienaV3Group | | exact | usm | auth-priv | | cienaAll |

+ + + + + + + +

***Test Case Results:***

Passed: Yes No Verified by Date/Time Comments

###### SNMP v3 Trap Configuration

***Objective:***

The objective of this section is to configure SNMP v3 Trap on the SAOS cli.

***SNMPv3 Trap:***

* + - * Same as the SNMP GET parameters but additional fields are added to specify the Trap target IP.

***Procedure:***

snmp usm local user cienaNoAuthNoPrivUser exit

exit exit exit

snmp usm local user cienaAuthNoPrivUser auth md5 key 63:69:65:6e:61:41:75:74:68:4b:65:79 snmp usm local user cienaAuthPrivUser auth md5 key 63:69:65:6e:61:41:75:74:68:4b:65:79 snmp usm local user cienaAuthPrivUser priv des key 63:69:65:6e:61:50:72:69:76:4b:65:79

snmp vacm group cienaV3Group access "" usm no-auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaV3Group access "" usm auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaV3Group access "" usm auth-priv context-match exact notify-view cienaAll snmp vacm group cienaV3Group member cienaNoAuthNoPrivUser security-model usm

snmp vacm group cienaV3Group member cienaAuthNoPrivUser security-model usm snmp vacm group cienaV3Group member cienaAuthPrivUser security-model usm snmp target TestTarget2 target-params TestUsmNoAuthNoPriv udp ip 10.176.137.38 snmp target TestTarget2 tag TestTag

snmp target TestTarget3 target-params TestUsmAuthNoPriv udp ip 10.176.137.38 snmp target TestTarget3 tag TestTag

snmp target TestTarget4 target-params TestUsmAuthPriv udp ip 10.176.137.38 snmp target TestTarget4 tag TestTag

snmp target-params TestUsmNoAuthNoPriv usm security-level no-auth-no-priv user-name cienaNoAuthNoPrivUser

snmp target-params TestUsmAuthNoPriv usm security-level auth-no-priv user-name cienaAuthNoPrivUser

snmp target-params TestUsmAuthPriv usm security-level auth-priv user-name cienaAuthPrivUser snmp vacm view cienaAll include internet

snmp notify Test-NOTIFY tag TestTag type trap

***Output:***

* show snmp

+

SNMP NOTIFY +

| Notification Name | Notification Tag | Notification Type |

+ + + +

| Test-NOTIFY | TestTag | trap |

+ + +

+

+

SNMP USM +

| User Name | Type | Auth Protocol | Priv Protocol | Engine ID |

+ + + + + +

| cienaNoAuthNoPrivUser | local | | | 80:00:05:23:01:0A:78:67:F8:00:00 |

| cienaAuthNoPrivUser | local | md5 | | 80:00:05:23:01:0A:78:67:F8:00:00 |

| cienaAuthPrivUser | local | md5 | des | 80:00:05:23:01:0A:78:67:F8:00:00 |

+ + +

+

+ + +

SNMP TARGET-PARAMS +

| Target Param Name | Security Name | User Name | Security Model | Security Level |

+ + + + + +

| TestUsmNoAuthNoPriv | | cienaNoAuthNoPrivUser | usm | no-auth-no-priv |

| TestUsmAuthNoPriv | | cienaAuthNoPrivUser | usm | auth-no-priv |

| TestUsmAuthPriv | | cienaAuthPrivUser | usm | auth-priv |

+ + +

+

+ + +

SNMP TARGET +

| Target Name | IP Address | Param Name | Tags | UDP Port | Retry Count | Timeout | Prefix Length |

+ + + + + + + + +

| TestTarget2 | 10.176.137.38 | TestUsmNoAuthNoPriv | TestTag | 162 | 3 | 1500 | 32 |

| TestTarget3 | 10.176.137.38 | TestUsmAuthNoPriv | TestTag | 162 | 3 | 1500 | 32 |

| TestTarget4 | 10.176.137.38 | TestUsmAuthPriv | TestTag | 162 | 3 | 1500 | 32 |

+ + +

+ SNMP VACM VIEW +

+ + + + + +

| Viewtree Name | Subtree | Type |

+ + + +

| cienaAll | internet | include |

+ + + +

+ SNMP VACM GROUP MEMBER +

| Group Name | Security Model | Security Name |

+ + + +

| cienaV3Group | usm | cienaNoAuthNoPrivUser |

| cienaV3Group | usm | cienaAuthNoPrivUser |

| cienaV3Group | usm | cienaAuthPrivUser |

+ + +

+

+

SNMP VACM GROUP ACCESS +

| Group Name | Context | Context Match | Security Model | Security Level | Read View | Notify View |

+ + + + + + + +

| cienaV3Group | | exact | usm | no-auth-no-priv | | cienaAll |

| cienaV3Group | | exact | usm | auth-no-priv | | cienaAll |

| cienaV3Group | | exact | usm | auth-priv | | cienaAll |

+ + + + + + + +

***Test Case Results:***

Passed: Yes No Verified by Date/Time Comments

###### Create New User Account

***Objective:***

Setup a new user account to access the system.

***Procedure:***

* SAOS 10.1 supports two local user groups:
  + SYSTEM\_ROLE\_DIAG : The user has access to CLI, NETCONF, and also to Linux shell.
  + SYSTEM\_ROLE\_USER : The user has access to CLI and NETCONF.
* Enter the following command on CLI to create a new local user User1:

config

system aaa authentication users user **User1** config username User1 role SYSTEM\_ROLE\_USER password Password1

* Verify that the user has been created:

5162\_001> show aaa users

+ USER ACCOUNT TABLE +

| Username | Role | Sessions | Lockout |

+ + + + +

| diag | SYSTEM\_ROLE\_DIAG | | |

| user | SYSTEM\_ROLE\_USER | | |

| **User1** | SYSTEM\_ROLE\_USER | | |

+ + + + +

* Ensure that the user has been added to NACM group -otherwise provisioning by local user will not be allowed.
  + config
  + nacm groups group super user-name User1

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### DHCPv6 Client Setup

***Objective:***

Ensure that with DHCPv6 client enabled, the interface will acquire an IPv6 address automatically. **Only stateful DHCPv6 (no SLAAC) is currently supported.**

***Procedure:***

* Dual IPv4 and IPv6 stack on mgmt. interfaces are supported as of 10.3 and onwards. Enable DHCPv6 client on mgmtbr0. Ensure that :
  + config
  + dhcpv6-client client mgmtbr0 admin-enable true
* Configure IPv4 static IP on the mgmtbr0 as well.
  + dhcp-client client mgmtbr0 admin-enable false
  + oc-if:interfaces interface mgmtbr0 ipv4 address address x.x.x.x config ip x.x.x.x prefix-length 20
  + rib vrf default ipv4 x.x.x.x/8 next-hop x.x.x.x description "lab default"

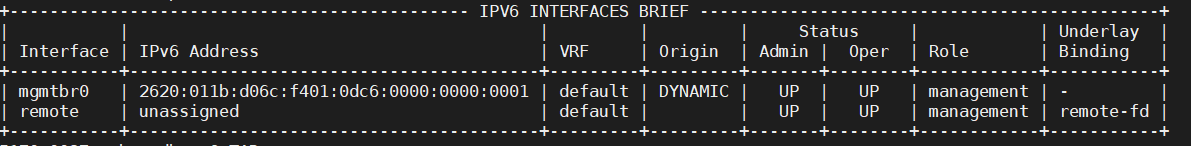
Ex:

dhcp-client client mgmtbr0 admin-enable false

oc-if:interfaces interface mgmtbr0 ipv4 address address 10.181.36.85 config ip 10.181.36.85 prefix-length 20

rib vrf default ipv4 10.0.0.0/8 next-hop 10.181.32.1 description "lab default"

* Display the IPv6 and IPv4 interfaces on the node.
  + 5170-0037> show ipv6 interfaces brief



* + 5170-0037> show ip interfaces brief

A screenshot of a computer

Description automatically generated with medium confidence

5170-0037> show dhcpv6

+-------- DHCPV6 CLIENT CONFIGURATION +

| Name | Value |

+ + +

| Interface Name | mgmtbr0 |

| Admin State | Enabled |

| Rapid Commit | Enabled |

| Requested Preferred Lifetime (s) | 0 |

| Requested Valid Lifetime (s) | 0 |

| Option | |

| DNS Server List | Enabled |

| Domain Search List | Enabled |

| Posix Time Zone | Disabled |

| TZDB Time Zone | Enabled |

| NTP Server | Enabled |

| Bootfile URL | Enabled |

+ + +

| Interface Name | remote |

| Admin State | Enabled |

| Rapid Commit | Enabled |

| Requested Preferred Lifetime (s) | 0 |

| Requested Valid Lifetime (s) | 0 |

| Option | |

| DNS Server List | Enabled |

| Domain Search List | Enabled |

| Posix Time Zone | Disabled |

| TZDB Time Zone | Enabled |

| NTP Server | Enabled |

| Bootfile URL | Enabled |

+ + +

+ DHCPV6 CLIENT STATE +

| Name | Value |

+ + +

| Interface Name | remote |

| Oper State | Enabled |

| DHCPv6 State | preinit |

| Config State | stateful |

| Renewal (T1) Time (s) | |

| Renewal (T1) Time Remaining (s) | |

| Rebinding (T2) Time (s) | |

| Rebinding (T2) Time Remaining (s) | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  |  |  | | Preferred Lifetime (s) Preferred Lifetime Remaining Valid Lifetime (s)  Valid Lifetime Remaining (s) | (s) | |  |  |  | |  | |  |  |  | |
| |  |  |  |  |  |  |  |  +  | | DHCPv6 Server DUID Option Value  DNS Server List Domain Search List Posix Time Zone TZDB Time Zone  NTP servers Boot File URL  Interface Name |  | |  |  |  |  |  |  |  |  +  | | mgmtbr0 | |  |  |  |  |  |  |  |  +  | |
| **|**  **|**  **|**  | | **Oper State DHCPv6 State Config State**  Renewal (T1) Time (s) |  | **|**  **|**  **|**  | | **Enabled bound stateful**  302400 | **|**  **|**  **|**  | |
| | | Renewal (T1) Time Remaining | (s) | | | 241733 | | |
| | | Rebinding (T2) Time (s) | | | | 453600 | | |
| | | Rebinding (T2) Time Remaining (s) | | | | 392933 | | |
| | | Preferred Lifetime (s) | | | | 604800 | | |
| | | Preferred Lifetime Remaining (s) | | | | 544133 | | |
| | | Valid Lifetime (s) | | | | 604800 | | |
| | | Valid Lifetime Remaining (s) | | | | 544133 | | |
| |  |  |  |  |  |  |  |  + | DHCPv6 Server DUID Option Value  DNS Server List Domain Search List Posix Time Zone TZDB Time Zone  NTP servers Boot File URL | | |  |  |  |  |  |  |  |  + | 0:1:0:1:25:22:d:24:0:0:5e:0:1:81 | |  |  |  |  |  |  |  |  + |

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

* + 1. **SNMP v2c Trap Configuration**

***Objective:***

The objective of this section is to configure SNMP v2c Trap on the SAOS cli.

* + - * Same as the SNMP GET parameters but additional fields are added to specify the Trap target IP.

***Procedure:***

snmp community t1 security-name cienaSecurityV2c text-name cienaV2cCommunity snmp vacm view cienaAll include internet

snmp vacm group cienaGroup access "" v2c no-auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaGroup member cienaSecurityV2c security-model v2c snmp target TestTarget1 target-params TestParamsV2c udp ip 10.176.137.38 snmp target-params TestParamsV2c v2c security-name cienaSecurityV2c snmp target TestTarget1 tag TestTag

snmp notify Test-NOTIFY type trap tag TestTag

***Output:***

* show snmp

+

SNMP NOTIFY +

| Notification Name | Notification Tag | Notification Type |

+ + + +

| Test-NOTIFY | TestTag | trap |

+ + + +

+ SNMP COMMUNITY +

| Community Index | Community Name | Security Name | Transport Tag |

+ + + + +

| t1 | cienaV2cCommunity | cienaSecurityV2c | |

+ + + + +

+ SNMP TARGET-PARAMS +

| Target Param Name | Security Name | User Name | Security Model | Security Level |

+ + + + + +

| TestParamsV2c | cienaSecurityV2c | | v2c | no-auth-no-priv |

+ + +

+

+ + +

SNMP TARGET +

| Target Name | IP Address | Param Name | Tags | UDP Port | Retry Count | Timeout | Prefix Length |

+ + + + + + + + +

| TestTarget1 | 10.176.137.38 | TestParamsV2c | TestTag | 162 | 3 | 1500 | 32 |

+ + + + + + + + +

+ SNMP VACM VIEW +

| Viewtree Name | Subtree | Type |

+ + + +

| cienaAll | internet | include |

+ + + +

+------------ SNMP VACM GROUP MEMBER +

| Group Name | Security Model | Security Name |

+ + + +

| cienaGroup | v2c | cienaSecurityV2c |

+ + +

+

+

SNMP VACM GROUP ACCESS +

| Group Name | Context | Context Match | Security Model | Security Level | Read View | Notify View |

+ + + + + + + +

| cienaGroup | | exact | v2c | no-auth-no-priv | | cienaAll |

+ + + + + + + +

***Test Case Results:***

Passed: Yes No Verified by Date/Time Comments

###### SNMP v2c Inform Configuration

***SNMP v2c Inform:***

* + - * Informs are same as Traps but the main difference is that the Informs are acknowledged back by the SNMP Manager.
      * SNMP Inform are enabled by specifying the type as ‘inform’ whereas type ‘trap’ will be used

for SNMP traps.

***Procedure:***

snmp community t1 security-name cienaSecurityV2c text-name cienaV2cCommunity snmp vacm view cienaAll include internet

snmp vacm group cienaGroup access "" v2c no-auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaGroup member cienaSecurityV2c security-model v2c snmp target TestTarget1 target-params TestParamsV2c udp ip 10.176.137.38 snmp target-params TestParamsV2c v2c security-name cienaSecurityV2c snmp target TestTarget1 tag TestTag

snmp notify Test-NOTIFY1 type inform tag TestTag

***Output:***

* show snmp

+

SNMP NOTIFY +

| Notification Name | Notification Tag | Notification Type |

+ + + +

| Test-NOTIFY1 | TestTag | inform |

+ + + +

+ SNMP COMMUNITY +

| Community Index | Community Name | Security Name | Transport Tag |

+ + + + +

| t1 | cienaV2cCommunity | cienaSecurityV2c | |

+ + + + +

+ SNMP TARGET-PARAMS +

| Target Param Name | Security Name | User Name | Security Model | Security Level |

+ + + + + +

| TestParamsV2c | cienaSecurityV2c | | v2c | no-auth-no-priv |

+ + +

+

+ + +

SNMP TARGET +

| Target Name | IP Address | Param Name | Tags | UDP Port | Retry Count | Timeout | Prefix Length |

+ + + + + + + + +

| TestTarget1 | 10.176.137.38 | TestParamsV2c | TestTag | 162 | 3 | 1500 | 32 |

+ + + + + + + + +

+ SNMP VACM VIEW +

| Viewtree Name | Subtree | Type |

+ + + +

| cienaAll | internet | include |

+ + + +

+------------ SNMP VACM GROUP MEMBER +

| Group Name | Security Model | Security Name |

+ + + +

| cienaGroup | v2c | cienaSecurityV2c |

+ + +

+

+

SNMP VACM GROUP ACCESS +

| Group Name | Context | Context Match | Security Model | Security Level | Read View | Notify View |

+ + + + + + + +

| cienaGroup | | exact | v2c | no-auth-no-priv | | cienaAll |

+ + + + + + + +

***Test Case Results:***

Passed: Yes No Verified by Date/Time Comments

###### SNMP v2c Inform Configuration

***SNMP v2c Inform:***

* + - * Informs are same as Traps but the main difference is that the Informs are acknowledged back by the SNMP Manager.
      * SNMP Inform are enabled by specifying the type as ‘inform’ whereas type ‘trap’ will be used

for SNMP traps.

***Procedure:***

snmp community t1 security-name cienaSecurityV2c text-name cienaV2cCommunity snmp vacm view cienaAll include internet

snmp vacm group cienaGroup access "" v2c no-auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaGroup member cienaSecurityV2c security-model v2c snmp target TestTarget1 target-params TestParamsV2c udp ip 10.176.137.38 snmp target-params TestParamsV2c v2c security-name cienaSecurityV2c snmp target TestTarget1 tag TestTag

snmp notify Test-NOTIFY1 type inform tag TestTag

***Output:***

* show snmp

+

SNMP NOTIFY +

| Notification Name | Notification Tag | Notification Type |

+ + + +

| Test-NOTIFY1 | TestTag | inform |

+ + + +

+ SNMP COMMUNITY +

| Community Index | Community Name | Security Name | Transport Tag |

+ + + + +

| t1 | cienaV2cCommunity | cienaSecurityV2c | |

+ + + + +

+ SNMP TARGET-PARAMS +

| Target Param Name | Security Name | User Name | Security Model | Security Level |

+ + + + + +

| TestParamsV2c | cienaSecurityV2c | | v2c | no-auth-no-priv |

+ + +

+

+ + +

SNMP TARGET +

| Target Name | IP Address | Param Name | Tags | UDP Port | Retry Count | Timeout | Prefix Length |

+ + + + + + + + +

| TestTarget1 | 10.176.137.38 | TestParamsV2c | TestTag | 162 | 3 | 1500 | 32 |

+ + + + + + + + +

+ SNMP VACM VIEW +

| Viewtree Name | Subtree | Type |

+ + + +

| cienaAll | internet | include |

+ + + +

+------------ SNMP VACM GROUP MEMBER +

| Group Name | Security Model | Security Name |

+ + + +

| cienaGroup | v2c | cienaSecurityV2c |

+ + +

+

+

SNMP VACM GROUP ACCESS +

| Group Name | Context | Context Match | Security Model | Security Level | Read View | Notify View |

+ + + + + + + +

| cienaGroup | | exact | v2c | no-auth-no-priv | | cienaAll |

+ + + + + + + +

***Test Case Results:***

Passed: Yes No Verified by Date/Time Comments

###### Create New User Account

***Objective:***

Setup a new user account to access the system.

***Procedure:***

* SAOS 10.1 supports two local user groups:
  + SYSTEM\_ROLE\_DIAG : The user has access to CLI, NETCONF, and also to Linux shell.
  + SYSTEM\_ROLE\_USER : The user has access to CLI and NETCONF.
* Enter the following command on CLI to create a new local user User1:

config

system aaa authentication users user **User1** config username User1 role SYSTEM\_ROLE\_USER password Password1

* Verify that the user has been created:

5162\_001> show aaa users

+ USER ACCOUNT TABLE +

| Username | Role | Sessions | Lockout |

+ + + + +

| diag | SYSTEM\_ROLE\_DIAG | | |

| user | SYSTEM\_ROLE\_USER | | |

| **User1** | SYSTEM\_ROLE\_USER | | |

+ + + + +

* Ensure that the user has been added to NACM group -otherwise provisioning by local user will not be allowed.
  + config
  + nacm groups group super user-name User1

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### DNS Client Setup

***Objective:***

Objective is to verify setting up DNS client

***Procedure:***

* Enter the following command on CLI with an example DNS server 192.168.10.100:

config

*oc-sys:system dns dns-client admin-status enabled*

*oc-sys:system dns dns-client domain-name ott.ciena.com oc-sys:system dns dns-client server 192.168.10.100*

* You should see something like the following:

5170-010> show dns

+ DNS-CLIENT +

| Name | Value |

+ + +

| Admin-status | enabled |

| Domain-name | ott.ciena.com |

| Domain-name-scope | user |

| Server-scope | user |

+ + +

+ USER-SERVERS +

| IP Address | Oper-status |

+ + +

| 192.168.10.100 | enabled |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### ZTP

***Objective:***

Objective is to install SAOS 10.x with ZTP process. Network based ZTP process is useful when we want to ensure the same version of software is automatically installed on multiple nodes in the network. ZTP only allowed over VLAN 127, and untagged is not supported.

***Procedure:***

* Ensure you have DHCP environment setup is been done with either of
  + Option 66/67 to provide tftp server and filename of Command File
  + Option 125 to provide URL of Command Fil
* Ensure that the image you want to download is located on an HTTP/TFTP server
* Verify that the command file is located at the TFTP server and the config file is supplied
* Start the node if it is the first time it is being powered up
* Once the device boots up, Login to UI container using the management IP you checked in the previous step (default login/passwd displayed below):

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

username: diag password: ciena123

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

* + 1. **Verify Re-Install or Upgrade Software**

***Objective:***

Objective is to verify downloading, installation, and activation of software.

***Procedure:***

* Load installation is through ONIE – Open Network Install Environment
* After initial installation of a SAOS load on a box, you should be able to upgrade to another load without need to go back to ONIE.
* \*Following the example below and enter the following command to download the build

from user’s own URL – please note the URL below is for reference only:

software download url [http://x.x.x.x/valimar-snapshot/manifest/saos-10-05-01-](http://x.x.x.x/valimar-snapshot/manifest/saos-10-05-01-0096.yml) [0096.yml](http://x.x.x.x/valimar-snapshot/manifest/saos-10-05-01-0096.yml)

* After the a few minutes, the build should have downloaded successfully. Execute a “show software” to check the download status.
* Once the build has downloaded successfully, execute the command install to install the software.

software install package saos-10-05-01-0096 defer-activation

* \*Once installation is complete, activate the load to complete the upgrade.

software activate package saos-10-05-01-0096

* After the a few minutes, the build should have been activated successfully. Execute a

“show software” to check the status. You should see something like this:

5144-009> show software

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| +  | | Name | | | SOFTWARE STATE  Value | +  | | | |
| +  | | Current operation | +  | | idle | +  | | | |
| |  |  |  |  +  |  |  |  |  | | RPC Status  Running package version Package build info Active bootchain  Components: BIOS image  BOOT FPGA image ONIE image  cn\_alarm\_1 | |  |  |  |  +  |  |  |  |  | | idle  saos-10-05-01-0096  Wed Dec 02 03:16:15 2020  01-05-01-0096  0017  00.00.2a Ciena\_2019.02.01-0040  01-05-01-0096 | autouser | onxvpnjk23 | |  |  |  |  +  |  |  |  |  | |
| | | cn\_central-logger\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_cfm\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_cnfp\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_collectd\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_dataplane\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_dhcp-ctrl\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_dhcpl3relay\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_dns\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_dot1x\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_eoam\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_erps\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_feds\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_hal\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_ipservices\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_lacp\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_lldp\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_ntp\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_pkix\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_pon-ctrl\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_ppm\_1 | | | 01-05-01-0096 |  |  | | |

| cn\_rstp\_1 | 01-05-01-0096 |

| cn\_sat\_1 | 01-05-01-0096 |

| cn\_snmp-agent\_1 | 01-05-01-0096 |

| cn\_storage\_1 | 01-05-01-0096 |

| cn\_svcdirectory\_1 | 01-05-01-0096 |

| cn\_sync-hal\_1 | 01-05-01-0096 |

| cn\_sync\_1 | 01-05-01-0096 |

| cn\_system\_1 | 01-05-01-0096 |

| cn\_tdm\_1 | 01-05-01-0096 |

| cn\_telemetry\_1 | 01-05-01-0096 |

| cn\_twamp\_1 | 01-05-01-0096 |

| cn\_ui\_1 | 01-05-01-0096 |

| cn\_val-gui\_1 | 01-05-01-0096 |

| cn\_ztp\_1 | 01-05-01-0096 |

| xg\_xgrade-agent\_1 | 01-05-01-0096 |

+ + +

| Available packages: | |

**| saos-10-05-01-0096 | activated** |

+ + +

\*can combine the steps and use “software install” without the defer-activation parameter. “software install” will download, install and activate the load on the system in one step.

**Test Case Results:**

Passed: Yes No Verified by Date/Time Comments

###### Verify Manual network-based installation

***Objective:***

Objective is to install SAOS 10.x on a system, using the manual network-based installation.

***Procedure:***

* Login to system console port.
* When ONIE comes up it will try to find the resource for ZTP. If you want to specify the location of the installer file manually, which is different from what it might fetch from network installer, you should stop it:

ONIE:/ # onie-discovery-stop

* Then proceed with the manual installation from the installer file from http, tftp or ftp server.

ONIE:/ # onie-nos-install <http://x.x.x.x/installer.bin> ONIE:/ # onie-nos-install tftp://x.x.x.x/installer.bin ONIE:/ # onie-nos-install ftp://x.x.x.x/installer.bin

Replace x.x.x.x with IP address or the URL of where the image is residing. Here is an example:

ONIE:/ # onie-nos-install <http://x.x.x.x/valimar-> snapshot/17-12-00-0141/meta-onie-installer-dnx/meta\_01-00- 00-0181-core.bin

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Verify USB-based installation of SAOS 10.x

***Objective:***

Objective is to install SAOS 10.x on a system using USB-based method.

***Procedure:***

* Ensure that the format of your USB stick is FAT32 formatted.
* Ensure that the image you want is on the USB stick
* Ensure that the image is named “**onie-installer**”. This is important. Currently, the load name cannot be named anything else.
* Start the node if it is the first time it is being powered up, or follow the following steps otherwise
* Login to UI container using the management IP you checked in the previous step:

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

username: diag password: ciena123

When ONIE comes up it will try to find the resource for ZTP. Wait for the installation to complete from here.

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Verify NTP or verify the date and time

***Objective:***

Setting date and time are required before application of licenses. Set NTP or date for Ciena SAOS 10.x using Linux commands. Proper data and time setup are required for license application.

***CLI NTP Procedure:***

* Establish a ssh connection to ValCLI

ssh [diag@X.X.X.X](mailto:diag@X.X.X.X)

password: ciena123

* Send the following config command
  + config

system ntp associations remote-ntp-server server-entry 10.33.80.21 admin-state enabled

* Check the NTP State with the following command
  + show ntp client
* The output would be something like:

+---------- NTP CLIENT STATE +

| Name | Value |

+ + +

| Admin State | enabled |

| Mode | polling |

| Polling Min Interval | 16 |

| Polling Max Interval | 16 |

| Auth Admin State | disabled |

| Synchronized | True |

| Delay | 62.161 |

| Offset | 0.006 |

| Jitter | 0.017 |

| Drift (PPM) | -4.485 |

+ + +

+--------- NTP CONFIGURED SERVERS +

| Address | Auth Key ID | Admin State |

+ + + +

| 10.33.80.21 | | enabled |

+ + + +

+ NTP OPER SERVERS

+

| Address | Auth Key ID | Server State | Server Condition | Auth State | Offset |

+ + + + +

+ +

| 10.33.80.21 | | reach | syspeer | none

| 0.006 |

+ + + + +

+ +

***Date & Time Set Procedure:***

* Login to UI using the management IP you checked in the previous step:

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

username: diag password: ciena123

* Enter the following command to change the date and time on the system. This will only work if NTP is disabled:

config

system set clock 2018-11-03T18:39:00Z

* Show the system time:

5162-002> show clock

+ System Clock +

| Name | Value |

+ + +

| Current Time | 2018-11-03 18:39:03 UTC |

* To enable NTP, the manually set clock will be overwritten.

config

system ntp admin-state enabled

5162-002> show clock

+ System Clock +

| Name | Value |

+ + +

| Current Time | 2018-11-08 13:22:28 UTC |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Dot1X – Authenticator Setup

***Objective:***

Verify the dot1x Authenticator setup.

Text

Description automatically generated

***Procedure:***

* Enable dot1x globally on system.
  + system dot1x config system-auth-control enabled
* Set the port to “authenticator”.
  + oc-if:interfaces interface 17 config dot1x port- capabilities authenticator true
  + oc-if:interfaces interface 17 config dot1x authenticator admin-status enabled/disabled
* Display Authenticator information.

5162-0028> show dot1x ports auth port 17

+ DOT1X PORT SUMMARY +

| Name | Value |

+ + +

| Port Name | 17 |

| Admin State | Enabled |

| Port Control | Auto |

| ReAuth Enabled | False |

| Quiet Period (sec) | 60 |

| Server Timeout (sec) | 30 |

| ReAuth Period (sec) | 3,600 |

| Max Retries | 2 |

| EAP Version | 2 |

| Control Direction | Both |

| Operational State | Disabled |

| Controlled Port Status | Unauthorized |

| Last EAPOL Frame Version | 0 |

| Last EAPOL Frame Source | 00:00:00:00:00:00 |

+ + +

+

+

DOT1X PORT STATISTICS

| | Eapol | Eapol | Eapol Start | Eapol Logoff | Eapol Resp | Eapol Resp | Eapol Req | Invalid Eapol | Eapol Req | Eapol Length |

| Port | Frame Tx | Frame Rx | Frame Rx | Frame Rx | Id Rx | Rx | Tx | Frame Rx | Id Tx | Error Frames |

+ + + + + + + +

+ + + +

| 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0

| 0 | 0 | 0 |

+ + + + +

+ + +

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Insertion of a FRU

***Objective:***

Verify the insertion of a FRU.

***Procedure:***

* Insert the FRU into the 5171 first slot, and display status. FRU type will automatically get detected on the system
  + show system components component slot1

5171-A> show system components component slot1

+ COMPONENT: SLOT1 +

| Name | Value |

+ + +

| name | slot1 |

| type | openconfig-platform-types:MODULE |

| id | INUIAGTCAA |

| description | slot1 manufactured on 10092019 |

| serial-no | M96DA5A8 |

| part-no | 170-0315-900 |

| fru-type | CFP2-QSFP28 |

| admin-state | enabled |

| module-state | Up |

+ + +

5171-A>

* Display all components of 5171.
  + show system components

5171-A> show system components

+ PLATFORM INFO +

| Name | Value |

+ + +

| name | 5171 |

| type | openconfig-platform-types:CHASSIS |

| id | INMCR00DRA |

| description | 5171 |

| mfg-name | Ciena |

| version | 1 |

| serial-no | M96F06AB |

| part-no | 170-5171-900 |

| base-mac | 20:80:58:81:87:80 |

| status-led | solid-green |

| alarm-led | off |

| psa-led | off |

| psb-led | off |

+ + +

+------- PLATFORM: 5171 +

| Component | Present |

+ + +

| fan-board | yes |

| fan1 | yes |

| fan2 | yes |

| fan3 | yes |

| fan4 | yes |

| fan5 | yes |

| fan6 | yes |

| fan7 | yes |

| fan8 | yes |

| fan9 | yes |

| fan10 | yes |

| fan11 | yes |

| fan12 | yes |

| psu-board | yes |

| psa | yes |

| psb | no |

| cpu1-temperature | yes |

| cpu2-temperature | yes |

| front-temperature | yes |

| switch-temperature | yes |

+ + +

+

+

MODULES

| Slot | Configured-Fru-Type | Admin-State | Fru-Type | Module- State |

+ + + + +

+

| slot1 | CFP2-QSFP28 | enabled | CFP2-QSFP28 | Up

|

| slot2 | qsfp28 | enabled | qsfp28 | Up

|

+ + + + +

+

5171-A>

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Layer 2 Control Protocol

Overview:

L2 control protocol (L2CP) allows the network operator to change the handling of L2 control frames such that they are discarded or forwarded as if they were data frames instead of being processed locally.

When an untagged L2CP frame is received on an ETTP, it is either trapped and sent to an L2 protocol for further processing, that is, peered, or it is treated as L2 data traffic, that is, classified as untagged data traffic. L2CP exposes a mechanism for modifying this default behavior, so that the L2CPs for certain protocols can be discarded or forwarded as L2 data traffic.

L2CP is supported on XGS platforms in SAOS 10.6

Scenario 1: L2CP Handling

Diagram

Description automatically generated with medium confidence

***Objective***

The objective of this test is to create an L2CP profile and apply discard/forward dispositions to L2 protocols.

The default behavior for most Layer 2 control protocols in 10.X is to be forwarded as L2 data. In this scenario, we will apply a discard disposition to 802.1x, link-oam and Cisco-CDP protocols as an example on a 392X device. The control frames will be dropped at the UNI-port.

Procedure

* Create L2CP profile
  + l2cp-profiles l2cp-profile l2cpf1 protocol-disposition port-auth

untagged-disposition discard/forward protocol-disposition cisco-cdp untagged-disposition discard/forward protocol-disposition link-oam untagged-disposition discard/forward

* Attach an L2 control plane profile to a forwarding domain
  + fds fd FD1
  + mode vpls vlan-id 20(The FD is created without vlan-id on DNX)
  + l2cp-profile l2cpf1
* Create Untagged and L2CP classifier
  + classifiers classifier untagged filter-entry vtag-stack untagged-exclude-priority-tagged true
  + classifiers classifier class\_l2cp filter-entry vtag-stack l2cp-exclude-priority true
* Create flow point and add the untagged and l2cp classifier to the flow-point
  + fps fp l2cp4 fd-name FD1 logical-port 4

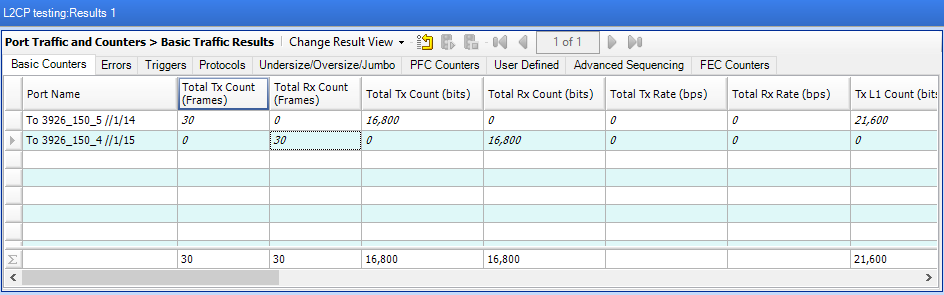
classifier-list untagged classifier-list class\_l2cp

ingress-l2-transform push-vid-400 vlan-stack 1 push-tpid tpid-8100 push-vid 20

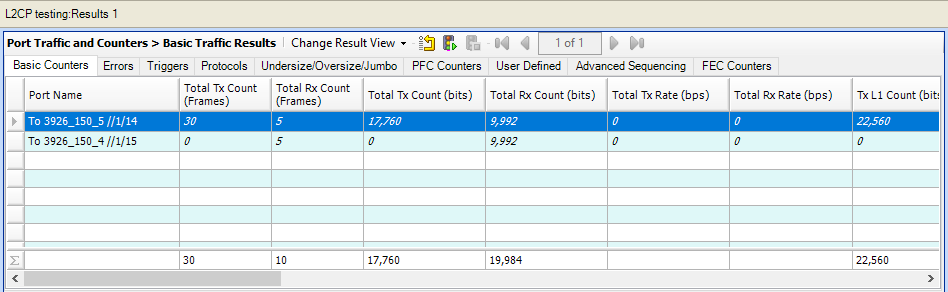
exit exit

egress-l2-transform pop-vid-20vlan-stack 1 pop-type

Before applying the l2cp profile, L2CP frames sent from one test port are forwarded and received on the other port.



After applying the “discard disposition” under L2CP profile, we can see that L2 control frames are no longer received on the other side of the test set as they get dropped at the UNI-port of device.



3926-150> show ettps ettp 4 statistics

+ ETTP STATISTICS +

| KEY | VALUE |

+ + +

| Name | 4 |

| | |

| In Bytes | 2100 |

| In Packets | 30 |

| In Broadcast Packets | 0 |

| Out Bytes | 503 |

| In Multicast Packets | 30 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| | | Out Packets | | | 3 | | |
| | | Out Unicast Packets | | | 0 | | |
| | | In Errors | | | 0 | | |
| | | Out Errors | | | 0 | | |
| | | Out Broadcast Packets | | | 0 | | |
| | | In Undersize Packets | | | 0 | | |
| | | Out Multicast Packets | | | 3 | | |
| | | In 64 Octet Packets | | | 0 | | |
| | | In 65 to 127 Octet Packets | | | 30 | | |
| | | In 128 to 255 Octet Packets | | | 0 | | |
| | | In 256 to 511 Octet Packets | | | 0 | | |
| | | In 512 to 1023 Octet Packets | | | 0 | | |
| | | In 1024 to 1518 Octet Packets | | | 0 | | |
| | | In 1519 to 2047 Octet Packets | | | 0 | | |
| | | In 2048 to 4095 Octet Packets | | | 0 | | |
| | | In 4096 to 9216 Octet Packets | | | 0 | | |
| | | Out 1519 to 2047 Octet Packets | | | 0 | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| | | Out 2048 to 4095 Octet | Packets | | | 0 | | |
| | | Out 4096 to 9216 Octet | Packets | | | 0 | | |
| | | In Oversize Packets |  | | | 0 | | |
| | | In Jabber Packets |  | | | 0 | | |
| | | In Crc Error Packets |  | | | 0 | | |
| | | Link Flap Events |  | | | 0 | | |
| | | Out Discards |  | | | 0 | | |
| | | In Unicast Packets |  | | | 0 | | |
| | | **In Discards Packets** |  | **|** | **30** | | |
| + |  |  | + |  | + |

L2CP configuration can be displayed by executing the commands below.

3926-150> show flow-points flow-point l2cp4

+ FLOW POINT +

| KEY | VALUE |

+ + +

| Name | l2cp4 |

| Forwarding Domain Name | FD1 |

| Logical Port | 4 |

| MTU Size | 2000 |

| Ingress L2 Transform | |

| Ingress Name | push-vid-20 |

| Ingress VLAN Stack | |

| Tag | 1 |

| Push TPID | tpid-8100 |

| Push VID | 20 |

| Egress L2 Transform | |

| Egress Name | pop-vid-20 |

| Egress VLAN Stack | |

| Tag | 1 |

| Pop Type | - |

| Classifier List | |

| | **untagged** |

| | **class\_l2cp** |

+ + +

+ FLOW POINT STATISTICS +

| KEY | VALUE |

+ + +

| Name | l2cp4 |

+ + +

3926-150> show classifiers

+ CLASSIFIER +

| Name | Filter Parameter |

+ + +

| **class\_l2cp | Classifier:untagged** |

| default-vid-127 | Classifier:tagged-all |

| **untagged | Classifier:untagged** |

+ + +

3926-150> show l2cp-profiles l2cp-profile l2cpf1

+ L2CP PROFILE +

| KEY | VALUE |

+ + +

| Name | l2cpf1 |

| Protocol Disposition | |

| Protocol | **port-auth** |

| Untagged Disposition | **discard** |

| | |

| Protocol | **cisco-cdp** |

| Untagged Disposition | **discard** |

| | |

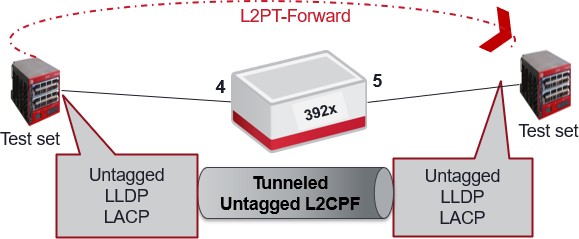
| Protocol | **link-oam** |

| Untagged Disposition | **discard** |

+ + +

Scenario 2: L2PT (Layer 2 Protocol Tunneling)

Layer 2 protocol tunneling is supported in 10.6 on DNX and XGS platforms. L2PT form requires that the frame’s original MAC DA get replaced with a configurable L2PT MAC address. In the reverse direction L2PT MAC address is replaced with proper IEEE or Cisco MAC DA.



***Objective:***

The objective of this test is to configure L2PT disposition for LACP, LACP Marker and LLDP as these protocols have a default “Peering” disposition. After provisioning the L2PT form, L2 protocol frames will be forwarded to the other test set instead of being processed on 392X device.

***Procedure***

* Create the L2PT MAC list with l2pt destination MAC
  + l2cp-profiles l2pt-macs 01:00:0C:CD:CD:D0
* Create the L2 control protocol profile
  + l2cp-profiles l2cp-profile l2cpf1
* Provision the forwarding-domain, classifiers and flow-point
  + fds fd FD1 mode vpls vlan-id 20 l2cp-profile l2cpf1
  + classifiers classifier untagged filter-entry vtag-stack untagged-exclude-priority-tagged true
  + classifiers classifier class\_l2cp filter-entry vtag-stack l2cp-exclude-priority true
  + fps fp l2cp4fd-name FD1 logical-port 4 classifier-list untagged

classifier-list class\_l2cp

ingress-l2-transform push-vid-20 vlan-stack 1 push-tpid tpid-8100 push-vid 20

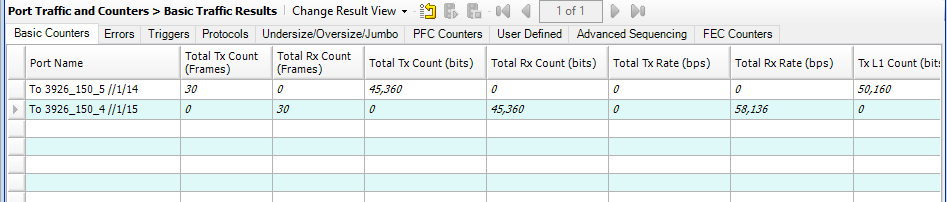
exit exit

egress-l2-transform pop-vid-20 vlan-stack 1 pop-type

The steps below should be provisioned under the l2cp profile:

* Set the protocol in the protocol-disposition
  + protocol-disposition lldp
  + protocol-disposition lacp
  + protocol-disposition lamp
* Set the L2PT MAC address for the protocol for which L2PT forwarding needs to be enabled. This should be same MAC that is added in l2pt-macs list:
  + l2pt-mac 01:00:0C:CD:CD:D0
* Set the untagged disposition as “l2pt-forward”:
  + untagged-disposition l2pt-forward

After applying the “l2pt-forward disposition” under L2CP profile, we can see that L2 control frames (LACP/LLDP/LACP Marker) are now l received on the other side of the test without getting processed on the device.



L2CP configuration can be displayed by executing the commands below.

3926-150> show l2cp-profiles l2cp-profile l2cpf1

+ L2CP PROFILE +

| KEY | VALUE |

+ + +

| Name | l2cpf1 |

| Protocol Disposition | |

| Protocol | lldp |

| Untagged Disposition | **l2pt-forward** |

| L2PT MAC Address | **01:00:0c:cd:cd:d0** |

| | |

| Protocol | lacp |

| Untagged Disposition | **l2pt-forward** |

| L2PT MAC Address | **01:00:0c:cd:cd:d0** |

| | |

| Protocol | lamp |

| Untagged Disposition | **l2pt-forward** |

| L2PT MAC Address | **01:00:0c:cd:cd:d0** |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Configure G.8275.2 T-GM

***Objective:***

The objective of this test is to configure an G.8275.2 T-GM. A G.8275.2 T-GM configuration is similar to a 8275.1 T-GM, but It requires an IP interface to be configured.

***Topology:***

Antenna connected to the GNSS input (SMB antenna input).

***Procedure:***

The prerequisite for this test is to enable the GNSS.

1. Set the PTP global parameters to a G.8275.2 profile and a GM clock type.

sync global network-option option-1 sync global reversion-mode revertive sync global wait-to-restore 0

sync ptp-global profile g.8275.2

sync ptp-global clock-type gm sync ptp-global protocol-version 2

sync ptp-global timestamp-mode one-step sync ptp-global max-global-session 44 sync ptp-global dscp 41

sync ptp-global ttl 255

1. Configure an IP interface. Note: The interface used below in on logical port 2.

classifiers classifier vlan501 filter-entry vtag-stack vtags 1 vlan-id 501 fds fd VLAN501 mode vpls

fps

fp VLAN501

stats-collection on fd-name VLAN501 logical-port 2

classifier-list-precedence 7 classifier-list vlan501

mtu-size 9216

egress-l2-transform push-vid-501 vlan-stack 1

push-tpid tpid-8100 push-vid 501

exit exit exit Exit

oc-if:interfaces interface if2 config name if2 vrfName default cn-if:type ip mtu 1500 admin-status true underlay-binding config fd VLAN501

oc-if:interfaces interface if2 ipv4 addresses address 20.20.20.1 config ip

20.20.20.1 prefix-length 24

1. Configure PTP outputs.

sync output-references ptp-output-reference PTP-Out interface if2 sync output-references ptp-output-reference PTP-Out max-grant-rate 64

sync output-references ptp-output-reference PTP-Out signalling on

***Expected Results:***

PTP outputs should be active.

show sync ptp output-references

+------------ SYNC PTP OUTPUT REFERENCES +

| Name | Interface | Oper State | PTP Port State |

+ + + + +

| PTP-Out | if2 | Up | Master |

+ + + + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

* + 1. MEP Support on QinQ

**CFM/Y.1731 PDU’s with l2-transform on MEP and flow-point**

Outgoing CFM or y.1731 pdu’s can be untagged, single tagged or double tagged. Tag on packet is determined by l2-transform configured on the MEP and egress/ingress transform configured on the fp on which the MEP is created.

From 10.7.0 onwards, all types of ingress and egress transforms will be applicable to the UP

MEP. The packet format for all types of CFM PDU’s will be same as the data traffic.

Xform on MEP : Dual-Tagged

The input packet format with MEP transform applied from CFM application :

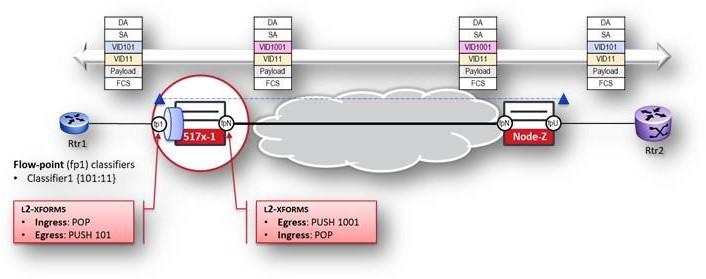
|  |  |  |  |
| --- | --- | --- | --- |
| **DA - SA** | **TAG1** | **TAG2** | **CFM PDU** |

Example configuration for l2-transfrom on the MEP(double-tagged).

***Objective:***

The objective of this test is to create UP MEP L2-transform with double tag.

***Topology:***



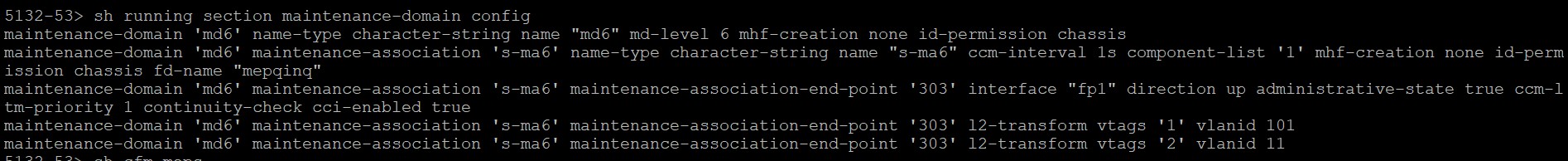
***Procedure:***

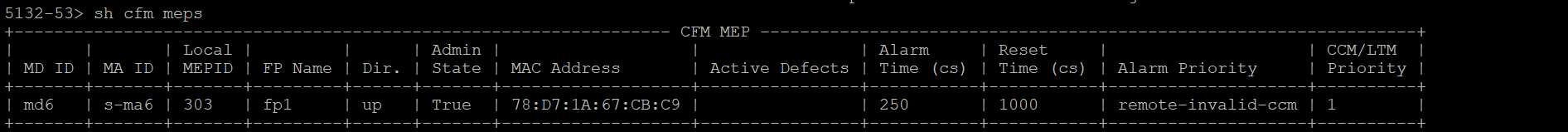
***Please note the configuration below highlights the configuration on one of the nodes 517x-1 from the above-mentioned topology***

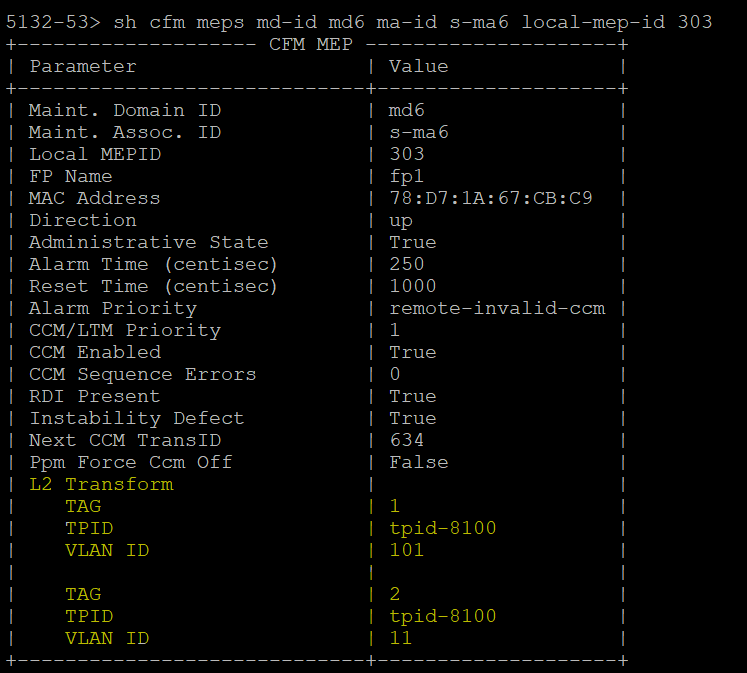
**Test Case Results:**

Passed: Yes No Verified by Date/Time Comments

###### Verification







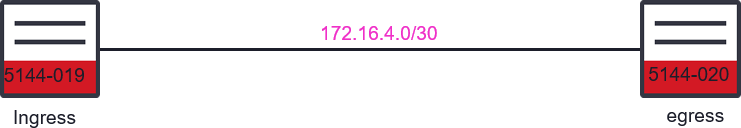
Test Case Results:

Passed: Yes Verified by Date/Time Comments

###### MPLS-TP Static Tunnel – LSP BFD – Hardware acceleration

***Objective:***

Validate that LSP BFD session can be enabled on MPLS-TP tunnel. Also test hardware acceleration on the LSP BFD session. Only supported on 51xx devices.



***Procedure:***

* Create static MPLS-TP tunnel with LSP BFD session – hardware acceleration disabled.
  + config

## Ingress Node

tp-corouted-tunnels tunnel to5144-20-b 192.168.44.236 192.168.44.237

tunnel-type static-ingress-corouted forward-out-segment forward-out-label 30

forward-out-segment next-hop-ip 172.16.4.2

reverse-in-segment reverse-in-label 31

source-tunnel-id 30

destination-tunnel-id 31

bfd-cfg-parms admin-down false **bfd-cfg-parms accelerate false** exit

exit

##Egress Node

tp-corouted-tunnels tunnel to5144-20-b 192.168.44.236 192.168.44.237

tunnel-type static-egress-corouted reverse-out-segment reverse-out-label 31

reverse-out-segment prev-hop-ip 172.16.4.1

forward-in-segment forward-in-label 30

source-tunnel-id 30

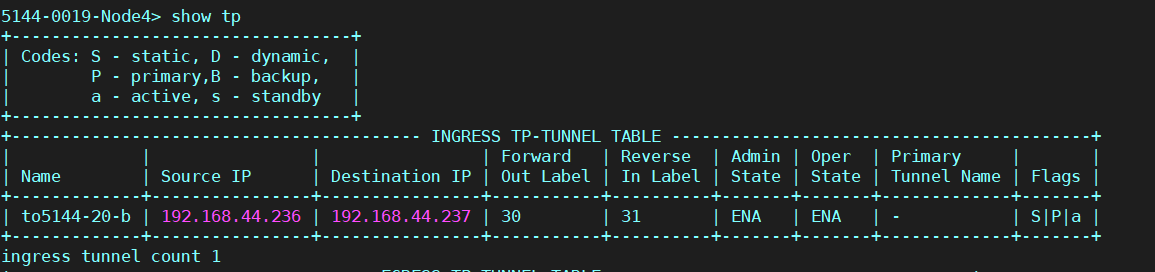
destination-tunnel-id 31 bfd-cfg-parms admin-down false **bfd-cfg-parms accelerate false** exit

exit

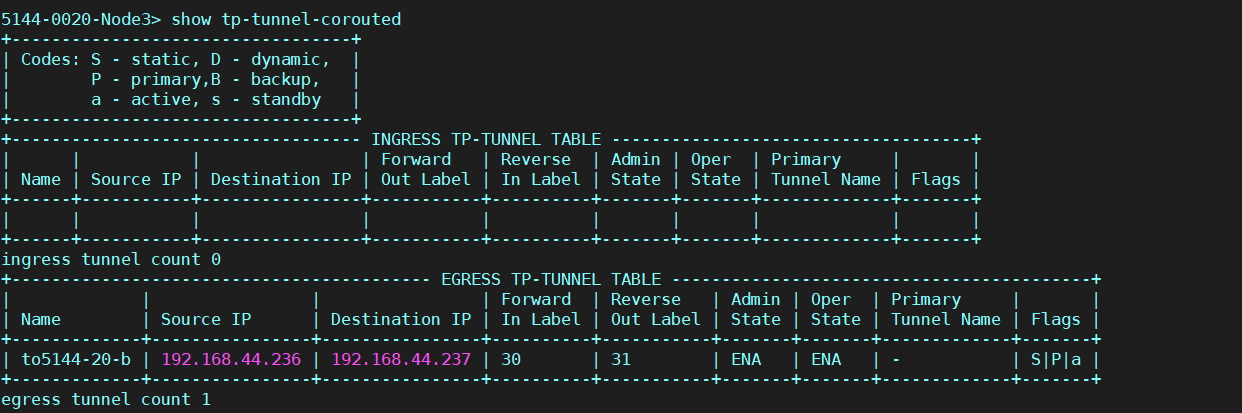
* Validate that the BFD session is not hardware accelerated, and the MPLS-TP tunnel is operational

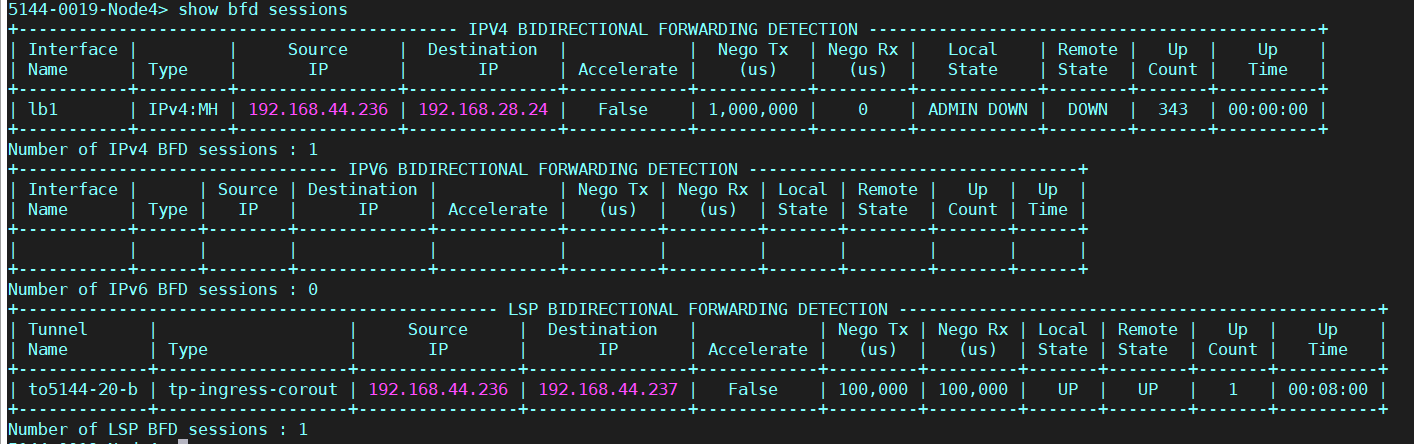
Local Node

* show tp-tunnel-corouted

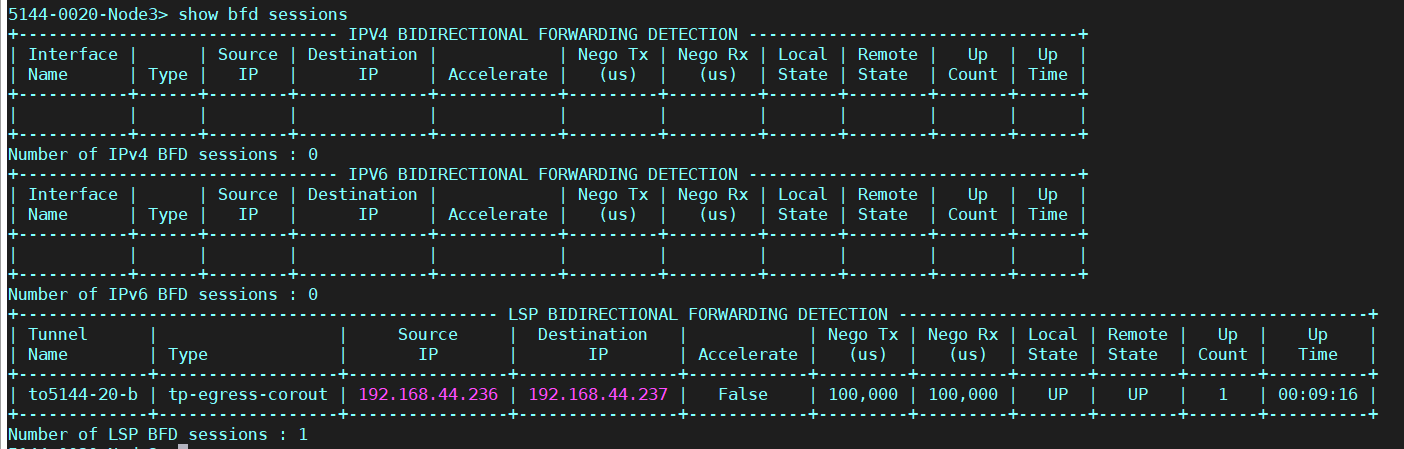


Remote Node



* + show bfd sessions Local Node

Remote Node



* Set the hardware acceleration to enabled – must admin-disable the BFD session first.

##Ingress Node

tp-corouted-tunnels tunnel to5144-20-b 192.168.44.236 192.168.44.237

bfd-cfg-parms statistics-collection on

bfd-cfg-parms admin-down true bfd-cfg-parms accelerate true

bfd-cfg-parms required-min-rx-interval 3300

bfd-cfg-parms desired-min-tx-interval 3300 apply

bfd-cfg-parms admin-down false

apply

exit exit

##Egress Node

tp-corouted-tunnels tunnel to5144-20-b 192.168.44.236 192.168.44.237

tunnel-type static-egress-corouted

bfd-cfg-parms statistics-collection on

bfd-cfg-parms admin-down true bfd-cfg-parms accelerate true

bfd-cfg-parms required-min-rx-interval 3300

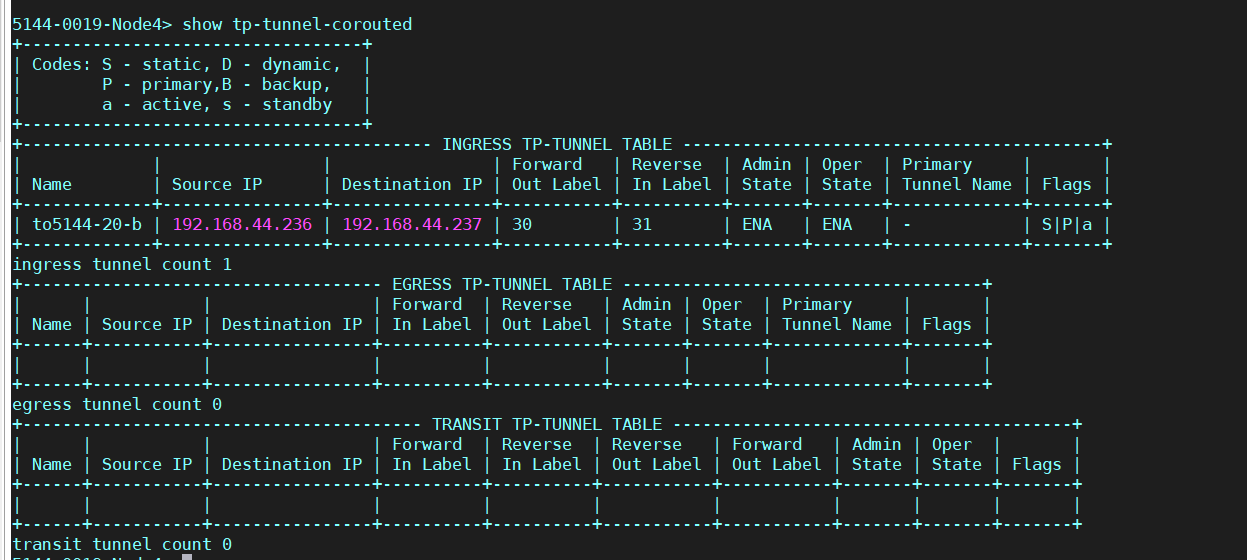
bfd-cfg-parms desired-min-tx-interval 3300 apply

bfd-cfg-parms admin-down false

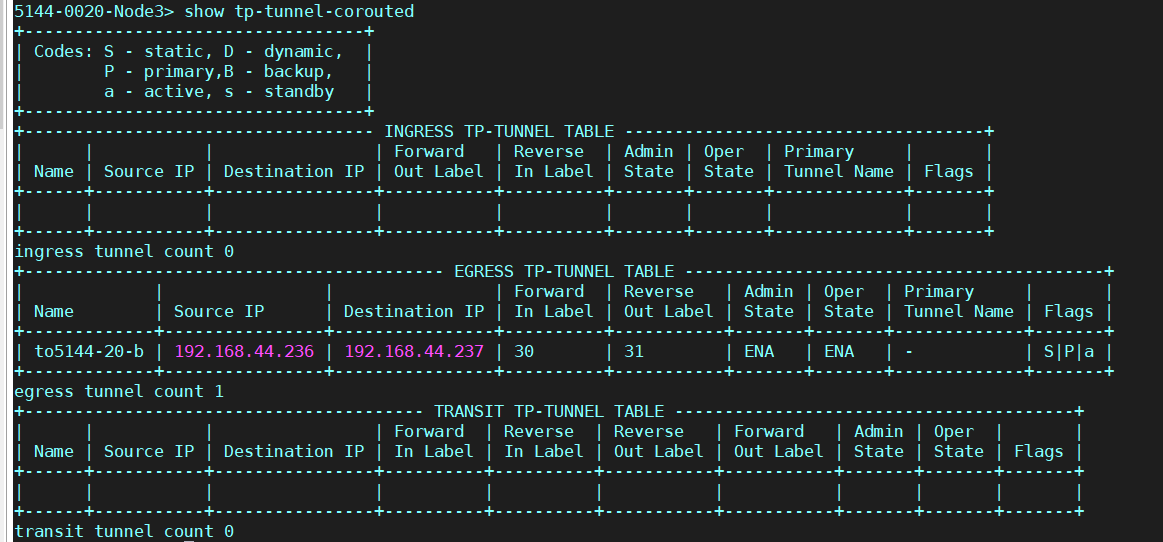
apply exit exit

* Validate that the MPLS-TP tunnel and the hardware accelerated bfd session are up.
  + show tp-tunnel-corouted

Local Node:

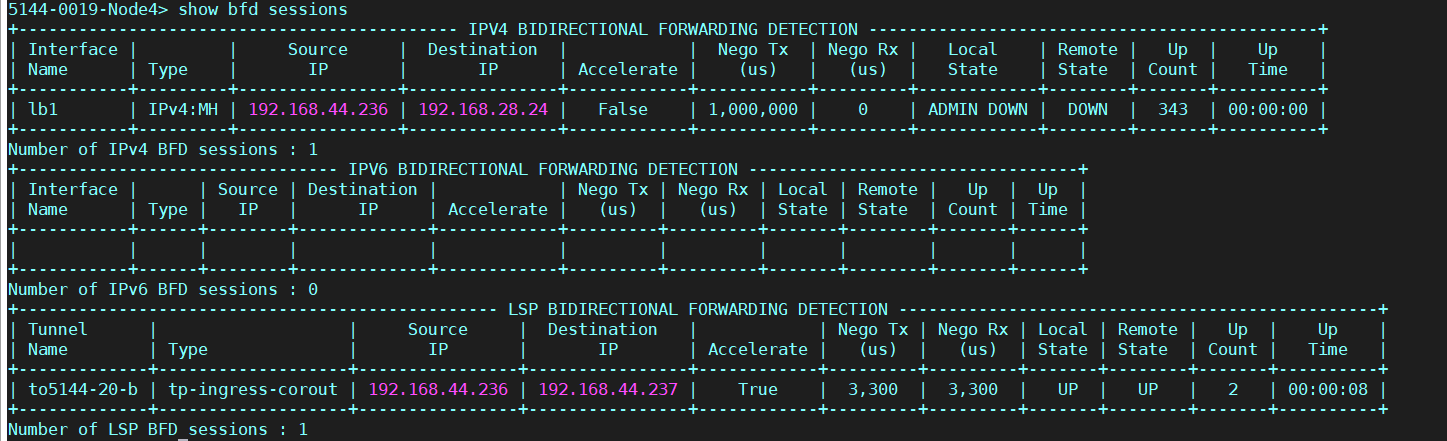


**Remote Node:**

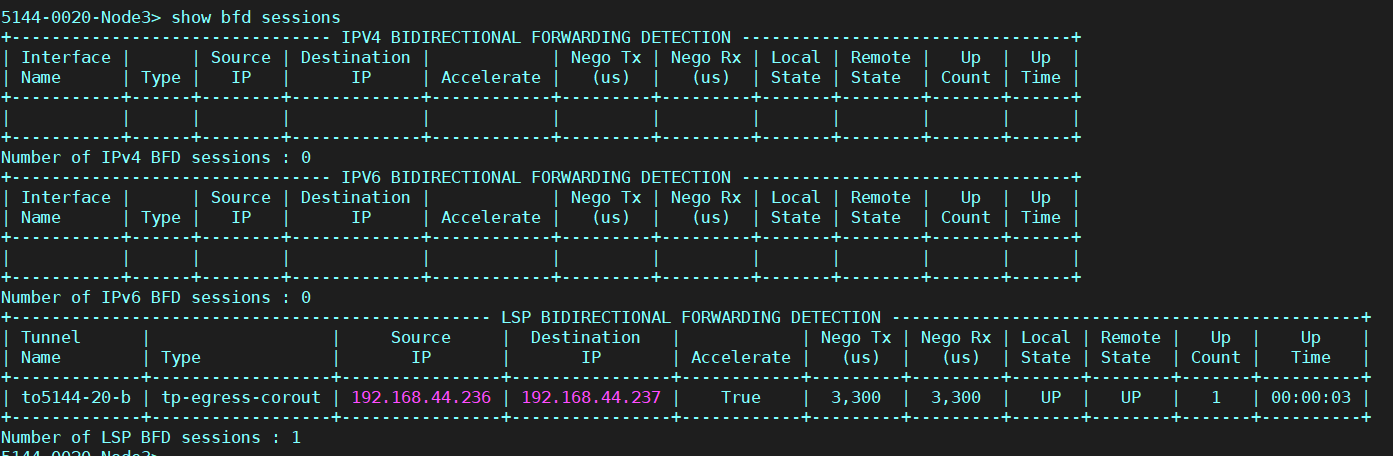


>show bfd sessions

**Local Node:**



**Remote Node:**



**Test Case Results:**

Passed: Yes No Verified by Date/Time Comments

###### Dynamic PWE – WTR

***Objective:***

Verify provisioning of WTR parameter.

***Procedure:***

* Go to the configuration terminal and provision the protected PWE.
  + config

pseudowires pseudowire PW1 mode spoke protect true role primary configured-pw peer-ip 192.168.28.24 pw-id 100

pseudowires pseudowire bkPW1 mode spoke protect true role backup primary-pw PW1 configured-pw peer-ip 192.168.28.78 pw-id 200

l2vpn-services l2vpn service1 signaling-type ldp pseudowire PW1

pseudowire bkPW1 forwarding-domain hvpls exit

exit

* Validate the PWE, note that PWE reversion is not set – ie: no reversion – even though the WTR is set to 30sec by default.

5144-0019-Node4> show pseudowires pseudowire PW1

+ PSEUDOWIRES STATE

+

| KEY | VALUE |

+ +

+

| PW Id | 100 |

| Name | PW1 |

| Peer IP | 192.168.28.24 |

| Oper State | DOWN |

| In Label | 52002 |

| Out Label | 52000 |

| Mode | Spoke |

| PW Role | Primary |

| PW Type | Dynamic |

| Service Type | ethernet |

| Protection State | passive |

| Remote PW Status | pseudowire-forwarding |

| Local PW Status | pseudowire-not-forwarding |

| Statistics Collection | Off |

| PW Load Balance | disabled |

| Operational Fat | None |

| Configured CW | non-preferred |

| Operational CW | OFF |

| Operational CC Type | cctype-4 |

| MTU | 1500 |

| Tunnel Type | OSPF-SR |

| Reversion Hold Time | 30 sec |

**| Configured PW-Reversion | none |**

| Manual Switchover | False |

| Ignore MTU Mismatch | False |

| MS-PW ID | NONE |

| MAC Withdraw | True |

| PW Fault Reason | no-fault |

| PW Status Local Refresh Timer | 600 sec |

+ +

+

* Configure the primary PWE so that the PWE reversion is enabled, and the Reversion Hold Time (WTR) is set to 300sec.

pseudowires pseudowire PW1 pw-reversion enabled pseudowires pseudowire PW1 reversion-hold-time 300

* Validate pseudowire, now pseudowire will revert to primary PWE when the fault recovers and the WTR hold timer expires.

5144-0019-Node4> show pseudowires pseudowire PW1

+ PSEUDOWIRES STATE +

| KEY | VALUE |

+ + +

| PW Id | 100 |

| Name | PW1 |

| Peer IP | 192.168.28.24 |

| Oper State | UP |

| In Label | 52002 |

| Out Label | 52000 |

| Mode | Spoke |

| PW Role | Primary |

| PW Type | Dynamic |

| Service Type | ethernet |

| Protection State | active |

| Remote PW Status | pseudowire-forwarding |

| Local PW Status | pseudowire-forwarding |

| Statistics Collection | Off |

| PW Load Balance | disabled |

| Operational Fat | None |

| Configured CW | non-preferred |

| Operational CW | OFF |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| | | Operational CC | Type | | | | cctype-4 | | |
| |  |  **|** | MTU  Tunnel Type  **Reversion Hold** | **Time** | |  |  **|** | | 1500  OSPF-SR  **300 sec** | |  |  **|** |
| **|**  |  |  |  |  |  |  + | **Configured PW-Reversion** Manual Switchover Ignore MTU Mismatch  MS-PW ID  MAC Withdraw  PW Fault Reason  PW Status Local Refresh | | Timer | **|**  |  |  |  |  |  |  + | **enabled** False False NONE  True  no-fault 600 sec | |  |  |  |  |  |  |  + |

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### FAT PW Configuration

***Objective:*** Objective of this section is to provide a breakdown of step by step configuration on each node that needs to be performed to enable FAT PW feature.

* LAG configuration
* Forwarding domain, flow points configuration
* IP interfaces configuration
* IGP such as ISIS or OSPF configuration (we are using ISIS L1 for our test purpose)
* LDP & MPLS configuration
* Targeted LDP and pseudo wire configuration
* FAT capability enable within pseudo wire context
* L2VPN service creation, associating it to attachment circuit & pseudowire
* Attachment circuit creation to transmit CE traffic over L2VPN infrastructure

***Procedure:***

***5170-0037 (PE1) Node:***

config

**# LAG Configuration**

oc-if:interfaces interface PE1-P1-LAG config name PE1-P1-LAG cn- if:type lag

oc-if:interfaces interface PE1-P1-LAG config agg agg-admin-mode agg-mode-lacp

oc-if:interfaces interface PE1-P1-LAG config agg member-ports 17 oc-if:interfaces interface PE1-P1-LAG config agg member-ports 18 exit

exit exit exit exit

oc-if:interfaces interface PE1-P1-LAG config agg member-ports 18 exit

exit

exit exit exit

**# NNI Port Classifier**

classifiers classifier vlan101 filter-entry vtag-stack vtags 1 vlan-id 101

**# FD**

fds fd fat-pw-fd mode vpls

**# FP**

fps

fp fat-pw-fp

fd-name fat-pw-fd logical-port PE1-P1-LAG stats-collection on

classifier-list-precedence 7 classifier-list vlan101

mtu-size 9216

egress-l2-transform push-vid-101 vlan-stack 1

push-tpid tpid-8100 push-vid 101

exit exit exit exit

**# IP Interfaces**

oc-if:interfaces interface PE1-P1-LAG-intr config name PE1-P1-LAG- intr cn-if:type ip admin-status true mtu 1500 underlay-binding config fd fat-pw-fd

oc-if:interfaces interface PE1-P1-LAG-intr ipv4 addresses address

11.11.11.1 config ip 11.11.11.1 prefix-length 24

oc-if:interfaces interface lb1 config name lb1 cn-if:type loopback

oc-if:interfaces interface lb1 ipv4 addresses address 37.37.37.1 config ip 37.37.37.1 prefix-length 32

**# ISIS Config**

isis instance 100 net 49.BBBB.0370.3703.7001.00 isis instance 100 level-type level-1

isis instance 100 interfaces interface lb1 exit

exit

interfaces interface PE1-P1-LAG-intr

exit exit exit exit

**# ISIS Interfaces**

isis instance 100 interfaces interface PE1-P1-LAG-intr level-type level-1

isis instance 100 interfaces interface lb1 level-type level-1

**# LDP**

ldp instance default lsr-id 37.37.37.1

ldp instance default interfaces interface lb1 enable-ipv4 true

ldp instance default interfaces interface PE1-P1-LAG-intr enable- ipv4 true

**# MPLS Label Switching**

mpls interfaces interface lb1 label-switching true

mpls interfaces interface PE1-P1-LAG-intr label-switching true

**# Targeted LDP for PW**

ldp instance default target-ldp peers 39.39.39.1 exit

exit exit exit

**# VPWS Dynamic PW**

pseudowires

pseudowire pe1\_pe2\_spoke\_pw1 mode spoke

pw-loadbalance fat-pw fat-capability tx-rx configured-pw

pw-id 1

peer-ip 39.39.39.1 exit

exit exit

**# UNI Port**

# Classifier

classifiers classifier vlan102 filter-entry vtag-stack vtags 1 vlan-id 102

**# FD**

fds fd AC\_UNI\_FD1 mode vpws

**# FP**

fps

fp AC\_UNI\_FP1 stats-collection on fd-name AC\_UNI\_FD1 logical-port 10

mtu-size 2000

cos-to-frame-map default-c2f frame-to-cos-map default-f2c classifier-list-precedence 102 classifier-list vlan102

exit exit

**# L2VPN**

l2vpn-services l2vpn L1

forwarding-domain AC\_UNI\_FD1 pseudowire pe1\_pe2\_spoke\_pw1 service-type vlan

signaling-type ldp mtu 1500

exit exit

**#REMOVE L2vpn services (this config is shared for reference only if end user wants to remove L2VPN)**

config t

no l2vpn-services no pseudowires

no ldp instance default target-ldp peers 4.4.4.4

***5170-0038 (P1) Node:***

**#P1:**

**# LAG Configuration**

config

oc-if:interfaces interface PE1-P1-LAG config name PE1-P1-LAG cn-if:type lag

oc-if:interfaces interface PE1-P1-LAG config agg agg-admin-mode agg-mode- lacp

oc-if:interfaces interface PE1-P1-LAG config agg member-ports 17 oc-if:interfaces interface PE1-P1-LAG config agg member-ports 18 exit

exit exit exit

oc-if:interfaces interface PE1-P1-LAG config agg member-ports 18

exit exit exit exit exit

**# NNI Port Classifier**

classifiers classifier vlan101 filter-entry vtag-stack vtags 1 vlan-id 101

**# FD**

fds fd fat-pw-fd mode vpls

**# FP**

fps

fp fat-pw-fp

fd-name fat-pw-fd logical-port PE1-P1-LAG stats-collection on

classifier-list-precedence 7 classifier-list vlan101

mtu-size 9216

egress-l2-transform push-vid-101 vlan-stack 1

push-tpid tpid-8100 push-vid 101

exit exit exit exit

**# IP Interfaces**

oc-if:interfaces interface PE1-P1-LAG-intr config name PE1-P1-LAG-intr cn- if:type ip admin-status true mtu 1500 underlay-binding config fd fat-pw- fd

oc-if:interfaces interface PE1-P1-LAG-intr ipv4 addresses address

11.11.11.2 config ip 11.11.11.2 prefix-length 24

oc-if:interfaces interface lb1 config name lb1 cn-if:type loopback

oc-if:interfaces interface lb1 ipv4 addresses address 38.38.38.1 config ip 38.38.38.1 prefix-length 32

**#P1 to PE2 config part # LAG Configuration** config

oc-if:interfaces interface P1-PE2-LAG config name P1-PE2-LAG cn-if:type lag

oc-if:interfaces interface P1-PE2-LAG config agg agg-admin-mode agg-mode- lacp

oc-if:interfaces interface P1-PE2-LAG config agg member-ports 37 oc-if:interfaces interface P1-PE2-LAG config agg member-ports 38 exit

exit exit exit exit

**# NNI Port Classifier**

classifiers classifier vlan90 filter-entry vtag-stack vtags 1 vlan-id 90

**# FD**

fds fd fat-pw-fd-2 mode vpls

**# FP**

fps

fp fat-pw-fp-2

fd-name fat-pw-fd-2 logical-port P1-PE2-LAG stats-collection on

classifier-list-precedence 7 classifier-list vlan90

mtu-size 9216

egress-l2-transform push-vid-90 vlan-stack 1

push-tpid tpid-8100 push-vid 90

exit exit exit exit

**# IP Interfaces**

oc-if:interfaces interface P1-PE2-LAG-intr config name P1-PE2-LAG-intr cn- if:type ip admin-status true mtu 1500 underlay-binding config fd fat-pw- fd-2

oc-if:interfaces interface P1-PE2-LAG-intr ipv4 addresses address

10.10.11.1 config ip 10.10.11.1 prefix-length 24

**# ISIS Config**

isis instance 100 net 49.BBBB.0380.3803.8001.00 isis instance 100 level-type level-1

isis instance 100 interfaces interface lb1 exit

exit

interfaces interface PE1-P1-LAG-intr

exit exit exit

interfaces interface P1-PE2-LAG-intr exit

exit exit exit

**# ISIS Interfaces**

isis instance 100 interfaces interface PE1-P1-LAG-intr level-type level-1 isis instance 100 interfaces interface P1-PE2-LAG-intr level-type level-1 isis instance 100 interfaces interface lb1 level-type level-1

**# LDP**

ldp instance default lsr-id 38.38.38.1

ldp instance default interfaces interface lb1 enable-ipv4 true

ldp instance default interfaces interface PE1-P1-LAG-intr enable-ipv4 true ldp instance default interfaces interface P1-PE2-LAG-intr enable-ipv4 true

**# MPLS Label Switching**

mpls interfaces interface lb1 label-switching true

mpls interfaces interface PE1-P1-LAG-intr label-switching true mpls interfaces interface P1-PE2-LAG-intr label-switching true

***5170-0039 (PE2) Node:***

**# LAG Configuration**

config

oc-if:interfaces interface P1-PE2-LAG config name P1-PE2-LAG cn-if:type lag

oc-if:interfaces interface P1-PE2-LAG config agg agg-admin-mode agg-mode- lacp

oc-if:interfaces interface P1-PE2-LAG config agg member-ports 17 oc-if:interfaces interface P1-PE2-LAG config agg member-ports 18 exit

exit exit exit exit

**# NNI Port Classifier**

classifiers classifier vlan90 filter-entry vtag-stack vtags 1 vlan-id 90

**# FD**

fds fd fat-pw-fd-2 mode vpls

**# FP**

fps

fp fat-pw-fp-2

fd-name fat-pw-fd-2 logical-port P1-PE2-LAG stats-collection on

classifier-list-precedence 7 classifier-list vlan90

mtu-size 9216

egress-l2-transform push-vid-90 vlan-stack 1

push-tpid tpid-8100 push-vid 90

exit exit exit exit

**# IP Interfaces**

oc-if:interfaces interface P1-PE2-LAG-intr config name P1-PE2-LAG-intr cn- if:type ip admin-status true mtu 1500 underlay-binding config fd fat-pw- fd-2

oc-if:interfaces interface P1-PE2-LAG-intr ipv4 addresses address

10.10.11.2 config ip 10.10.11.2 prefix-length 24

oc-if:interfaces interface lb1 config name lb1 cn-if:type loopback

oc-if:interfaces interface lb1 ipv4 addresses address 39.39.39.1 config ip 39.39.39.1 prefix-length 32

**# ISIS Config**

isis instance 100 net 49.BBBB.0390.3903.9001.00 isis instance 100 level-type level-1

isis instance 100 interfaces interface lb1 exit

exit

interfaces interface P1-PE2-LAG-intr exit

exit exit exit

**# ISIS Interfaces**

isis instance 100 interfaces interface P1-PE2-LAG-intr level-type level-1 isis instance 100 interfaces interface lb1 level-type level-1

**# LDP**

ldp instance default lsr-id 39.39.39.1

ldp instance default interfaces interface lb1 enable-ipv4 true

ldp instance default interfaces interface P1-PE2-LAG-intr enable-ipv4 true

**# MPLS Label Switching**

mpls interfaces interface lb1 label-switching true

mpls interfaces interface P1-PE2-LAG-intr label-switching true

**# Targeted LDP for PW**

ldp instance default target-ldp peers 37.37.37.1

exit exit exit exit

**# VPWS Dynamic PW**

pseudowires

pseudowire pe1\_pe2\_spoke\_pw1 mode spoke

pw-loadbalance fat-pw fat-capability tx-rx configured-pw

pw-id 1

peer-ip 37.37.37.1 exit

exit exit

**# UNI Port**

**# Classifier**

classifiers classifier vlan103 filter-entry vtag-stack vtags 1 vlan-id 103

**# FD**

fds fd AC\_UNI\_FD1 mode vpws

**# FP**

fps

fp AC\_UNI\_FP1 stats-collection on fd-name AC\_UNI\_FD1 logical-port 10

mtu-size 2000

cos-to-frame-map default-c2f frame-to-cos-map default-f2c classifier-list-precedence 103 classifier-list vlan103

exit exit

**# L2VPN Service**

l2vpn-services l2vpn L1

forwarding-domain AC\_UNI\_FD1 pseudowire pe1\_pe2\_spoke\_pw1 service-type vlan

signaling-type ldp mtu 1500

exit exit

**#REMOVE L2vpn services (this config is shared for reference only if end user wants to remove L2VPN)**

config t

no l2vpn-services no pseudowires

no ldp instance default target-ldp peers 4.4.4.4

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

* + 1. FAT PW Verification & Results

***Objective:***

Objective of this section is to provide a cli commands for verification of FAT PW status & results analysis. We will be using various alternate methods to verify, however at the moment there is no direct cli command available in 10.5.1 to verify FAT PW status. We will capture cli outputs from PE nodes PW.

***Procedure:***

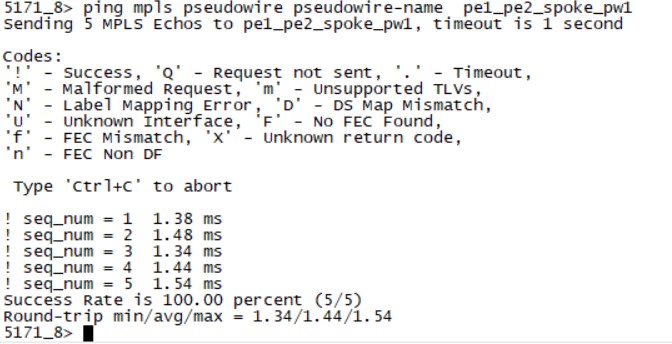
On PE nodes

***Verify PW status:***

Table

Description automatically generated

Ping response of PW



***Verify FAT signalling enable on node:***

A picture containing diagram

Description automatically generated

* On PE1 node the output of ettps shows an even spread of traffic on ingress direction of LAG ports 20 & 21, for traffic originated by ixia connected for pt 1 5 and destined towards ixia connected port 1 at PE2.

This uniform distribution of traffic along with wireshark snapshot of packet capture proves that 10x node is hashing traffic on two links of LAG for a L2VPN VPLS.

PE 1 ETTP stats

Table

Description automatically generated with low confidence

**PE 2 ETTP stats**

Table

Description automatically generated with low confidence

* Ingress Packet Capture taken on port 20 of PE2 node which shows the of FAT PW label (label 360 can be seen generated)

Graphical user interface, application, table, Excel

Description automatically generated

* For details of hashing algorithm works please refer to FAT PW Signaling capability 10.5 TOI topic, however in our test setup we are using ixia to create two different source MACs, which separates different traffic flows, essentially resulting in FAT label generation and efficient hashing. Snapshot setting from Ixia can be seen below

Graphical user interface, application

Description automatically generated

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Add a COS to frame map to a flow point

***Objective:***

Objective is to verify binding of a COS to frame map to an egress flow point

In this section, following the steps will configure the parts of the picture highlighted in red.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Chart  Description automatically generated Shape  Description automatically generated with low confidence  Chart  Description automatically generated Chart  Description automatically generated  PCP COS Color COS Color PCP  Forwarding Domain FD1  Flow Point Flow Point  FP1 FP2 | | | | |
|  | Port 1 |  | Port 2 |  |

***Procedure:***

* Go to the configuration terminal
  + config
* Enter the following commands

In addition to adding the map to the flow point, the map show be used in the l2-trasform if a re-marking of the packets needed.

fps fp FPT logical-port 1 fd-name FD1

stats-collection on

**frame-to-cos-map FTC1 egress-l2-transform EL2T1 vlan-stack 1**

**stamp-pcp map exit**

* Go back out of configuration terminal

# exit

* Check if the COS to frame map is associated with the flow point:
  + show flow-points flow-point FPT

You should see something like the following:

+ Flow Point +

| KEY | VALUE |

+ + +

| Name | FPT |

| Forwarding Domain Name | FD1 |

| Logical Port | 1 |

| MTU Size | 2000 |

| Egress L2 Transform | |

| Egress Name | EL2T1 |

| Egress Vlan Stack | |

| Tag | 1 |

| Stamp Pcp | map |

| Frame To CoS Map | FTC1 |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

Ingress Metering - QoS Flow and QoS meter profile

***Objective:***

Objective is to create QoS flow and QoS meter profile. Parent interface for QoS flow is on flow point only, logical port as parent interface is NOT supported.

The classifiers that can be used to create QoS flow are:

51xx : single vlan, double vlan, untagged, internal cos, or any

39xx : single vlan, untagged, single vlan + PCP, IPv4 based DSCP, Ipv6 based DSCP, DSCP+Mask, or any

***Procedure:***

* Create ingress meter profile (~2G) and ensure that the profile can be attached to QoS flow:
  + meter-profiles meter-profile **mp2G-qos** cir **2000000** cbs 256 eir **10000** ebs 128 color-aware false coupling-flag false shared-meter-instance false valid-interface-type **qos-flow**
  + meter-profiles meter-profile **mp2G-qos2** cir **2000000** cbs 256 eir **10000** ebs 128 color-aware false coupling-flag false shared-meter-instance false valid-interface-type **qos-flow**
* Create ingress meter profiles and ensure that the profile can be attached to a parent flow point.
  + meter-profiles meter-profile **mp7G** cir **6000000** cbs 256 eir **500000** ebs 128 color-aware false coupling-flag false shared-meter-instance true valid-interface-type **flow-point**
  + meter-profiles meter-profile **mp4G-fp** cir **4000000** cbs 256 eir **10000** ebs 128 color-aware false coupling-flag false shared-meter-instance true valid-interface-type **flow-point**
  + meter-profiles meter-profile **mp2G-fp** cir **2000000** cbs 256 eir **10000** ebs 128 color-aware false coupling-flag false shared-meter-instance true valid-interface-type **flow-point**
* Validate the meter profiles:

5170-0010-R1> **show meter-profiles**

+ METER PROFILE +

| Name | CIR Kbps | EIR Kbps |

+ + + +

| **mp2G-fp** | 2000000 | 10000 |

| **mp2G-qos** | 2000000 | 10000 |

| **mp2G-qos2** | 2000000 | 10000 |

| **mp4G-fp** | 4000000 | 10000 |

| mp6G-qos | 6000000 | 10000 |

| **mp7G** | 6000000 | 500000 |

| mp600M | 200000 | 400000 |

+ + + +

* Create the classifier to use for QoS flow. classifiers classifier internalcos8 filter-entry internal-cos internal-cos 8 exit

classifiers classifier anycos filter-entry any

exit

* Create QoS flow that uses the “mp2G-qos” and “mp2G-qos2” meter profiles.

##create QoS flow that classifies on internal Cos of 8 or 16. qos-flows qos-flow qf1-cos8-cos16 meter-profile **mp2G-qos**

parent-fp CustomerQos classifier-list internalcos8 classifier-list internalcos16 classifier-list-precedence 10 stats-collection on

exit exit

##create QoS flow that is a catch all QoS flow.

qos-flows qos-flow **qos-catchall**

meter-profile **mp2G-qos2** parent-fp CustomerQos classifier-list anycos classifier-list-precedence 11 stats-collection on

exit exit

* Validate the QoS flows.

5170-0010-R1> show qos-flows

+

QOS FLOWS +

| Name | Meter Profile | Parent Logical Port | Parent Flow Point | Stats Collection |

+ + + + + +

| qf1-cos8-cos16 | mp2G-qos | - | CustomerQos | on |

| qos-catchall | mp2G-qos2 | - | CustomerQos | on |

+ + +

+

+

+ + + QOS FLOWS STATS

| Name | Accepted Bytes | Accepted Frames | Yellow Bytes | Yellow Frames | Dropped Bytes | Dropped Frames |

+ + +

+

+ + + +

| qf1-cos8-cos16 | 0 | 0 | 0 | 0 | 0 | 0

|

| qos-catchall | 0 | 0 | 0 | 0 | 0 | 0

|

+ + +

+

+ + + +

* Next step is to setup meter profiles on parent flow point, please see next testcase.

Test Case Results:

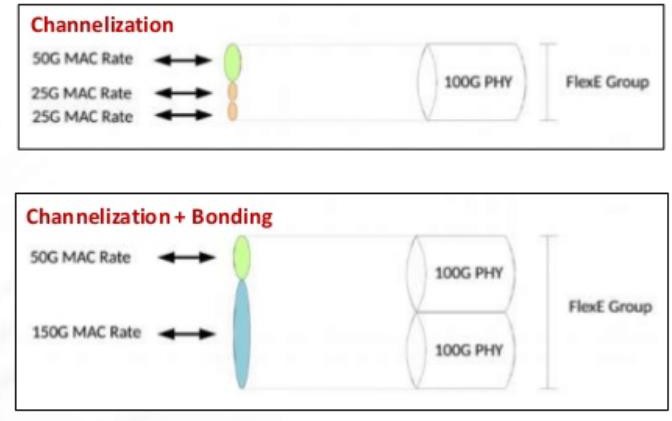
Passed: Yes No Verified by Date/Time Comments

#### FlexE Introduction

The general capabilities supported by FlexE are:

* Bonding e.g., supporting a 200G MAC over two bonded 100GBASE-R PHYs
* Channelization e.g. support a 50G and two 25G MACs over a 100GBASE-R PHY
* A picture containing text, weapon, knife

  Description automatically generatedSubrating e.g., supporting a 75G MAC over a 100GBASE-R PHY



Sebastien Gareau, Hardware Systems Architect at Ciena, talks about the industry effort to introduce flexibility at the Ethernet service layer.

<https://www.ciena.com/insights/videos/Chalk-Talk---What-is-Flex-Ethernet-FlexE.html>

###### Configure a FlexE Client Port

***Objective:***

The objective of this test is to configure a 25GE L1 flexE client port.

***Topology:***



***Procedure:***

1. Set the client port (port 1) to 25GE, remove the default remote flow point, remove the port binding and set the port to L1 cross connect mode. The user can enable or disable RS-FEC as required.

oc-if:interfaces interface 1 config port-speed 25Gb

oc-if:interfaces interface 1 config forward-error-correction disabled no fps fp remote-fp1

no logical-ports logical-port 1 binding

oc-if:interfaces interface 1 config ettp-mode l1-cross-connect

***Expected Results:***

Port 1 should be configured as a FlexE client and set to layer 1 cross connect mode.

5164> show ettps ettp 1

+ ETTP +

| KEY | VALUE |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| + |  | + |  | + |
| | | Name | | | 1 | | |
| | | Description | | | 1 | | |
| | | Type | | | ettp | | |
| | | Admin Status | | | True | | |
| | | Mode | | | auto | | |
| | | Link Flap Detect | | | False | | |
| | | Link Flap Count | | | 5 | | |
| | | Link Flap Detect Time | | | 10 | | |
| | | Link Flap Hold Time | | | 300 | | |
| | | Duplex | | | full | | |
| | | Port Speed | | | 25Gb | | |
| | | Flow Control | | | off | | |
| | | Auto Negotiation | | | False | | |
| | | Forward Error Correction | | | disabled | | |
| | | PTP Id | | | 1 | | |
| | | ETTP Mode | | | l1-cross-connect | | |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Configure FlexE Network Port

***Objective:***

The objective of this test is to configure FlexE network ports.

***Topology:***

A screenshot of a computer

Description automatically generated with medium confidence

***Procedure:***

The user sets NNI ports to FlexE mode.

1. Configure NNI ports for FlexE mode. In the example below ports 33 and 34 are configured as FlexE NNI ports. Port binding is removed and the port is set to FlexE.

no fps fp remote-fp33

no logical-ports logical-port 33 binding

no oc-if:interfaces interface 33 config ptp-id

flexe-ports flexe-port flexe-port1 ptp-id 33 port-speed 100Gb no fps fp remote-fp34

no logical-ports logical-port 34 binding

no oc-if:interfaces interface 34 config ptp-id

flexe-ports flexe-port flexe-port2 ptp-id 34 port-speed 100Gb

***Expected Results:***

NNI ports are set to FlexE mode.

5164> show flexe-ports flexe-port flexe-port1

+ FLEXE PORT +

| Key | Value |

+ + +

| FlexE Port | flexe-port1 |

| Admin State | enabled |

| PTP ID | 33 |

| Port Speed | 100Gb |

| Forward Error Correction | auto |

+ + +

+--- FLEXE PORT STATUS +

| Key | Value |

+ + +

| FlexE Port | flexe-port1 |

| Oper State | disabled |

+ + +

5164> show flexe-ports flexe-port flexe-port2

+ FLEXE PORT +

| Key | Value |

+ + +

| FlexE Port | flexe-port2 |

| Admin State | enabled |

| PTP ID | 34 |

| Port Speed | 100Gb |

| Forward Error Correction | auto |

+ + +

+--- FLEXE PORT STATUS +

| Key | Value |

+ + +

| FlexE Port | flexe-port2 |

| Oper State | disabled |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Create a FlexE Group

***Objective:***

The objective of this test is to create a 200 GE FlexE Group (also know as port binding).

***Topology:***

A screenshot of a computer

Description automatically generated with medium confidence

***Procedure:***

Configure a 200 GE FlexE group with ports 33 and 34.

2. Create a FlexE group by adding FlexE ports “flexe-port1” and “flexe-port2” (created in the previous step) to the group. The group is also assigned slot granularity (5G) and a calendar (slot map).

flexe-groups flexe-group group1 group-number 1

calendar-slot-granularity slot-5G phy-type flexe-phy-100GBASE-R calendar calendar-A

calendar-protocol-enable false

flexe-phys 1 local-interface flexe-port1 flexe-phys 2 local-interface flexe-port2 exit

exit

***Expected Results:***

A 200 GE FlexE group should have been created with 40 5G calendar slots.

5164> show flexe-groups flexe-group group1

+ FLEXE GROUPS +

| KEY | VALUE |

+ + +

| FlexE Group | group1 |

| Admin State | enabled |

| Group No. | 1 |

| Calendar Slot Granularity | slot-5G |

| Phy Type | flexe-phy-100GBASE-R |

| Calendar | calendar-A |

| FlexE Phys | |

| Phy No. In Grp | 1 |

| Local Interface | flexe-port1 |

| | |

| Phy No. In Grp | 2 |

| Local Interface | flexe-port2 |

+ + +

###### Create a FlexE Channel

***Objective:***

The objective of this test is to create a 25G FlexE channel.

***Topology:***



***Procedure:***

Configure a 25 FlexE channel.

* + - 1. Create a FlexE channel by assigning 5G calendar slots equal to the bandwidth required. In the following example we are creating a 25G FlexE channel.

flexe-channels flexe-channel channel-1

channel-number 512 group-name group1

channel-mapping L1-mapped

|  |  |  |
| --- | --- | --- |
| calendar-A-slots-list | 1 | 1 |
| exit |  |  |
| calendar-A-slots-list | 1 | 2 |
| exit |  |  |
| calendar-A-slots-list | 1 | 3 |
| exit |  |  |
| calendar-A-slots-list | 1 | 4 |
| exit |  |  |
| calendar-A-slots-list | 1 | 5 |
| exit |  |  |
| exit |  |  |
| exit  ***Expected Results:*** |  |  |

A 25 GE FlexE channel should have been created.

5164> show flexe-groups flexe-group group1

+ FLEXE GROUPS +

| KEY | VALUE |

+ + +

| FlexE Group | group1 |

| Admin State | enabled |

| Group No. | 1 |

| Calendar Slot Granularity | slot-5G |

| Phy Type | flexe-phy-100GBASE-R |

| Calendar | calendar-A |

| FlexE Phys | |

| Phy No. In Grp | 1 |

| Local Interface | flexe-port1 |

| | |

| Phy No. In Grp | 2 |

| Local Interface | flexe-port2 |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Create a FlexE Cross Connect

***Objective:***

The objective of this test is to create a FlexE cross connect.

***Topology:***

A screenshot of a computer

Description automatically generated with medium confidence

***Procedure:***

Create a channel MAC termination point and then cross connect the channel MAC termination point with the FlexE client port.

* + - 1. Create a MAC termination point on the 25G FlexE channel.

oc-if:interfaces interface macEttp1 config name macEttp1 type ettp ettp-mode flexe-mac oc-if:interfaces interface macEttp1 config name macEttp1 flexe-channel channel-1

* + - 1. Cross connect the FlexE channel with the FlexE client port.

flexe-cross-connects flexe-cross-connect fxc-1 ettp-end-point-a macEttp1 ettp-end-point- b 1

***Expected Results:***

The cross connect should have been created successfully.

5164> show ettps ettp macEttp1

+ ETTP +

| KEY | VALUE |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| + |  | + |  | + |
| | | Name | | | macEttp1 | | |
| | | Type | | | ettp | | |
| | | Admin Status | | | True | | |
| | | Mode | | | auto | | |
| | | Link Flap Detect | | | False | | |

| Link Flap Count | 5 |

| Link Flap Detect Time | 10 |

| Link Flap Hold Time | 300 |

| Duplex | full |

| Forward Error Correction | auto |

| ETTP Mode | flexe-mac |

| FlexE Channel ID | channel-1 |

+ + +

5164> show flexe-cross-connects

+ FLEXE-CROSS-CONNECTS +

| Flexe-Cross-Connect | End-Point-A | End-Point-B |

+ + + +

| fxc-1 | Ettp: macEttp1 | Ettp: 1 |

+ + + +

5164> show flexe-cross-connects flexe-cross-connect fxc-1

+----- FLEXE-CROSS-CONNECTS +

| Key | Value |

+ + +

| Flexe-Cross-Connect | fxc-1 |

| Ettp-End-Point-A | macEttp1 |

| Ettp-End-Point-B | 1 |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### L2 FlexE

Layer 2 FlexE is now supported in 10.6+ on the following devices: 5130, 5164, 5166 and 5168. When network devices are connected via L2 FlexE, client ports and flexE channels are connected to FDs via FPs. Conceptually, a FlexE channel becomes a “logical port” and uses a 10.x FD/FP L2 configuration method for DP connectivity.

L2 Cross Connect L2 Cross Connect



FlexE

ETTP

10GE

FlexE

ETTP

L2 FD

10G ETTP

L2 FD

10G ETTP

Figure (1): Device has GPS and PTP Inputs

Layer 2 FlexE Configuration

***Objective:***

The objective of this test is to configure a L2 FlexE channel.

***Procedure:***

* Configure a FlexE Group:

flexe-groups flexe-group group1 group-number 1

calendar-slot-granularity slot-5G phy-type flexe-phy-100GBASE-R calendar calendar-A

calendar-protocol-enable false

flexe-phys 3 local-interface flexe-port1

* Configure a FlexE channel (10G channel configured in this example):

flexe-channels flexe-channel channel-1 channel-number 512

group-name group1

channel-mapping L2-mapped calendar-A-slots-list 3 1

calendar-A-slots-list 3 2

calendar-B-slots-list 3 11

calendar-B-slots-list 3 12

* Create a mac termination point and a “FlexE” logical port:

oc-if:interfaces interface macEttp1 config name macEttp1 type ettp ettp-mode flexe-mac

oc-if:interfaces interface macEttp1 config name macEttp1 flexe-channel channel-1

logical-ports logical-port flexe\_lp\_1 binding macEttp1

* Create a forwarding domain and a flow point on the “FlexE” logical port.

fds fd fd\_vlan mode vpls

fps fp fp\_flexe\_lp\_1 classifier-list AnyTag classifier-list untagged stats-collection on

fd-name fd\_vlan

logical-port flexe\_lp\_1 mtu-size 9216

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### WebGUI – Create BGP Instance

***Objective:***

Validate the creation of BGP Instance from WebGUI.

***Procedure:***

* On CLI, verify that the BGP instance has not been created.

show bgp

show bgp peers

5162-004> show bgp peers

+

+

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| | |  Received | Sent | | | | | | | Up  | | | Peer | | Received | | Advertised | | Last | | |
| |  Prefix | | Remote |  | Prefix | | Peer | Time  | | | | | Table | | Pkt | | Pkt | | Reset | | |

BGP PEERS

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| | | Peer | | AS | | Type | (hh:mm:ss) | | Version | | Count | | Count | | (hh:mm:ss) |
| | | Count | | | Count | State | |  |  |  |  |
| + | + |  | + + + | + |  | + | + |

+ + + +

| | | | | | | | |

| | |

+ + + + + + + +

+ + + +

5162-004> show bgp

+ BGP +

| Name | Value |

+ + +

| | |

+ + +

* On WebGUI, on left hand side navigation pane, select L3/BGP.
* Then select Configure BGP.

Graphical user interface, text, application, chat or text message

Description automatically generated

* Select MP-BGP for configuration. Fill in the necessary information and then click Save. Can choose Advanced Settings for more detailed info.

Graphical user interface, application

Description automatically generated

* Validate that BGP peers have been added.

Graphical user interface, application

Description automatically generated

* Validate that the BGP peering has been established.

Graphical user interface, text, application

Description automatically generated

* Validate on CLI as well.

Show bgp

Show bgp peer

5162-004> show bgp

+ BGP +

| Name | Value |

+ + +

| AS | 484848 |

| Table version | 1 |

| Prefix count | 0 |

| Router ID | 62.62.62.223 |

+ + +

5162-004> show bgp peer

+

BGP PEERS

+

| | | | Up | Peer | Received | Advertised | Last | Received | Sent | |

| | Remote | Peer | Time | Table | Pkt | Pkt

| Reset | Prefix | Prefix | |

| Peer | AS | Type | (hh:mm:ss) | Version | Count | Count | (hh:mm:ss) | Count | Count | State |

+ + +

+ +

+ + + +

+ + +

| 26.26.26.235 | 484848 | internal | 00:06:27 | 1 | 123 | 133

| 00:06:32 | 0 | 0 | Established |

| 66.66.66.140 | 484848 | internal | 00:01:25 | 1 | 4 | 4

| - | 0 | 0 | Established |

+ + +

+ +

5162-004>

+ + + +

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments