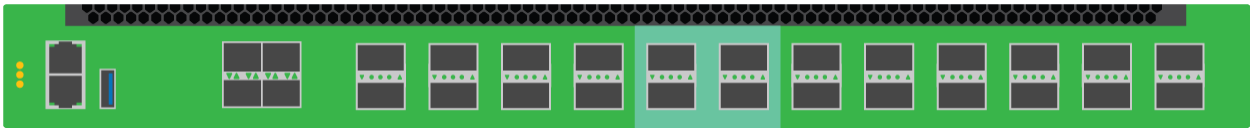
GARLAND TECHNOLOGY

See every bit, byte, and packet®

User Guide

AF40G24AC / AF40G24DC



06/2025

Release Version: 3.0.16.r10

Notice

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

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Table of Contents

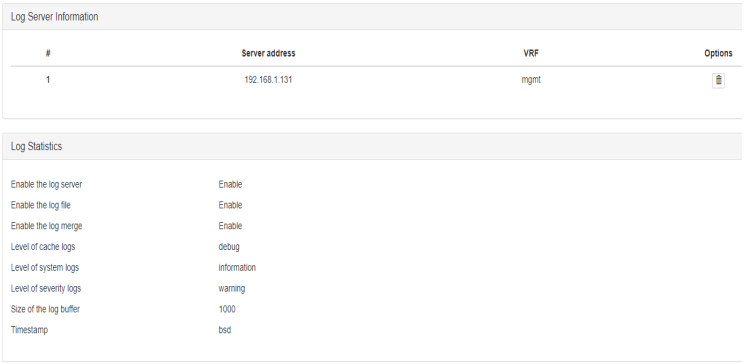
Syslog

Advanced Features provides the ability to send syslog messages to a syslog server via the management interface.

Enable Syslog

1. Select System Management.
2. Select Log Management.
3. Enable the log server.
4. Select the desired Level of system timestamp.
5. Select the desired Level of cache logs.
6. Select the desired Level of system logs.
7. Select the desired Level of severity logs.
8. Enter the desired Size of log buffer.
9. Select Submit.
10. Enter the desired Address of the log server's IP address.
11. Select Submit.
12. Multiple log servers may be entered.

The Log Server Information panel will display the configuration.



13. The log server may be deleted by selecting the Trash Can in the Options column.

NTP Timing

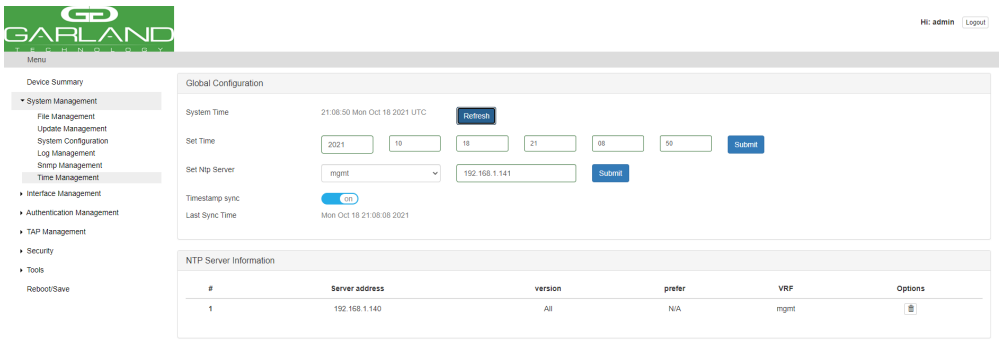
Advanced Features provides the ability to time from an NPT timing source. There are two options to setup NPT timing:

- Basic NTP Timing
- Authenticated NTP Timing

Basic NTP Timing

1. Select System Management.
2. Select Time Management.
3. Enter the NTP server IP Address.
4. Select Submit.
5. Enable Timestamp sync.

The Global Configuration and NTP Server Information will be displayed.



Additional NTP Servers may be applied by repeating Steps 4 and 5. The first NTP server added will be the highest priority, #1. Additional NTP servers will be #2, #3 etc.

Authenticated NTP Timing

Authenticated NTP Timing must be configured via CLI.

Connect to the Advanced Features

Connect to the Advanced Features unit. A connection to the unit may be established using two options:

- Directly connected to the Console Interface to COM Port using Putty/Serial connection
- Connected via the IP Management Interface using Putty/SSH connection

1. Press the Return key.
2. Enter enable.

3. Enter configure terminal.
4. Enter the following command to configure the minimum distance between the unit and the NTP server. The default is 1ms, (X=1ms to 1000ms).

```
Switch(config)# ntp minimum-distance X
```

5. Enter the following command to define the NTP server IP address (xxx.xxx.xxx.xxx), define the NTP protocol version (Y=1,2,3), define the authentication key (Z=1-64000) and define as the preferred server (prefer).

```
Switch(config)# ntp server mgmt-if XXX.XXX.XXX.XXX version Y key Z prefer
```

6. Enter the following command to enable/disable NTP authentication.

```
Switch(config)# ntp authentication enable / disable
```

7. Enter the following command to create a NTP key ID (X=1-64000) and define the key value (Y=key string).

```
Switch(config)# ntp key X Y
```

8. Enter the following command to authenticate the NTP server identity (X=1-64000).

```
Switch(config)# ntp trustedkey X
```

9. Enter the following command to display the NTP server configuration.

```
Switch# show ntp
```

10. Enter the following command to display the NTP status.

```
Switch# show ntp status
```

11. Enter the following command to display the NTP statistics.

```
Switch# show ntp statistics
```

12. Enter the following command to display the NTP associations.

```
Switch# show ntp associations
```

13. Enter the following command to display the NTP Key(s).

```
Switch# show ntp key
```

14. Enter the following command to clear the NTP statistics.

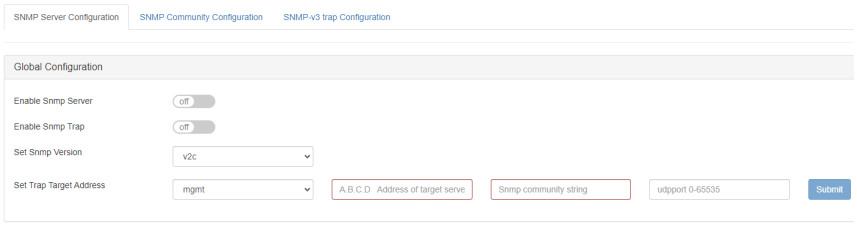
```
Switch# clear ntp statistics
```

SNMP v2c

The following procedure may be used to configure SNMP v2c.

1. Select System Management.
2. Select SNMP Management.

The SNMP Server Configuration Tab panel will be displayed.

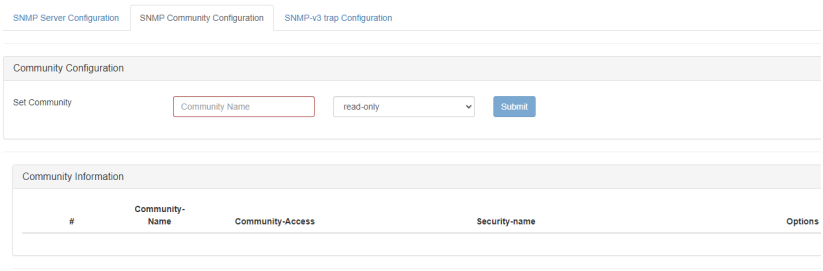


3. Enable SNMP Server.
4. Enable SNMP Trap.
5. Select the SNMP Version.
6. Enter the A.B.C.D Address of Target Server.
7. Enter the SNMP Community String.
8. Enter UDP Port Number.
9. Select Submit.

Trap Target Information will be displayed. Additional Trap Targets may be added.

10. Delete the Trap Target by selecting the Trash Can under the Options column.
11. Select the SNMP Community Configuration Tab.

The SNMP Community Configuration Tab panel will be displayed.



12. Enter the Community Name.
13. Select the Set Community option.

14. Select submit.

    The Community Information will be displayed.

15. Delete the Community Information by selecting the Trash Can under the Options column.

SNMP v3

The following procedure may be used to configure SNMPv3 on the Advanced Aggregators. The Advanced Aggregators support two versions of SNMPv3, MD5/DES or SHA/AES. SNMPv3 may be set up via the GUI or via CLI commands. This procedure focuses on the CLI command method.

Connect to the Advanced Features

Connect to the Advanced Features unit. A connection to the unit may be established using two options:

- Directly connected to the Console Interface to COM Port using Putty/Serial connection
- Connected via the IP Management Interface using Putty/SSH connection

1. Press the Return key.
2. Enter enable.
3. Enter configure terminal.

SNMPv3 MD5 / DES

1. Enter the following commands.

```
Switch(config)# snmp-server enable

Switch(config)# snmp-server trap enable all

Switch(config)# snmp-server community public read-only
```

The Community String public may be substituted with another desired option.

read-only may be substituted with read-write.

```
Switch(config)# snmp-server usm-user username authentication md5 md5password
                privacy des despassword
```

Substitute username with the desired username defined on the MIB Browser.
Substitute md5password with the desired MD5 password defined on the MIB Browser.
Substitute despassword with the desired DES password defined on the MIB Browser.

```
Switch(config)# snmp-server group grp1 user username security-model usm
```

Substitute username with the desired username defined on the MIB Browser.

```
Switch(config)# snmp-server access grp1 security-model usm priv

Switch(config)# snmp-server notify notify1 tag tempteg

Switch(config)# snmp-server target-params parm1 user username security-model v3
                message-processing v3 priv
```

Substitute username with the desired username defined on the MIB Browser.

```
Switch(config)# snmp-server target-address targ1 param parm1 mgmt-if
                xxx.xxx.xxx.xxx taglist tempteg
```

Substitute xxx.xxx.xxx.xxx with the desired MIB Browser IP Address.

SNMPv3 SHA / AES

1. Enter the following commands.

```
Switch(config)# snmp-server enable

Switch(config)# snmp-server trap enable all

Switch(config)# snmp-server community public read-only
```

The Community String public may be substituted with another desired option.

read-only may be substituted with read-write.

```
Switch(config)# snmp-server usm-user username authentication sha shapassword
                privacy aes aespassword
```

Substitute username with the desired username defined on the MIB Browser.
Substitute shapassword with the desired SHA password defined on the MIB Browser.
Substitute aespassword with the desired AES password defined on the MIB Browser.

```
Switch(config)# snmp-server group grp1 user username security-model usm
```

Substitute username with the desired username defined on the MIB Browser.

```
Switch(config)# snmp-server access grp1 security-model usm priv

Switch(config)# snmp-server notify notify1 tag tempteg

Switch(config)# snmp-server target-params parm1 user username security-model v3
                message-processing v3 priv
```

Substitute username with the desired username defined on the MIB Browser.

```
Switch(config)# snmp-server target-address targ1 param parm1 mgmt-if
                xxx.xxx.xxx.xxx taglist tempteg
```

Substitute xxx.xxx.xxx.xxx with the desired MIB Browser IP Address.

Port Group

PortGroups allow for multiple ports to be grouped. A PortGroup may be used as an ingress entity when creating a TAP Group. When a PortGroup is used in a TAP Group a flow must be applied. The flow may have multiple specific traffic entries or may be created as a pass all.

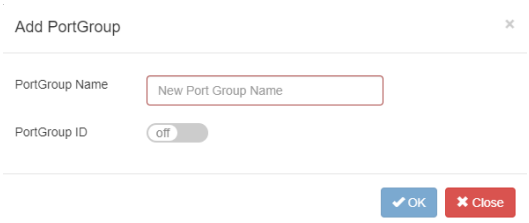
PortGroups provide the following benefits:

- Aggregates the traffic from multiple ports
- Eliminates the need to create multiple TAP Groups to the same egress entity
- Multiple ports sharing a single flow
- Ports may be added or removed without affecting the TAP Group

Create a Port Group

1. Select Interface Management.
2. Select PortGroup Config.
3. Select + Add PortGroup.

    The Add PortGroup panel will appear.

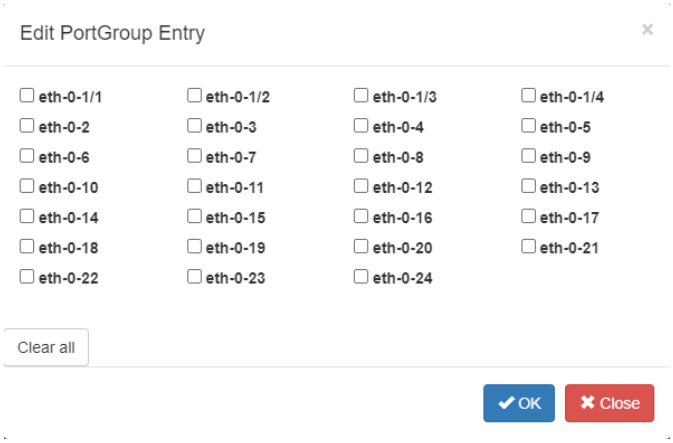


4. Enter the PortGroup Name.
5. Enter the PortGroup ID, optional.
6. Select OK.

    The PortGroup will be displayed. The member count will display zero (0) until ports are added.

7. Select the Edit icon in the Options column to add the desired ports.

The Edit PortGroup Entry panel will be displayed.



8. Select the desired ports.

9. Select Clear all too clear any selected ports.

10. Select OK.

The PortGroup will be displayed. the member count will display the number of ports assigned.

11. Ports may be added or removed by selecting the Edit icon.

12. Select the Trash Can to delete the PortGroup.

iloop

Advanced Features supports up to 24 iloop ports. The 24 iloop ports support up to a maximum total bandwidth of 120G. Iloop ports are virtual internal ports that may be used as an ingress or egress entity when creating a TAP Group.

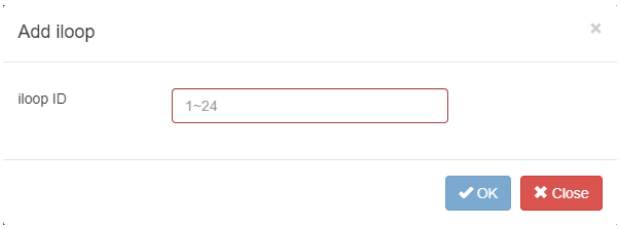
Iloop ports provide the following benefits:

- Allow for a flow (filter and/or action) between a physical port(s) and iloop port
- Allow for a flow (filter and/or action) between an iloop port and physical port(s)

Create an iloop Port

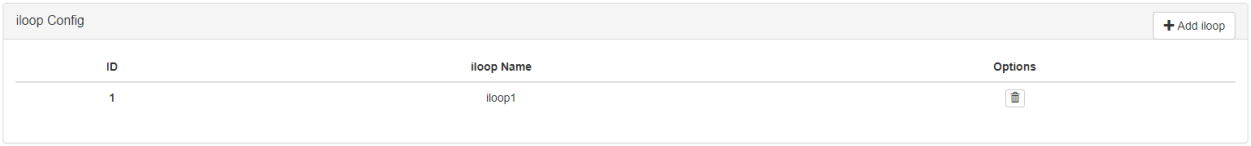
1. Select Interface Management.
2. Select iloop.
3. Select + Add iloop.

The Add iloop panel will be displayed.



4. Enter the iloop ID, optional.
5. Select OK.

The iloop will be displayed.

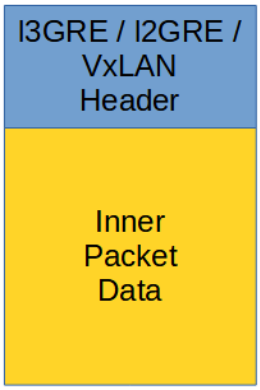


6. Select the Trash Can in the Options column to delete the iloop.

Inner Match

Decapsulate I3GRE/I2GRE/VXLAN

Typically, packet decapsulation decisions are made using header data only. However, in some cases it is necessary to make packet decapsulation decisions based on using the header data and inner packet data. Inner Match may be used to decapsulate I3GRE, I2GRE and VxLAN packets using the header data and inner packet data.



Decapsulating the I3GRE, I2GRE or VxLAN header from a packet using Inner Match involves three configuration procedures.

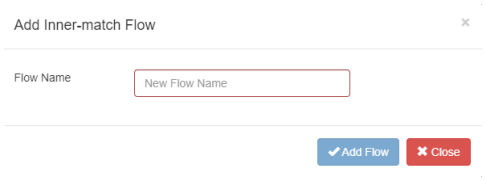
- Create the Inner Match
- Create the Flow
- Create the TAP Group

This section discusses the procedures to create the Inner Match Flow and the Flow. The procedure to create a TAP Group is discussed in the TAP Group section.

Create the Inner Match

1. Select TAP Management.
2. Select Inner Match.
3. Select + Add Inner-match Flow.

The Add Inner-match Flow panel will appear.



4. Enter the Flow Name.
5. Select Add Flow.

   The Inner Match flow will be displayed.

6. Select the + in the Options column to define the attributes.

   The Add Flow Entry panel will be displayed.

   Inner Match Rule Section

   - Determines the packet inner match filter criteria

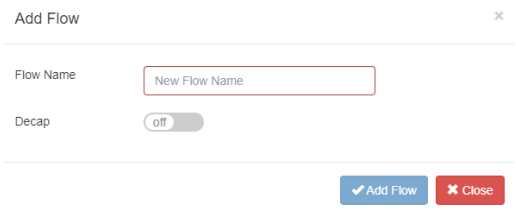
7. Select the desired inner match options and enter the desired values.
8. Select OK.
9. Select the flow name to display the attributes.

   The Flow Entry panel will be displayed.

Create the Flow

1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

   The Add Flow panel will appear.

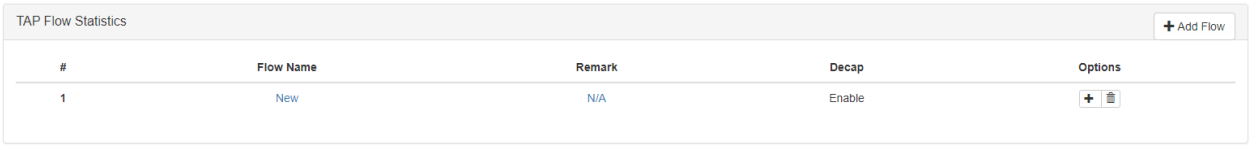


4. Enter the Flow Name.

5. Enable Decap.

6. Select Add Flow.

The flow will be displayed.



7. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule (l3GRE)

8. Select permit for the Action.

9. Select gre for the IP Protocol Number.

10. Select any other desired options and enter the desired values to define which l3GRE packets will be decapsulated. The defaults may be used.

11. Select OK.

Flow Match Rule (l2GRE)

8. Select permit for the Action.

9. Select nvgre for the IP Protocol Number.
10. Select any other desired options and enter the desired values to define which l2GRE packets will be decapsulated. The defaults may be used.
11. Select OK.

Flow Match Rule (VXLAN)

8. Select permit for the Action.
9. Select udp for the IP Protocol Number.
10. Enable Dst-port.
11. Select eq for the Type.
12. Enter 4789 for the Port.
13. Enable Inner Match.
14. Select desired Inner Match flow.
15. Enable Vxlan-VNI.
16. Enter the desired VxLAN VNI value.
17. Enter the desired Wildcard value.
18. Select OK.
19. Select the flow name to display the attributes.

The Flow Entry panel will be displayed

Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

Custom SSL Certificates

Custom SSL certificates may be applied and used to support HTTPS services on the Advanced Features units. Configuring custom SSL certificates involves the following configuration procedures:

- Display the Default Services
- Disable the HTTP Service
- Enable the HTTPS Service
- Login to the GUI via HTTPS and Upload the Custom SSL Certificate
- Apply the Custom SSL Certificate

Connect to the Advanced Features

Connect to the Advanced Features unit. A connection to the unit may be established using two options:

- Directly connected to the Console Interface to COM Port using Putty/Serial connection
- Connected via the IP Management Interface using Putty/SSH connection

Display the Default Services

The default services configuration are displayed via the console interface. Use the following procedure to display the default services configuration.

1. Press the Return key.
2. Enter enable.
3. Enter the following command to display the default services configuration.

```
Switch# show services
Networking services configuration:
Service Name     Status        Port       Protocol   Service ACL
---------------+-------------+----------+----------+------------
http             enable        80         TCP        -
https            disable       443        TCP        -
rpc-api          disable       -          TCP        -
telnet           disable       23         TCP        -
```

```
ssh             enable        22          TCP         -
snmp            disable       161         UDP         -
```

Disable the HTTP Service

1. Enter the following commands to disable the HTTP service.

```
Switch# configure terminal
Switch(config)# service http disable
Switch(config)# exit
Switch# show services
Networking services configuration:
Service Name     Status        Port       Protocol   Service ACL
---------------+-------------+----------+----------+------------
http             disable       80         TCP        -
https            disable       443        TCP        -
rpc-api          disable       -          TCP        -
telnet           disable       23         TCP        -
ssh              enable        22         TCP        -
snmp             disable       161        UDP        -
```

Enable the HTTPS Service

1. Enter the following commands to enable the HTTPS service.

```
Switch# configure terminal
Switch(config)# service https enable
Switch(config)# exit
Switch# show services
Networking services configuration:
Service Name     Status        Port       Protocol   Service ACL
---------------+-------------+----------+----------+------------
http             disable       80         TCP        -
https            enable        443        TCP        -
rpc-api          disable       -          TCP        -
telnet           disable       23         TCP        -
ssh              enable        22         TCP        -
snmp             disable       161        UDP        -
```

Login to the GUI via HTTPS and Upload the Custom SSL Certificate

The PEM file that is uploaded onto the Advanced Features unit must contain both the key.pem and cert.pem files. The file name must be like “key_AFTest.pem”.

Key_AFTest.pem example:

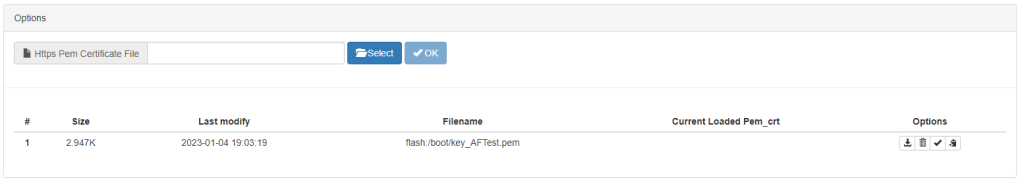
```
-----BEGIN PRIVATE KEY-----
cbhsdabsdahcbsacascakhscbdkndsjnbsdjkcvbskjdcvbskjdbvskdjvbskdvbksdbcskdcbskd
bskdbcfcc
ahscbahscbaksdhcbakshcbasdhcbakhbcahscbakhscbakshcbakshcbakhscashscacajscahscakhscb
akhscb ahscashcajshcajshcahsc&%VBGFFGBjsxncsjbdb#$%^^ujdsfbibfwfbwhfbwhbshbvskdhcvbd
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
cbhsdabsdahcbsacascakhscbdkndsjnbsdjkcvbskjdcvbskjdbvskdjvbskdvbksdbcskdcbskd
bskdbcfcc
ahscbahscbaksdhcbakshcbasdhcbakhbcahscbakhscbakshcbakshcbakhscashscacajscahscakhscb
akhscb ahscashcajshcajshcahsc&%VBGFFGBjsxncsjbdb#$%^^ujdsfbibfwfbwhfbwhbshbvskdhcvbd
-----END CERTIFICATE-----
```

1. Launch the web browser and enter the IP address.
2. Login to the GUI.
3. Select System Management.
4. Select Update Management.
5. Select the Select image file (Upload files to boot) Choose File.
6. Select the “key_AFTest.pem”.
7. Select Upload only.
8. Select File Management.
9. Select the Boot files Tab.
10. Verify the new “key_AFTest.pem”.

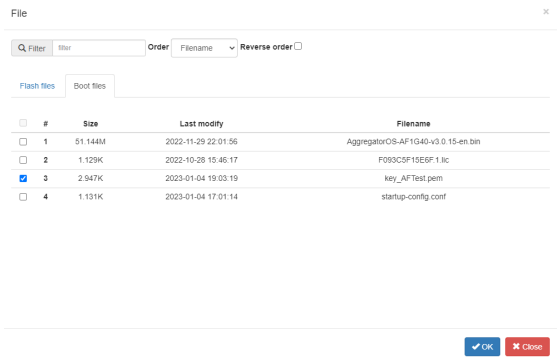
Apply the Custom SSL Certificate

1. Select Security.
2. Select Https Pem_crt.

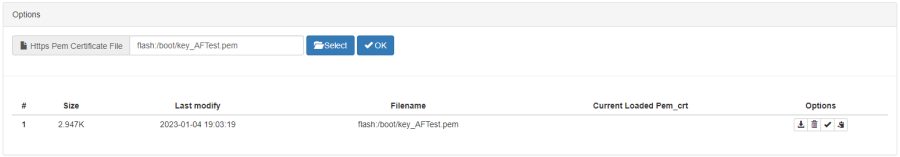
The key_AFTest.pem *will be displayed.*



3. Select the Select option.
4. Select the Boot files Tab.
5. Select the pem file “key_AFTest.pem”.

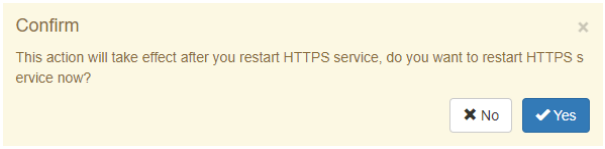


6. Select OK.
7. Verify the Https Pem Certificate File, new “key_AFTest.pem”.



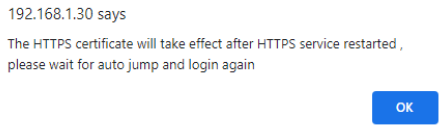
8. Select OK.

The Confirm message will be displayed.



9. Select Yes.

The HTTPS restart message will be displayed.

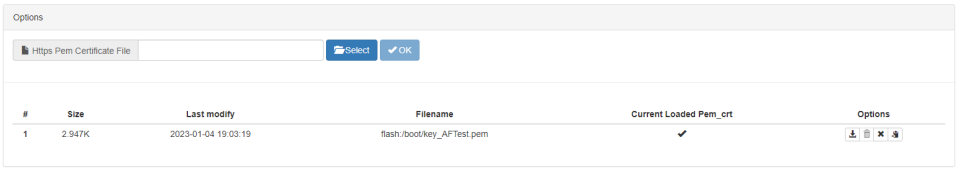


10. Select OK.

The GUI will refresh.

11. Login to the GUI.

12. Select Security.
13. Select Https Pem_crt.
14. Verify the Current Loaded Pem_crt.



15. Select the Download icon to download the pem file.
16. Select the Cancel icon to cancel the current loaded pem file. This will cause the GUI to be restarted back to the login display.
17. Select the Backup icon to create a pem_BAK file.
18. Select the Delete icon to delete the pem file.

    The pem file must be canceled before deleting is allowed.

TACACS+

Configuring TACACS+ on the Advanced Features involves the following configuration procedures:

- Configuring TACACS+
- Configuring the login access
- Creating users on the TACACS+ Server
- Delete TACACS+

TACACS+ may be set up via the GUI or via CLI commands. This procedure focuses on the CLI command method.

Connect to the Advanced Features

Connect to the Advanced Features unit. A connection to the unit may be established using two options:

- Directly connected to the Console Interface to COM Port using Putty/Serial connection
- Connected via the IP Management Interface using Putty/SSH connection

Configuring TACACS+

1. Press the Return key.
2. Enter enable.
3. Enter configure terminal.
4. Enter the following commands to configure TACACS+ on the Advanced Features unit:

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication login tacacs tacplus local
Switch(config)# aaa authorization exec tacacs tacplus local
Switch(config)# tacacs-server host mgmt-if xxx.xxx.xxx.xxx key secretkey
                 auth-port 49
```

TACACS+ Server IP Address

Key (optional) defined in the tac_plus.conf file

Configuring the login access

1. Enter the following commands to configure the login access on the Advanced Features to the TACACS+ server.

```
Switch(config)# line vty 0 7
Switch(config-line)# exec-timeout 0 0
Switch(config-line)# privilege level 4
Switch(config-line)# no line-password
Switch(config-line)# login authentication tacacs
Switch(config-line)# authorization exec tacacs
Switch(config-line)# exit
```

```
Switch(config)# exit
Switch#
```

Creating users on the TACACS+ Server

The following is an example.

Authentication Username = afuser1
Password = password1
Authorization Administrator privilege level 4

```
user = afuser1 {
global = cleartext "password1"
service = exec {
}
}
```

Delete TACACS+

Should the TACACS+ Server become unavailable for login and access to the unit and local login is desired, enter the following commands. This will delete all the TACACS+ configuration on the Advanced features unit and allow access.

Connect to the Advanced Features

Connect to the Advanced Features unit. A connection to the unit may be established using two options:

- Directly connected to the Console Interface to COM Port using Putty/Serial connection
- Connected via the IP Management Interface using Putty/SSH connection

1. Press the Return key.
2. Enter enable.
3. Enter configure terminal.
4. Enter the following command to delete TACACS+ on the unit.

```
Switch(config)# no aaa new-model
Switch(config)# exit
Switch#
```

TAP Group

TAP Groups are always unidirectional connections from an ingress entity to an egress entity. An ingress entity may be an individual port, range of ports, Link Aggregation Group or Port Group. Egress entities may be an individual port, range of ports or Link Aggregation Group. TAP Groups control the method that traffic is received on an ingress entity, filtering, packet modifications and distribution to an egress entity. TAP Group modifications are limited to adding or deleting ingress and/or egress ports. This section provides information on creating TAP Groups regardless of the application.

The following options should be considered prior to creating a TAP Group.

Direction Ingress

Port(s)	
Link Aggregation Name	*A Link Aggregation Group MUST have been previously created.*
Iloop	*The iloop port MUST have been previously created.*
Port Group	*A Port Group MUST have been previously created.*
Truncation	*Truncation MUST have been previously enabled.*
De-duplicate	*De-duplicate MUST have been previously enabled.*
Untag	
VLAN Mark	
Flow	*A Flow MUST have been previously created.*
Edit Packet	
Edit VLAN	

Direction Egress

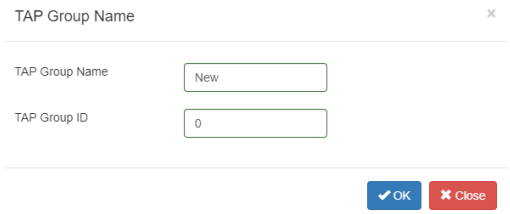
Port	
Link Aggregation Name	*A Link Aggregation Group MUST have been previously created.*
Timestamp	*Timestamp MUST have been previously enabled.*

Create a TAP Group

1. SelectTAP Management.
2. Select TAP Group Table.

3. Select + Add TAP Group.

The TAP Group Name panel will appear.

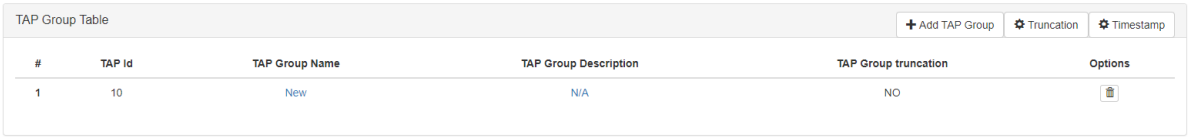


4. Enter the TAP Group Name.
5. Enter the TAP Group ID if desired, optional.

The system will assign an ID.

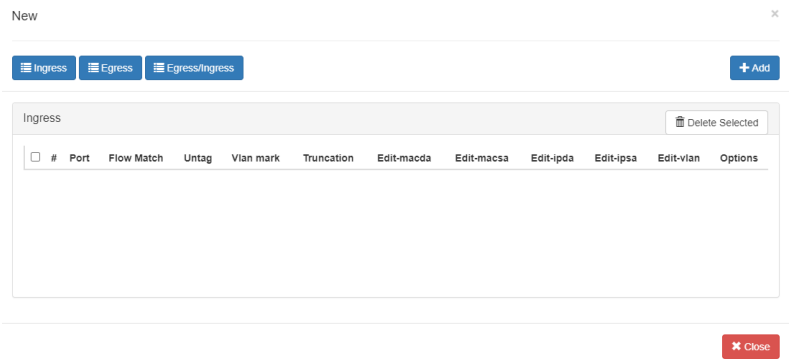
6. Select OK.

The TAP Group will be displayed.



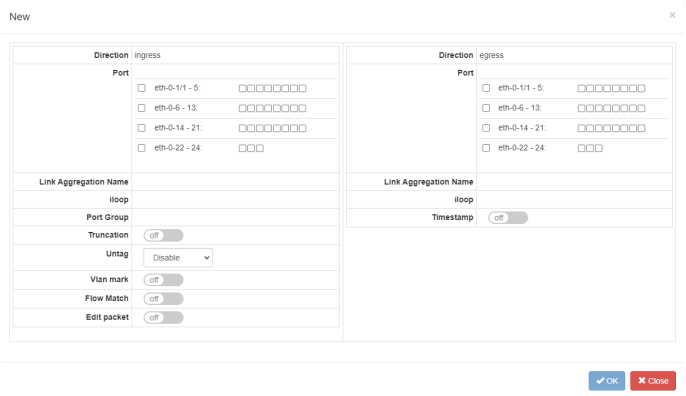
7. Select the TAP Group Name.

The TAP Group panel will appear.



8. Select the + Add.

The TAP Group add detail panel will appear.



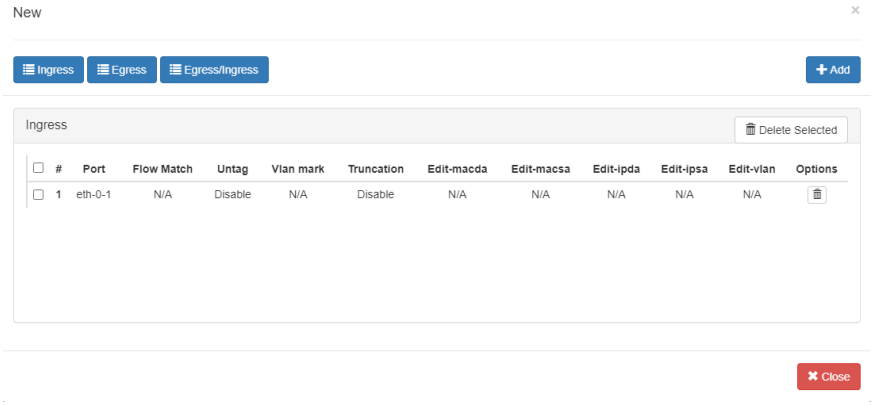
Direction Ingress

9. Select the desired ingress port(s), optional. Ingress ports may be selected individually or by range. Grayed port(s) may not be selected.
10. Select the desired Link Aggregation Name, optional. The link aggregation group MUST have been created previously.
11. Select the desired iloop port, optional. The iloop port MUST have been created previously.
12. Select the desired Port Group, optional. The port group MUST have been created previously.
13. Truncation may be applied. When enabled all other options are disabled. The truncation value will be applied per the global truncation value previously configured.
14. De-duplicate may be applied. The de-duplicate value will be applied per the global de-duplicate value previously configured.
15. Untag may be applied. Untag has three options, double-vlan, outer-vlan and inner-vlan. This option is controlled by the Svlan-tpid value applied to the ingress port(s). The port Svlan-tpid value may be displayed or modified on the Interface Management / Interface Status panel.
16. VLAN Mark may be applied. The range is 1-4094. This option is controlled by the Svlan-tpid value applied to the ingress port(s). The port Svlan-tpid value may be displayed or modified on the Interface Management / Interface Status panel.
17. Flow Match may be applied. A flow must be previously created to appear in the flow pull down panel. Flows control three functions, permit or deny traffic, provide filtering options and determine actions applied. The flow match option may be disabled and a pass all option will be applied. However, if no flow is applied the option to display TAP statistics, under the TAP Management / TAP Statistics panel is disabled.
18. Edit packet may be applied. DMAC, SMAC, SIP, DIP and VLAN packet modifications are supported. Packet modifications will be made to any ingress entity selected.

Direction Egress

19. Select the desired egress port(s), optional. Egress ports may be selected individually or by range. Grayed port(s) may not be selected.
20. Select the desired Link Aggregation Name, optional. The link aggregation group MUST have been previously created.
21. Select the desired iloop port, optional. The iloop port MUST have been created previously.
22. Timestamp may be applied. Timestamp MUST have been previously enabled.
23. Select OK to save the TAP Group.
24. Select Close to cancel.

The TAP Group will be displayed.



25. Select Ingress to display the entities and options. Individual ports may be deleted by selecting the Trash Can. A range of ports may be deleted by selecting the boxes and select Delete Selected.
26. Select Egress to display the entities and options. Individual ports may be deleted by selecting the Trash Can. A range of ports may be deleted by selecting the boxes and select Delete Selected.
27. Select Egress/Ingress to display the entities and options. Individual ports may be deleted by selecting the Trash Can. A range of ports may be deleted by selecting the boxes and select Delete Selected.
28. Select + Add to apply additional ingress or egress entities.

Truncation

The Advanced Features supports truncation. The truncation byte values range from 64 to 144 bytes, the default is 144 bytes. When truncation is applied to a packet the bytes after the truncation value are sliced. Example, if the truncation value is set to 80 bytes and a packet has 1024 bytes, after the packet is truncated, bytes 1 through 80 are kept and bytes 81 through 1024 are sliced. Any packet smaller than the truncation value will pass normally.
Truncation may be enabled, defined, and applied via the following methods:

- To a flow per the global value
- To an ACL, define value and assign it to egress port(s).
- To ingress port(s) via TAP Group

This section discusses the procedure to enable truncation and define the global value, apply truncation to a flow and apply truncation to an ACL. The procedure to apply truncation to ingress port(s) as the TAP group is created is discussed in the TAP Group section.

Enable Truncation and Define Global Value

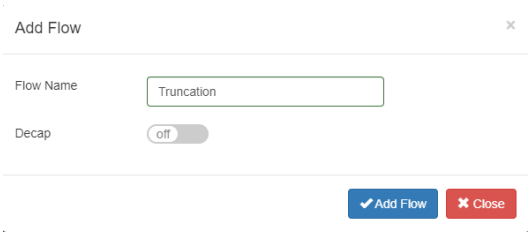
1. Select TAP Management.
2. Select TAP Group Table.
3. Select Truncation.

   The Truncation Length panel will be displayed.
4. Enable Truncation Length.
5. Enter the Truncation byte length.
6. Select OK.

Apply to a Flow

1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

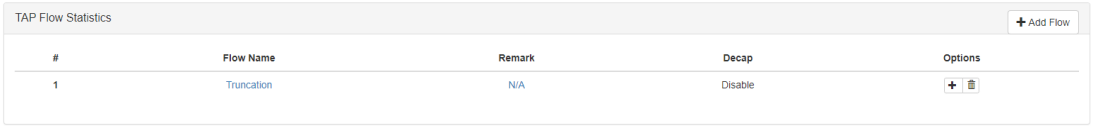
   The Add Flow panel will appear.



4. Enter the Flow Name.

5. Select Add Flow.

The flow will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule Options

7. Enable and define the desired options.

Flow Action Options

8. Enable Truncation.

All other action options are disabled.

9. Select OK.

10. Select the flow name to display the attributes.

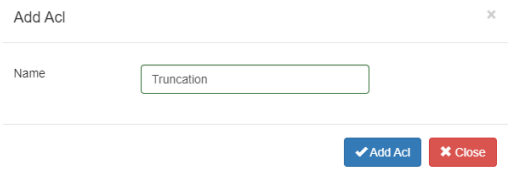
The Flow Entry panel will be displayed

Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

Apply to an ACL, Define Value and Assign to Egress Port(s)

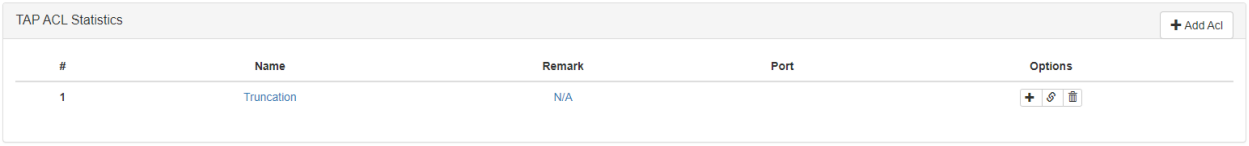
1. Select TAP Management.
2. Select ACL.
3. Select + Add ACL.

The Add ACL panel will appear.



4. Enter the ACL Name.
5. Select Add ACL.

The ACL will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

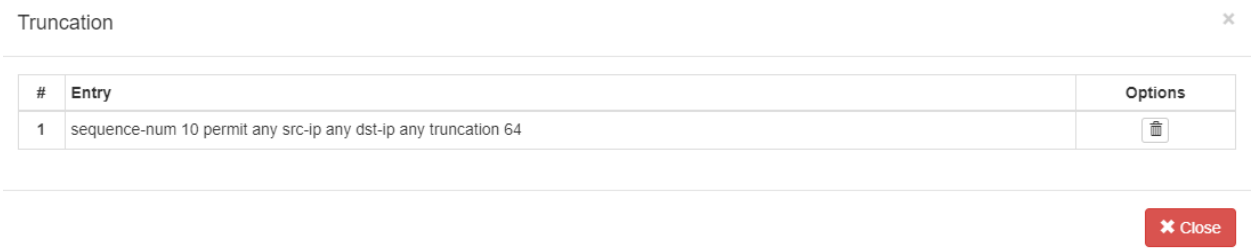
ACL Match Rule Options

7. Enable and define the desired options.

ACL Truncation Options

8. If desired, enable Truncation.
9. Enable Truncation Length.
10. Enter the desired value.
11. Select OK.
12. Select the ACL name to display the attributes.

The Flow Entry panel will be displayed



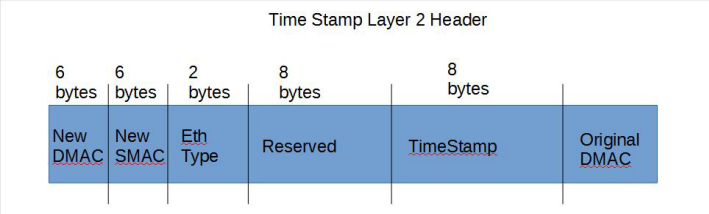
13. Select Apply under the Options column.
14. Select the desired egress port(s).
15. Select OK.

The ACL will be displayed with the assigned port(s).

Timestamp

In traditional data center applications, devices are used to sample network traffic. As traffic increases, there is a growing requirement for extended performance monitoring.

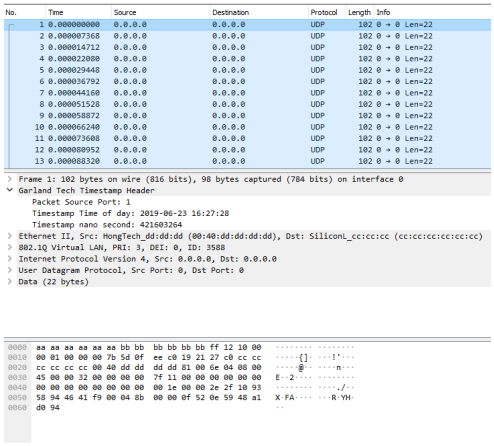
The Advanced Features provides a flexible packet time stamping function. The time stamp function is set up to insert a new 30-byte Layer 2 header before the original DMAC address. The Time Stamp Layer 2 header is defined as follows.



The time stamping is performed before the packet enters the switching chip. This function supports the standard Time of Day format and is accurate down to 8 nano-second resolutions. Software can distinguish these packets by the new EthType that has been added into the packet. The Time Stamp EthType is defined as 0xff12.

> *When Layer 3 routing or filtering is to be performed, the additional Time Stamp header needs to be removed.*

Garland Technology has produced a Wireshark plugin that will capture and display these packets as shown below.

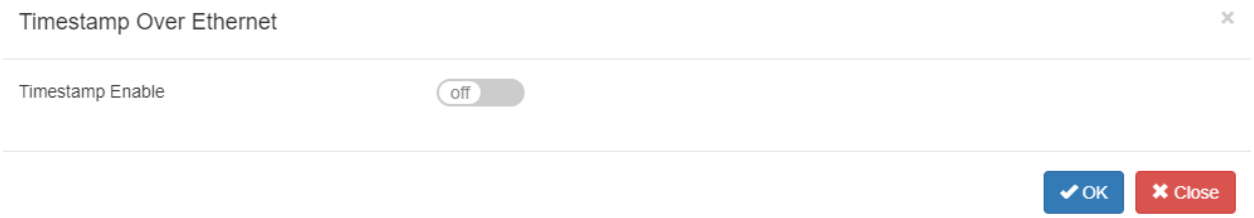


This section discusses the procedure to enable Timestamp. The procedure to apply Timestamp is discussed in the TAP Group section.

Enable Timestamp

1. Select TAP Management.
2. Select TAP Group Table.
3. Select Timestamp.

The Timestamp over Ethernet panel will appear.



4. Select Timestamp Enable.

5. Enter the Dst-mac for the new Time Stamp L2 segment.
6. Enter the Src-mac for the new Time Stamp L2 segment.
7. Enter 0xff12 for the Ether Type.
8. Select OK.

Timestamp may be applied to any egress port(s) when a TAP Group is created.

UDF

The Advanced Features provides the ability to configure a UDF (user defined filter) that is used as part of a flow to allow the system to filter traffic based on specific packet data. Layer2 UDFs are configured under TAP Management/UDF. While Layer3 and Layer4 UDFs are configured under TAP Management/Flow.

- Layer2, Layer3 and Layer4 are supported
- Up to four UDFs are supported, 0-3.
- Each offset value must be defined in multiples of 4 bytes up to 63 bytes

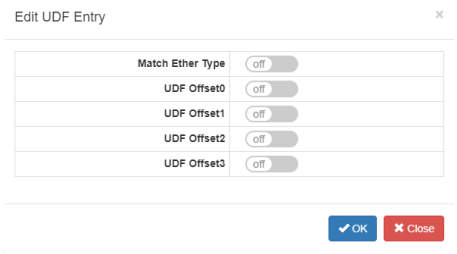
Create a Layer2 UDF

1. Select TAP Management.
2. Select UDF.
3. Select + Add UDF.

The Add UDF panel will be displayed.

4. The UDF Type displayed, l2 Header.
5. Select the UDF ID.
6. Select Add UDF.
7. Select the UDF Name to display, 0-3.
8. Select the Edit icon in the option column to edit the UDF entry.

The Edit UDF Entry panel will be displayed.



Match Ether Type option may be enabled. If enabled, then the Value-Wildcard option will be presented.

UDF Offset0 option may be enabled. If enabled, then the Value option will be presented.

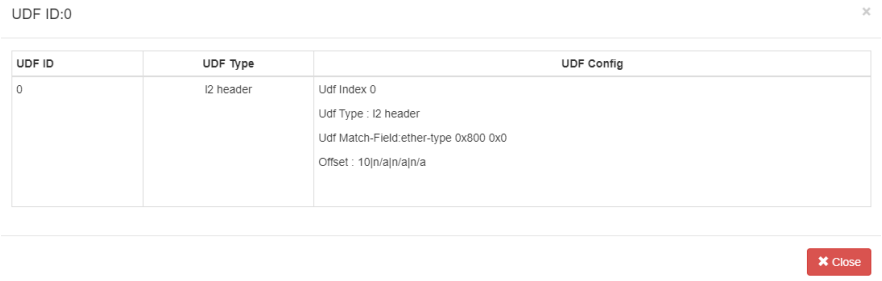
UDF Offset1 option may be enabled. If enabled, then the Value option will be presented.

UDF Offset2 option may be enabled. If enabled, then the Value option will be presented.

UDF Offset3 option may be enabled. If enabled, then the Value option will be presented.

9. Enable Match Ether Type.
10. Enter the desired Value and Wildcard.
11. Enable the desired UDF Offset, 0-3. All four Offsets may be enabled.
12. Enter the desired UDF Offset Value, 0-63. Value must be entered in multiples of 4.
13. Select OK.
14. Select the UDF Name, 0-4 to display.

The UDF ID panel will be displayed.



Apply an Layer2 UDF to a Flow

1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

The Add Flow panel will be displayed.

4. Enter the Flow Name.
5. Select Add Flow.
6. Select + in the options column to create an entry.
7. Enable UDF in the Match Rule section.
8. Select the UDF Type, Layer 2.
9. Select the UDF ID, 0-3.
10. Select the Offset Opt options.
11. Select the UDFx type.

If value is selected, then the UDFx Value and UDFx Wildcard options will be displayed.

12. Enter the desired UDFx Value.
13. Enter the desired UDFx Wildcard.
14. Select OK to save the flow.

Create and Apply a Layer3/Layer4 UDF

1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

The Add Flow panel will be displayed.

4. Enter the Flow Name.
5. Select Add Flow.
6. Select + in the options column to create an entry.
7. Enable UDF in the Match Rule section.
8. Select Layer3 or Layer4.
9. Enter the Value.
10. Enter the Wildcard.
11. Enter the Offset, 0-60. Value must be entered in multiples of 4.
12. Select OK to save the flow.

ACL

The Advanced Features provides the ability to configure an ACL (egress ip access-list) that allow the system to filter and/or modify traffic packets. An ACL provides these functions via entries. An ACL may have one or more entries. The entries within an ACL act individually to provide the overall ACL requirements. An ACL entry may be configured as a permit or denied. Permit and deny entries may be combined within the same ACL.

An entry has two configuration considerations:

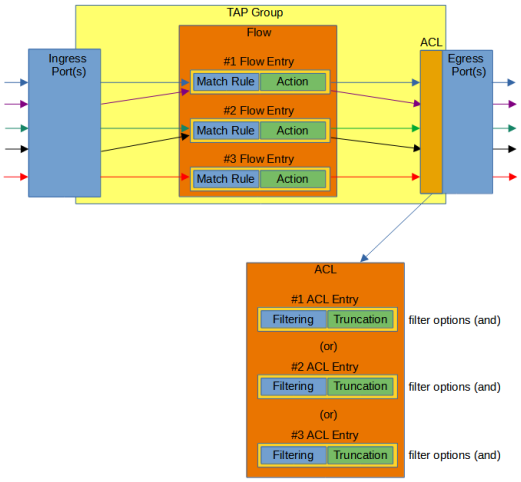
- Filtering
- Truncation

  Truncation may be applied per the global value length or applied per a unique value length.

The truncation modifications, if enabled are performed on the traffic packets that are defined and allowed to pass via the entry filtering section.

Figure 1 expresses the basic concepts of an ACL. In this example the ACL contains three entries. As entries are added, a priority is established. The highest priority is assigned to entry #1, the first entry added to the ACL. Followed by entry #2 and entry #3. Entries may be added or deleted, but not modified.

Figure 1



Also as shown in Figure 1, the entry filtering options are considered by the system as “and” options. Meaning for traffic to be permitted or denied, it must match all defined filtering options.

The entry priority is considered by the system as (or). Meaning if traffic packets are presented to an ACL, entry #1 the highest priority is considered first. If the traffic matches the priority #1 entry, then it is permitted or denied to the egress port(s). If not, then entry #2 is considered followed by entry #3. This process is continued for all entries within the ACL. If, however, no entry matches a specific traffic, the traffic will be dropped.

The ACL shown in Figure 2 accomplishes the following:

1. If a traffic packet has an IPv4 source IP address of 10.10.10.10 it will pass.
2. If a traffic packet has an IPv4 source IP address of 10.10.10.11 it will pass. Any packet larger than 80 bytes will be truncated at 80 bytes.
3. If a traffic packet has an IPv4 source IP address of 10.10.10.12 it will pass. Any packet larger than 100 bytes will be truncated at 100 bytes.

4. If a traffic packet has an IPv4 source IP address of 10.10.10.13 and IPv4 destination IP address of 10.10.10.50 it will pass.

Figure 2

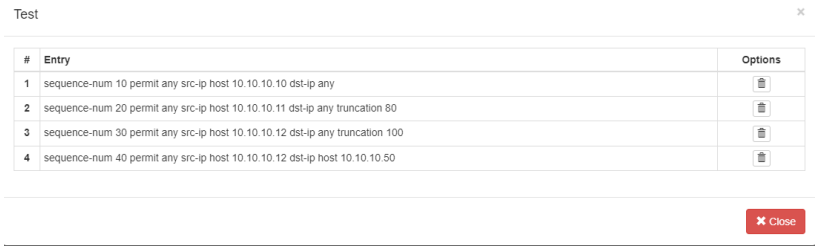
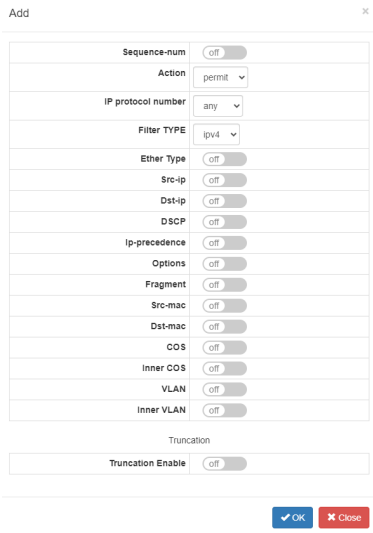


Figure 3 is an example of adding a new ACL entry. It displays the default options.

Figure 3



Sequence-num may be enabled. If enabled, then the Value option will be presented. If disabled, then the system will automatically apply a sequence-number and the entry will be added as the last entry within the ACL.

Action may be configured as either permit or deny.

Ip Protocol number may be used to select a specific protocol type.

Filter Type may be used to select IPv4 or IPv6.

Ether Type may be enabled. If enabled, then the Value and Wildcard options will be presented.

Src-ip may be enabled. If enabled, then the Source IP and Source Wildcard options will be presented.

Dst-ip may be enabled. If enabled, then the Destination IP and Destination Wildcard options will be presented.

DSCP may be enabled. If enabled, then the Value option will be presented.

Ip-precedence may be enabled. If enabled, then the Value option will be presented.

Options is N/A.

Fragment may be enabled. If enabled, then the Fragment Option will be presented.

Src-mac may be enabled. If enabled, then the Type option will be presented. If host is selected, then the Src-mac option will be presented. If MAC is selected, then the Src-mac and Wildcard options will be presented.

Dst-mac may be enabled. If enabled, then the Type option will be presented. If host is selected, then the Dst-mac option will be presented. If MAC is selected, then the Dst-mac and Wildcard options will be presented.

COS may be enabled. If enabled, then the COS Value option will be presented.

Inner COS may be enabled. If enabled, then the Inner COS Value option will be presented.

VLAN may be enabled. If enabled, then the ID and Wildcard options will be presented.

Inner VLAN may be enabled. If enabled, then the Inner VLAN IP and Wildcard options will be presented.

Create an ACL

1. Select TAP Management.
2. Select ACL.
3. Select + Add Acl.

    The Add Acl panel will be displayed.

4. Enter the Name.
5. Select Add Acl.
6. Select + in the options column to create an entry.
7. Enable, define, or select all desired entry options.
8. Select OK.

9. Select the Name to display the ACL entries.
10. Select the trash can in the options column to delete the ACL.

Apply an ACL

ACLs may be applied to egress port(s) via two methods:

Method 1

1. Select the chain icon in the ACL options column for the desired ACL.
2. Select all desired port(s).
3. Select OK.

Method 2

1. Select Interface Management.
2. Select Interface Status.
3. Select the N/A for the desired port(s) in the filter column.
4. Select enable.
5. Select the desired ACL.
6. Select OK.

Flow

The Advanced Features provides the ability to create flows that allow the system to filter and/or modify traffic packets. A flow provides these functions via entries. A flow may have one or more entries. The entries within a flow act individually to provide the overall flow requirements. A flow entry may

be configured as a permit or deny. Permit and deny entries may be combined within the same flow.

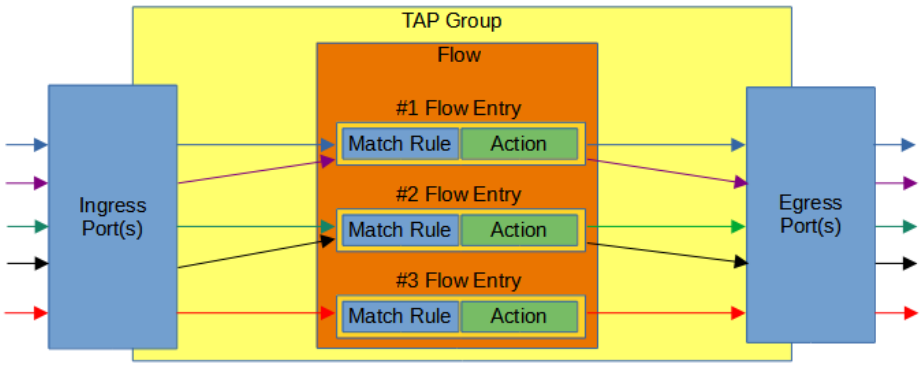
An entry has two configuration considerations:

- Match Rule
  - The match rule section provides traffic filtering.
- Action
  - The action section provides traffic modification.

The entry action section modifications, if enabled are performed on the traffic packets that are defined and allowed to pass via the entry match rule section.

Figure 1 expresses the basic concepts of a flow. In this example the flow contains three entries. As illustrated, an entry may accommodate one or more traffic streams. Also, as entries are added, a priority is established. Entries may be added or deleted, but not modified.

Figure 1

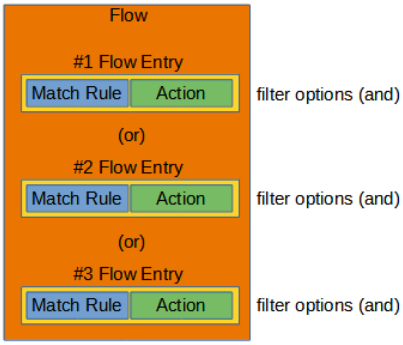


As shown in Figure 2, the entry match rule options are considered by the system as “and” options. Meaning for traffic to be permitted or denied, it must match all defined filtering options.

The entry priority is considered by the system as (or). Meaning if traffic packets are presented to a flow, entry #1 the highest priority is considered first. If the traffic matches the priority #1 entry, then it is permitted or denied to the egress port(s). If not, then entry #2 is considered followed by entry #3.

This process is continued for all entries within the flow. If, however, no entry matches a specific traffic, the traffic will be dropped.

Figure 2

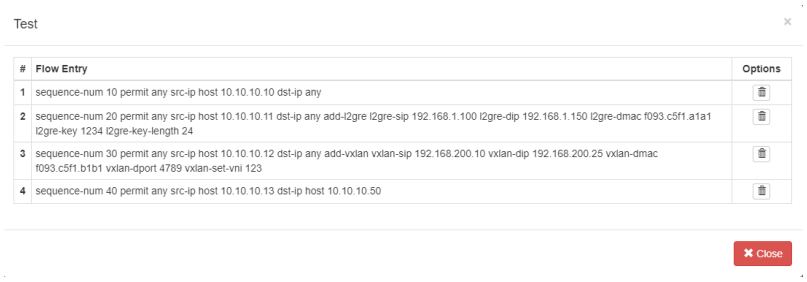


The flow shown in Figure 3 accomplishes the following:

1. If a traffic packet has an IPv4 source IP address of 10.10.10.10 it will pass.
2. If a traffic packet has an IPv4 source IP address of 10.10.10.11 it will pass. There is an action defined to add a l2GRE header.
3. If a traffic packet has an IPv4 source IP address of 10.10.10.12 it will pass. There is an action defined to add a VXLAN header.
4. If a traffic packet has an IPv4 source IP address of 10.10.10.13 and IPv4 destination IP address of 10.10.10.50 it will pass.

   All other traffic packets will be dropped.

Figure 3



The flow shown in Figure 4 is an example of a pass all for IPv4 and IPv6 traffic.

1. This entry will pass all IPv4 traffic packets.
2. This entry will pass all IPv6 traffic packets.

Figure 4

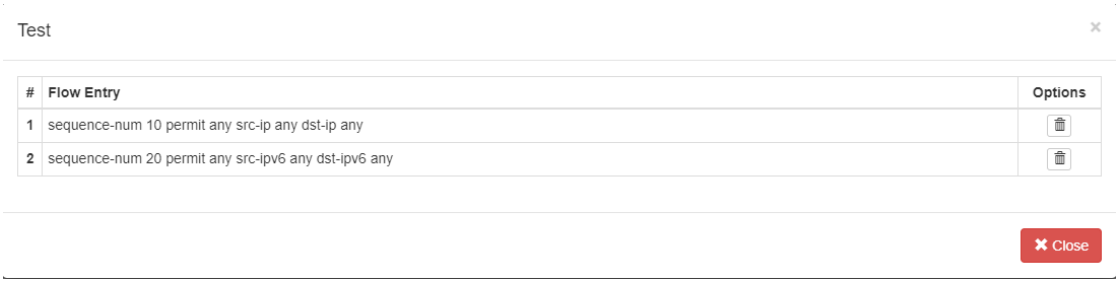


Figure 5 is an example of adding a new flow entry. It displays the default match rule section.

Sequence-num may be enabled. If enabled, then the Value option will be presented. If disabled, then the system will automatically apply a sequence-number and the entry will be added as the last entry within the ACL.

Action may be configured as either permit or deny.

Ip Protocol number may be used to select a specific protocol type.

Protocol Version may be used to select IPv4 or IPv6.

Ether Type may be enabled. If enabled, then the Value and Wildcard options will be presented.

Src-ip may be enabled. If enabled, then the Source IP and Source Wildcard options will be presented.

Dst-ip may be enabled. If enabled, then the Destination IP and Destination Wildcard options will be presented.

DSCP may be enabled. If enabled, then the Value option will be presented.

Ip-precedence may be enabled. If enabled, then the Value option will be presented.

Options is N/A.

Fragment may be enabled. If enabled, then the Fragment Option will be presented.

Src-mac may be enabled. If enabled, then the Type option will be presented. If host is selected, then the Src-mac option will be presented. If MAC is selected, then the Src-mac and Wildcard options will be presented.

Dst-mac may be enabled. If enabled, then the Type option will be presented. If host is selected, then the Dst-mac option will be presented. If MAC is selected, then the Dst-mac and Wildcard options will be presented.

COS may be enabled. If enabled, then the COS Value option will be presented.

Inner COS may be enabled. If enabled, then the Inner COS Value option will be presented.

VLAN may be enabled. If enabled, then the ID and Wildcard options will be presented.

Inner VLAN may be enabled. If enabled, then the Inner VLAN IP and Wildcard options will be presented.

UDF may be enabled. Layer2 UDFs must have been previously created.

Figure 5

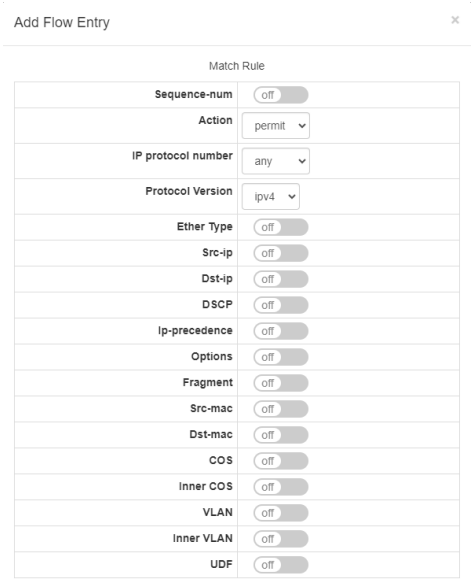


Figure 6 is an example of adding a new flow entry. It displays the default action section.

Truncation may be enabled. If enabled, then the global truncation value configured under the TAP Management/TAP Group Table/Truncation feature will be applied.

Untag option allows for the removal of packet VLANs.

Strip-header may be enabled. If enabled, then the Strip-position and Strip-offset options will be presented.

VLAN mark may be enabled. If enabled, then the ID option will be presented.

Edit packet may be enabled. If enabled:
Add-macaddr option will be presented. If enabled, then the Dst-mac and Src-mac options will be Presented.
Edit-macda may be enabled. If enabled, then the Dst-mac option will be presented.
Edit-macsa may be enabled. If enabled, then the Src-mac option will be presented.
Edit-ipda may be enabled. If enabled, the Dst-ip Type and Dst-ip options will be presented.
Edit-ipsa may be enabled. If enabled, the Src-ip Type and Src-ip options will be presented.
Edit-vlan may be enabled. If enabled, then the Type, ID and COS options will be presented.

Add l2GRE may be enabled. If enabled, then the L2gre-src-ip, L2gre-dest-ip, L2gre-dest-mac, L2gre-key-length and L2gre-key-num options will be presented.

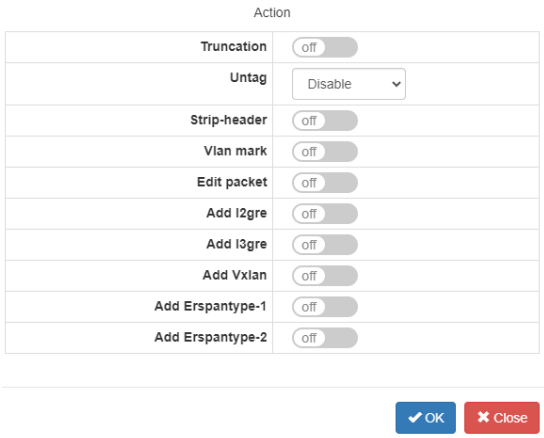
Add l3GRE may be enabled. If enabled, then the L3gre-src-ip, L3gre-dest-ip and L3gre-dest-mac option will be presented.

Add Vxlan may be enabled. If enabled, then the Vxlan-dest-mac, Vxlan-src-ip, Vxlan-dest-ip, Vxlan-dst-port, Vxlan-src-port and Vxlan-vni-num options will be presented. The default Vxlan-dst-port is 4789.

Add Erspantype-1 may be enabled. If enabled, then the Erspantype-1-dest-mac, Erspantype-1-src-ip and Erspantype-1-dest-ip options will be presented.

Add Erspantype-2 may be enabled. If enabled, then the Erspantype-2-dest-mac, Erspantype-2-src-ip, Erspantype-2-dest-ip and Erspantype-2-spanid options will be presented.

Figure 6



When creating a TAP Group the system allows for:

A specific flow to be selected for the ingress port(s). If a specific flow is selected, then the system allows for additional TAP Groups to be created using the same ingress ports.

No specific flow to be selected for the ingress port(s). If no specific flow is selected, then the system does not allow for additional TAP Groups to be created using the same ingress ports and they will appear grayed out when creating additional TAP Groups.

If a flow was selected when a TAP Group was created, then Flow Statistics may be displayed under the TAP Management/TAP Statistics panel.

A flow may be selected when creating a TAP Group that does not have any entries. If this happens then all traffic will be dropped.

A flow and entries may be created via CLI commands through the console interface, SSH/management interface or through the rpc-api service. If a flow and entries are created via CLI commands, they may be displayed in the GUI.

A flow may be used in multiple TAP Groups.

If a flow is assigned to a TAP Group(s) the entries may be modified without having to make any modifications to the TAP Group.

Create a Flow

1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

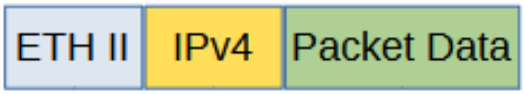
   The Add Flow panel will be displayed.
4. Enter the Flow Name.
5. Select Add Flow.
6. Select + in the options column to create an entry.
7. Select the Flow Name to display the flow entries.
8. Select the trash can in the options column to delete the flow.

I2GRE

Encapsulate

When a packet is encapsulated with a I2GRE header the new I2GRE header segments are added to the original packet. The I2GRE header segments consists of L2, L3 and I2GRE as shown below.

Original Packet



I2GRE Encapsulated Packet

Encapsulating a packet with a I2GRE header involves two configuration procedures.

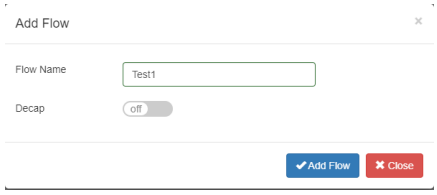
- Create a flow to add the I2GRE header
- Create a TAP Group

  This section discusses the procedure to create a flow to add the I2GRE header. The procedure to create a TAP Group is discussed in the TAP Group section.

Create a Flow

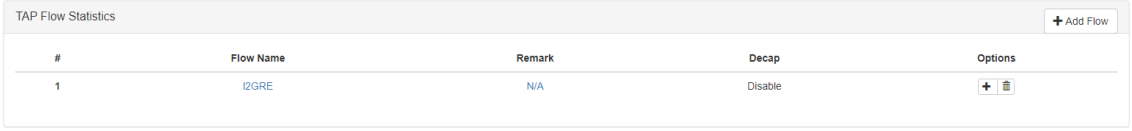
1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

   The Add Flow panel will appear.



4. Enter the Flow Name.
5. Select Add Flow.

   The flow will be displayed.



6. Select the + in the Options column to define the attributes.

   The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule Options

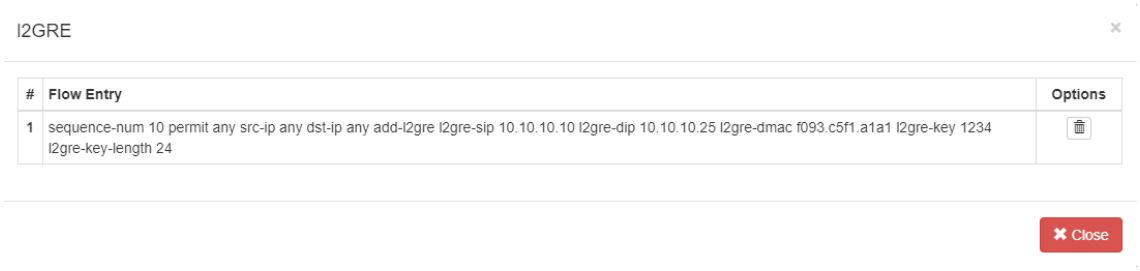
7. Select permit for the Action.
8. Select any for the IP Protocol Number.
9. Select any other desired options and enter the desired values to define which packets will be encapsulated. The defaults may be used to encapsulate all packets.

Flow Action Options

10. Enable Add l2gre.
11. Enter the desired L2gre-src-ip. This defines the source IP address in the L3 segment of the l2GRE header.
12. Enter the desired L2gre-dest-ip. This defines the destination IP address in the L3 segment of the l2GRE header.
13. Enter the desired L3gre-dest-mac. This defines the destination MAC address in the L2 segment of the l2GRE header.
14. Select the desired L2gre-key-length, 16, 20, 24, 32, the default is 24.
15. Enter the desired L2gre-key-num.
16. Select OK.

17. Select the flow name to display the attributes.

The Flow Entry panel will be displayed



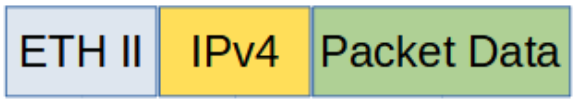
Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

Decapsulate All l2GRE

When a l2GRE packet is decapsulated the l2GRE header segments are removed from the packet as shown below.

l2GRE Encapsulated Packet

l2GRE Decapsulated Packet



Decapsulating the l2GRE header from a packet(s) involves two configuration procedures.

- Create a flow to strip the l2GRE header
- Create a TAP Group

This section discusses the procedure to create a flow to strip the l2GRE header. The procedure to create a TAP Group is discussed in the TAP Group section.

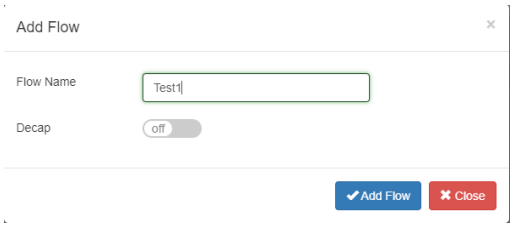
Create a Flow

1. Select TAP Management.

2. Select Flow.

3. Select + Add Flow.

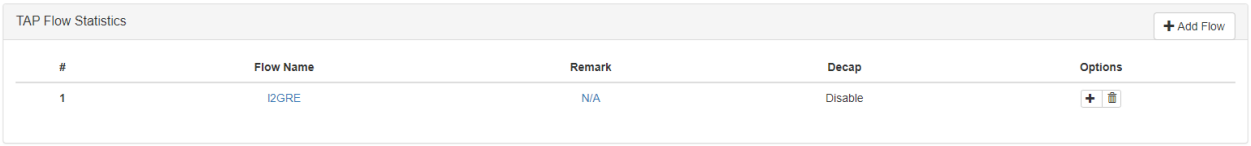
The Add Flow panel will appear.



4. Enter the Flow Name.

5. Select Add Flow.

The flow will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule Options

7. Select permit for the Action.

8. Select nvgre for the IP Protocol Number.

9. Select any other desired options and enter the desired values to define which l2GRE packets will be decapsulated. The defaults may be used to decapsulate all l2GRE packets.

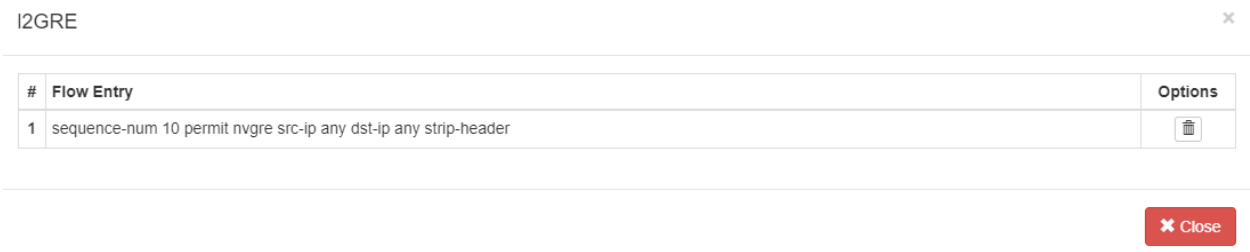
Flow Action Options

10. Enable Strip-header.

11. Select OK.

12. Select the flow name to display the attributes.

The Flow Entry panel will be displayed



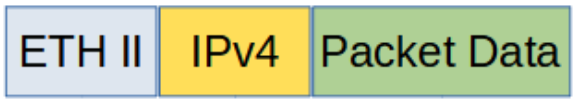
Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

Decapsulate l2GRE per VNI

When a l2GRE packet is decapsulated the l2GRE header segments are removed from the packet as shown below.

l2GRE Encapsulated Packet

l2GRE Decapsulated Packet



Decapsulating the l2GRE header from a packet(s) per VNI involves two configuration procedures.

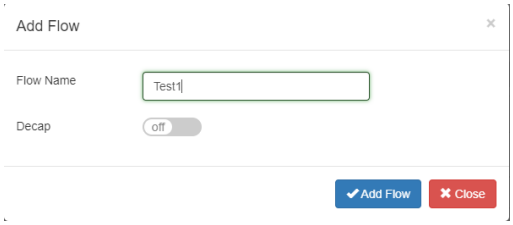
- Create a flow to strip the l2GRE header
- Create a TAP Group

This section discusses the procedure to create a flow to strip the I2GRE header. The procedure to create a TAP Group is discussed in the TAP Group section.

Create a Flow

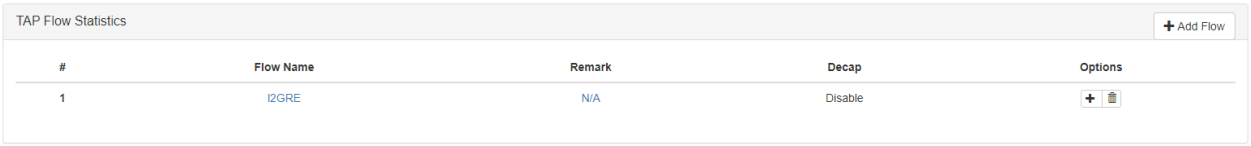
1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

The Add Flow panel will appear.



4. Enter the Flow Name.
5. Select Add Flow.

The flow will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria

- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

  Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule Options

7. Select permit for the Action.

8. Select nvgre for the IP Protocol Number.

9. Enable NVGRE-VNI.

10. Enter the desired Value.

11. Enter the desired Wildcard.

12. Select any other desired options and enter the desired values to define which l2GRE packets will be decapsulated. The defaults may be used to decapsulate all l2GRE packets.

Flow Action Options

13. Enable Strip-header.

14. Select OK.

15. Select the flow name to display the attributes.

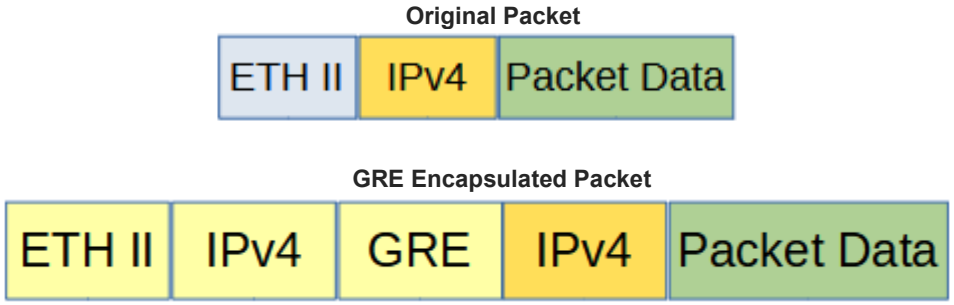
    The Flow Entry panel will be displayed

Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

l3GRE

Encapsulate

When a packet is encapsulated with a l3GRE header the original L2 segment is removed from the packet and the new l3GRE header segments are added. The l3GRE header segments consists of L2, L3 and GRE as shown below.



Encapsulating a packet with a l3GRE header involves two configuration procedures.

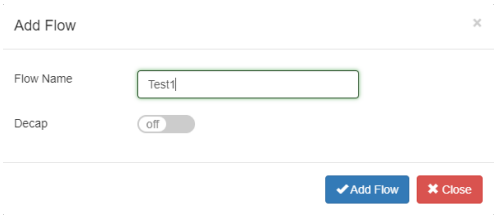
- Create a flow to add the l3GRE header
- Create a TAP Group

  This section discusses the procedure to create a flow to add the l3GRE header. The procedure to create a TAP Group is discussed in the TAP Group section.

Create a Flow

1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

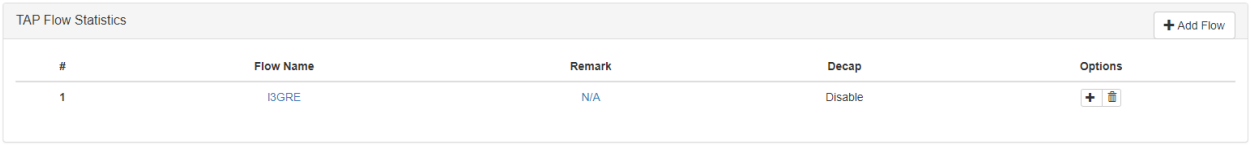
   The Add Flow panel will appear.



4. Enter the Flow Name.

5. Select Add Flow.

The flow will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule Options

7. Select permit for the Action.

8. Select any for the IP Protocol Number.

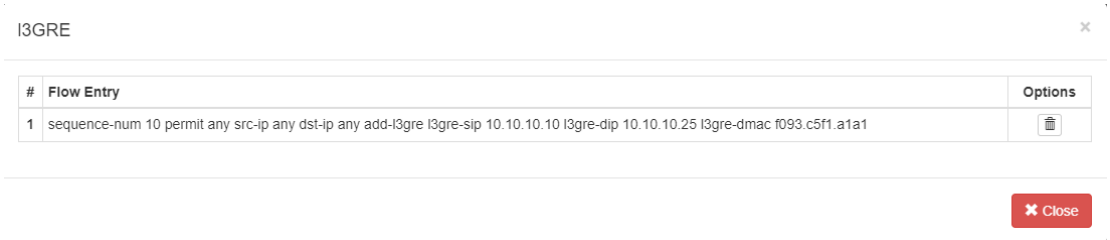
9. Select any other desired options and enter the desired values to define which packets will be encapsulated. The defaults may be used to encapsulate all packets.

Flow Action Options

10. Enable Add l3gre.
11. Enter the desired L3gre-src-ip. This defines the source IP address in the L3 segment of the l3GRE header.
12. Enter the desired L3gre-dest-ip. This defines the destination IP address in the L3 segment of the l3GRE header.
13. Enter the desired L3gre-dest-mac. This defines the destination MAC address in the L2 segment of the l3GRE header.
14. Select OK.

15. Select the flow name to display the attributes.

The Flow Entry panel will be displayed

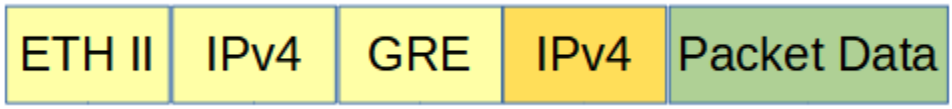


Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

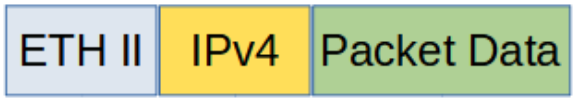
Decapsulate

When a l3GRE packet is decapsulated the l3GRE header segments are removed from the packet and a new L2 segment is added as shown below.

l3GRE Encapsulated Packet



l3GRE Decapsulated Packet



Decapsulating the l3GRE header from a packet(s) involves two configuration procedures.

- Create a flow to strip the l3GRE header

- Create a TAP Group

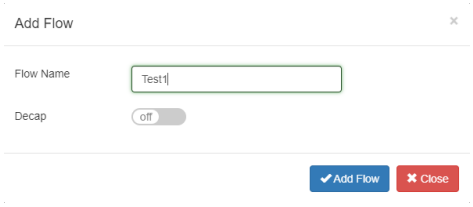
  This section discusses the procedure to create a flow to strip the GRE header. The procedure to create a TAP Group is discussed in the TAP Group section.

Create a Flow

1. Select TAP Management.
2. Select Flow.

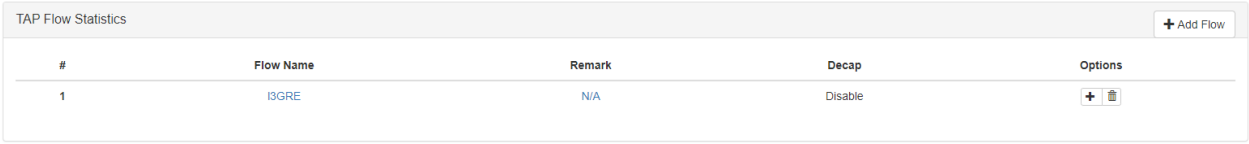
3. Select + Add Flow.

   The Add Flow panel will appear.



4. Enter the Flow Name.
5. Select Add Flow.

   The flow will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule Options

7. Select permit for the Action.
8. Select gre for the IP Protocol Number.
9. Select any other desired options and enter the desired values to define which l3GRE packets will be decapsulated. The defaults may be used to decapsulate all l3GRE packets.

Flow Action Options

10. Enable Strip-header.
11. Enable Edit packet.
12. Enable Edit-macda.
13. Enter the desired Dst-mac. This defines the destination MAC address for the new L2 segment added to the packet.
14. Enable Edit-macsa.
15. Enter the desired Src-mac. This defines the source MAC address for the new L2 segment added to the packet.
16. Select OK.
17. Select the flow name to display the attributes.

The Flow Entry panel will be displayed

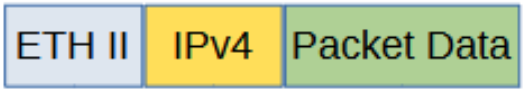
Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

VXLAN

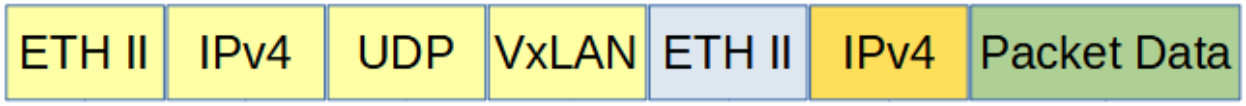
Encapsulate

When a packet is encapsulated with a VxLAN header the new VxLAN header segments are added to the original packet. The VxLAN header segments consists of L2, L3, UDP and VxLAN as shown below.

Original Packet



VxLAN Encapsulated Packet



Encapsulating a packet with a VxLAN header involves two configuration procedures.

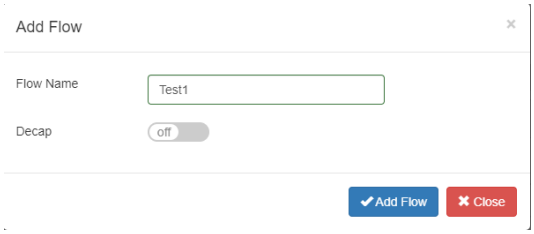
- Create a flow to add the VxLAN header
- Create a TAP Group

This section discusses the procedure to create a flow to add the VxLAN header. The procedure to create a TAP Group is discussed in the TAP Group section.

Create a Flow

1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

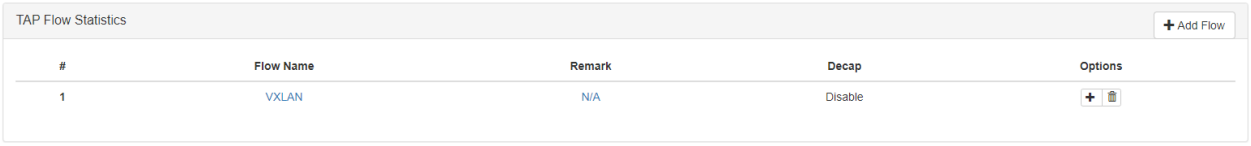
The Add Flow panel will appear.



4. Enter the Flow Name.

5. Select Add Flow.

The flow will be displayed.



6. Select the + in the Options column to define the attributes.

   The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule Options

7. Select permit for the Action.
8. Select any for the IP Protocol Number.
9. Select any other desired options and enter the desired values to define which packets will be encapsulated. The defaults may be used to encapsulate all packets.

Flow Action Options

10. Enable Add Vxlan.
11. Enter the desired Vxlan-dest-mac. This defines the destination MAC address in the L2 segment of the VXLAN header.
12. Enter the desired Vxlan-src-ip. This defines the source IP address in the L3 segment of the VXLAN header.
13. Enter the desired Vxlan-dest-ip. This defines the destination IP address in the L3 segment of the VXLAN header.
14. Enable Vxlan-dst-port if other than the default 4789 is desired in the VXLAN header. The system will automatically define the UDP destination port value as 4789.
15. Enable Vxlan-src-port if other than the default 0 is desired in the VXLAN header. The system will automatically define the UDP source port value as 0.
16. Enter the desired Vxlan-vni-num.
17. Select OK.
18. Select the flow name to display the attributes.

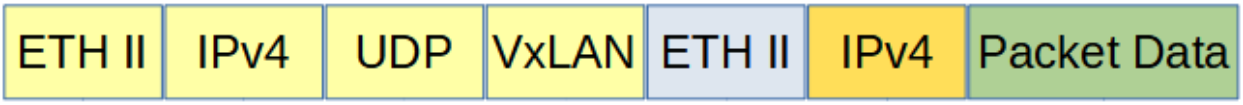
The Flow Entry panel will be displayed

Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

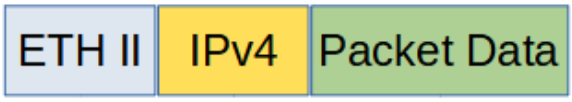
Decapsulate

When the VxLAN header is decapsulated from a packet, the VxLAN header segments are removed as shown below.

VxLAN Encapsulated Packet



VxLAN Decapsulated Packet



Advanced Features supports two methods to decapsulate VxLAN headers.

- Packets per VxLAN VNI
- All VxLAN packets

The flow to decapsulate VxLAN packets per VxLAN VNI may be configured via the GUI. The flow to decapsulate all VxLAN packets must be configured via CLI commands.

Decapsulating the VxLAN header from a packet(s) involves two configuration procedures.

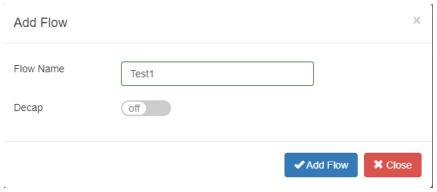
- Create a flow to strip the VxLAN header
- Create a TAP Group

This section discusses the procedure to create a flow to strip the VxLAN header. The procedure to create a TAP Group is discussed in the TAP Group section.

Create a Flow (Decapsulate VXLAN per VNI)

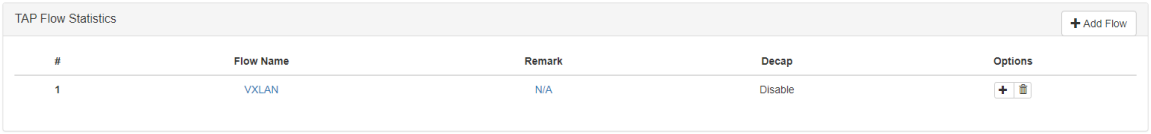
1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

The Add Flow panel will appear.



4. Enter the Flow Name.
5. Select Add Flow.

The flow will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria

- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

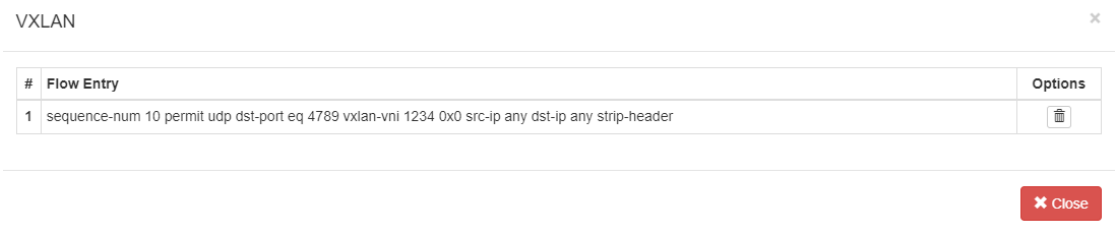
Flow Match Rule Options

7. Select permit for the Action.
8. Select udp for the IP Protocol Number.
9. Enable Dst-port.
10. Select eq for the Type.
11. Enter 4789 for the Port.
12. Enable Vxlan-VNI.
13. Enter the desired VxLAN VNI ID.
14. Enter the desired Wildcard.
15. Select any other desired options and enter the desired values to define which packets will be decapsulated. The defaults may be used.

Flow Action Options

16. Enable Strip-header.
17. Select OK.
18. Select the flow name to display the attributes.

The Flow Entry panel will be displayed



Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

Create a Flow (Decapsulate All VXLAN)

Decapsulating all VXLAN packets must be configured via CLI commands.

Connect to the Advanced Features

Connect to the Advanced Features unit. A connection to the unit may be established using two options:

- Directly connected to the Console Interface to COM Port using Putty/Serial connection
- Connected via the IP Management Interface using Putty/SSH connection

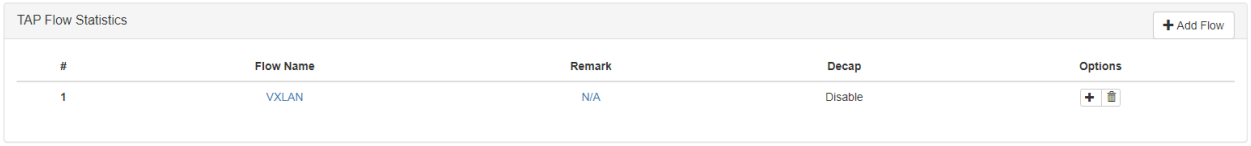
1. Press the Return key.
2. Enter enable.
3. Enter configure terminal.
4. Enter the following commands to create the flow.

```
Switch(config)# flow VXLAN
```

VXLAN is the flow name.

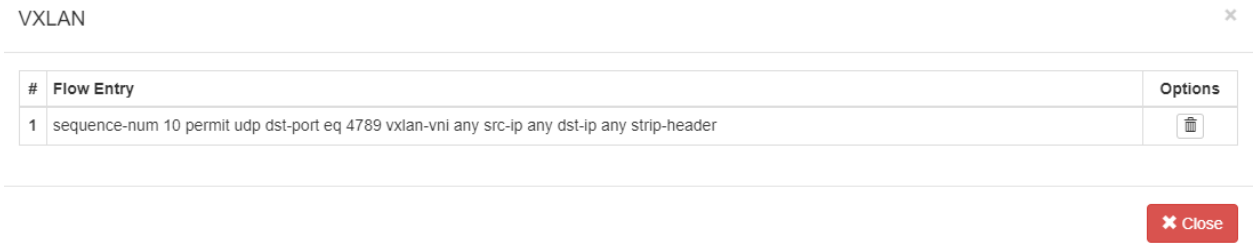
```
Switch(config-flow-VXLAN)# permit udp dst-port eq 4789 vxlan-vni any src-ip any
                           dst-ip any strip-header
```

5. Once the flow is created it will be displayed in the GUI.



6. Select the flow name to display the attributes.

The Flow Entry panel will be displayed



Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

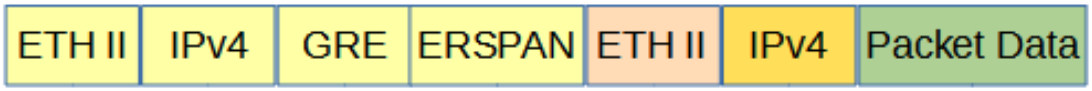
ERSPAN Type 1

Encapsulate

When a packet is encapsulated with an ERSPAN Type 1 header the new ERSPAN Type 1 header segments are added to the original packet. The ERSPAN Type 1 header segments consists of L2, L3, GRE and ERSPAN Type 1 as shown below.

Original Packet

ERSPAN Type 1 Encapsulated Packet



Encapsulating a packet with an ERSPAN Type 1 header involves two configuration procedures.

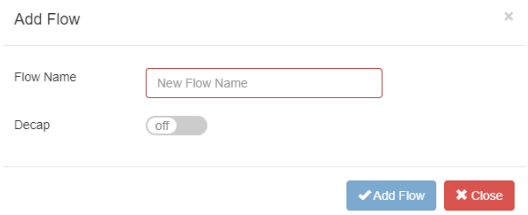
- Create a flow to add the ERSPAN Type 1 header
- Create a TAP Group

This section discusses the procedure to create a flow to add the ERSPAN Type 1 header. The procedure to create a TAP Group is discussed in the TAP Group section.

Create a Flow

1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

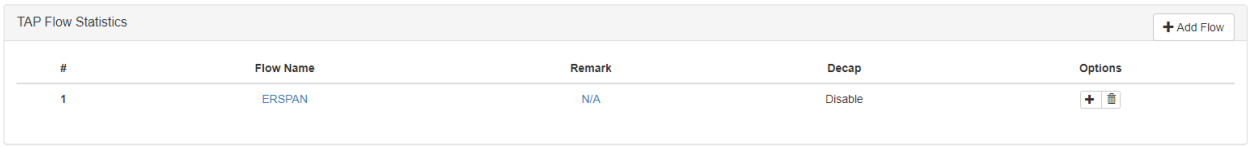
The Add Flow panel will appear.



4. Enter the Flow Name.

5. Select Add Flow.

The flow will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule Options

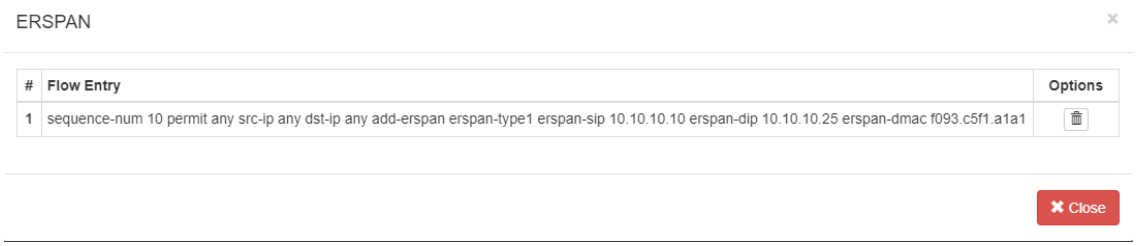
7. Select permit for the Action.
8. Select any for the IP Protocol Number.
9. Select any other desired options and enter the desired values to define which packets will be encapsulated. The defaults may be used to encapsulate all packets.

Flow Action Options

10. Enable Add Erspantype-1.
11. Enter the desired Erspantype-1-dest-mac. This defines the destination MAC address in the L2 segment of the ERSPAN header.
12. Enter the desired Erspantype-1-src-ip. This defines the destination IP address in the L3 segment of the ERSPAN header.
13. Enter the desires Erspantype-1-dest-ip. This defines the destination IP address in the L3 segment of the ERSPAN header.
14. Select OK.

15. Select the flow name to display the attributes.

The Flow Entry panel will be displayed

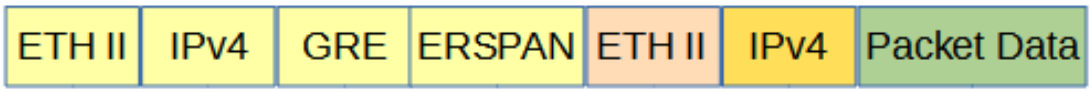


Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

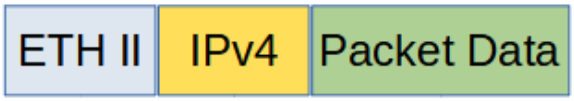
Decapsulate (New L2)

When this method is used to decapsulate an ERSPAN Type 1 packet the ERSPAN Type 1 header segments are removed from the packet along with the original L2 segment. A new L2 segment is added as shown below.

ERSPAN Type 1 Encapsulated Packet



ERSPAN Type 1 Decapsulated Packet



Decapsulating the ERSPAN Type 1 header from a packet(s) involves two configuration procedures.

- Create a flow to strip the ERSPAN Type 1 header
- Create a TAP Group

This section discusses the procedure to create a flow to strip the ERSPAN Type 1 header. The procedure to create a TAP Group is discussed in the TAP Group section.

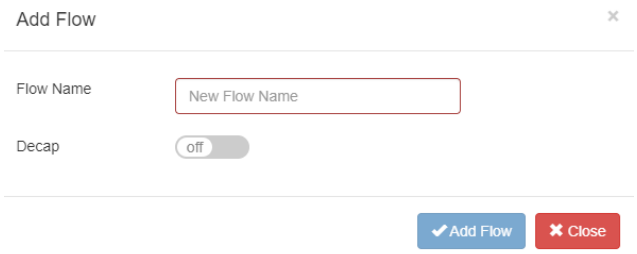
Create a Flow

1. Select TAP Management.

2. Select Flow.

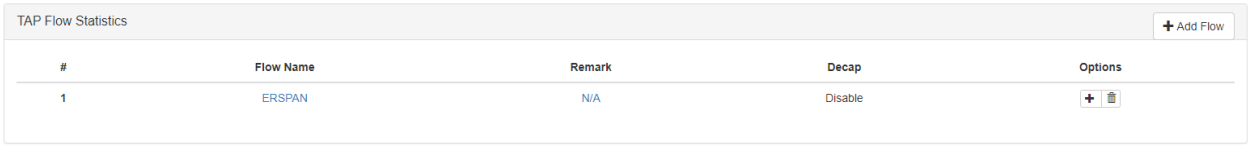
3. Select + Add Flow.

The Add Flow panel will appear.



4. Enter the Flow Name.
5. Select Add Flow.

The flow will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule Options

7. Select permit for the Action.
8. Select gre for the IP Protocol Number.

9. Select any other desired options and enter the desired values to define which ERSPAN packets will be decapsulated. The defaults may be used to decapsulate all ERSPAN packets.

Flow Action Options

10. Enable Strip-header.
11. Enable Strip-position.
12. Select L4 for the Type.
13. Enable Strip-offset.
14. Enter 4 for the Value.
15. Enable Edit packet.
16. Enable Edit-macda.
17 Enter the desired Dst-mac. This defines the destination MAC address for the new L2 segment added to the packet.
18. Enable Edit-macsa.
19. Enter the desired Src-mac. This defines the source MAC address for the new L2 segment added to the packet.
20. Select OK.
21. Select the flow name to display the attributes.

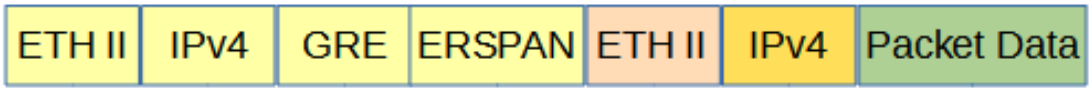
The Flow Entry panel will be displayed

Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

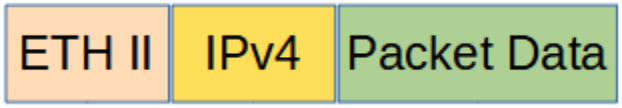
Decapsulate (Original Packet Retained)

When this method is used to decapsulate an ERSPAN Type 1 packet the ERSPAN Type 1 header segments are removed from the packet. The original packet is not modified as shown below.

ERSPAN Type 1 Encapsulated Packet



ERSPAN Type 1 Decapsulated Packet



Decapsulating the ERSPAN Type 1 header from a packet(s) involves two configuration procedures.

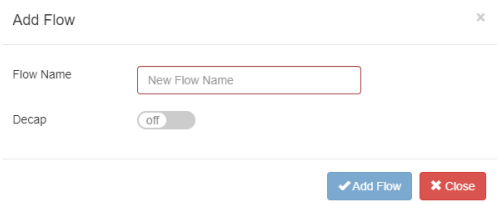
- Create a flow to strip the ERSPAN Type 1 header
- Create a TAP Group

  This section discusses the procedure to create a flow to strip the ERSPAN Type 1 header. The procedure to create a TAP Group is discussed in the TAP Group section.

Create a Flow

1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

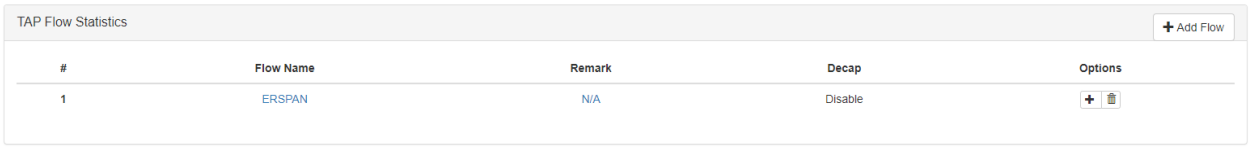
   The Add Flow panel will appear.



4. Enter the Flow Name.

5. Select Add Flow.

The flow will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule Options

7. Select permit for the Action.
8. Select any for the IP Protocol Number.
9. Select any other desired options and enter the desired values to define which ERSPAN packets will be decapsulated. The defaults may be used to decapsulate all ERSPAN packets.

Flow Action Options

10. Enable Strip-header.
11. Enable Strip-position.
12. Select L4 for the Type.
13. Enable Strip-offset.
14. Enter 4 for the Value.
15. Select OK.

16. Select the flow name to display the attributes.

The Flow Entry panel will be displayed

Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

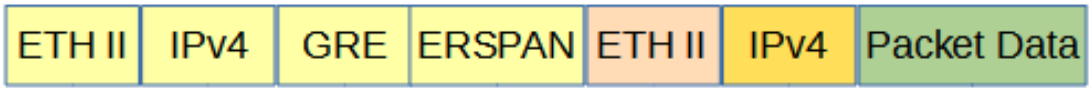
ERSPAN Type 2

Encapsulate

When a packet is encapsulated with an ERSPAN Type 2 header the new ERSPAN Type 2 header segments are added to the original packet. The ERSPAN Type 2 header segments consists of L2, L3, GRE and ERSPAN Type 2 as shown below.

Original Packet

ERSPAN Type 2 Encapsulated Packet



Encapsulating a packet with an ERSPAN Type 2 header involves two configuration procedures.

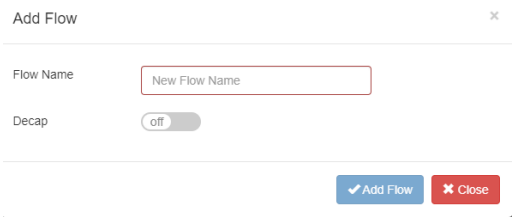
- Create a flow to add the ERSPAN Type 2 header
- Create a TAP Group

  This section discusses the procedure to create a flow to add the ERSPAN Type 2 header. The procedure to create a TAP Group is discussed in the TAP Group section.

Create a Flow

1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

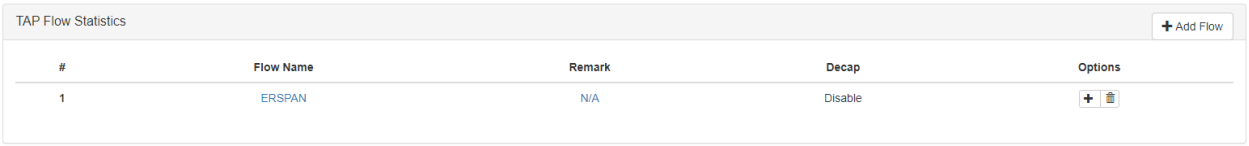
   The Add Flow panel will appear.



4. Enter the Flow Name.

5. Select Add Flow.

The flow will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule Options

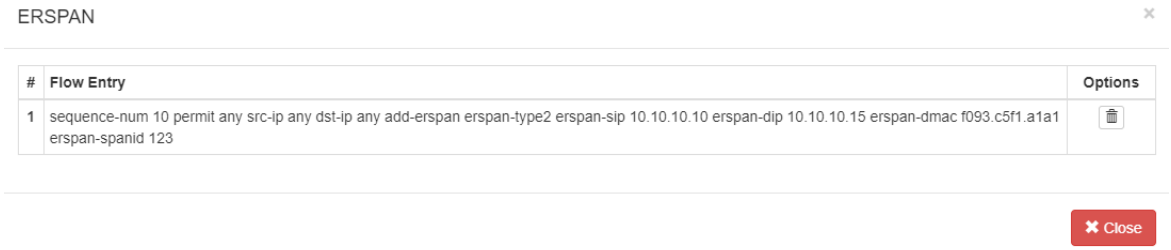
7. Select permit for the Action.
8. Select any for the IP Protocol Number.
9. Select any other desired options and enter the desired values to define which packets will be encapsulated. The defaults may be used to encapsulate all packets.

Flow Action Options

10. Enable Add Erspantype-2.
11. Enter the Erspantype-2-dest-mac. This defines the destination MAC address in the L2 segment of the ERSPAN header.
12. Enter the Erspantype-2-src-ip. This defines the destination IP address in the L3 segment of the ERSPAN header.
13. Enter the Erspantype-2-dest-ip. This defines the destination IP address in the L3 segment of the ERSPAN header.
14. Enter the desired Erspantype-2-spanid number.

15. Select OK.
16. Select the flow name to display the attributes.

The Flow Entry panel will be displayed

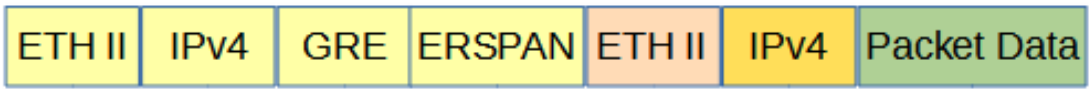


Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

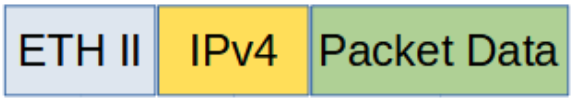
Decapsulate (New L2)

When this method is used to decapsulate an ERSPAN Type 2 packet the ERSPAN Type 2 header segments are removed from the packet along with the original L2 segment. A new L2 segment is added as shown below.

ERSPAN Type 2 Encapsulated Packet



ERSPAN Type 2 Decapsulated Packet



Decapsulating the ERSPAN Type 2 header from a packet(s) involves two configuration procedures.

- Create a flow to strip the ERSPAN Type 2 header
- Create a TAP Group

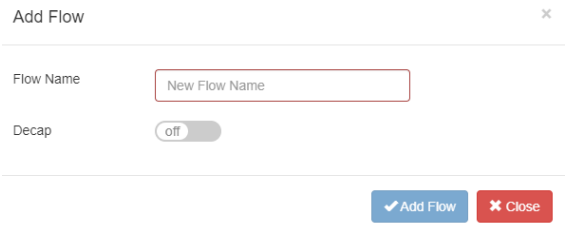
This section discusses the procedure to create a flow to strip the ERSPAN Type 2 header. The procedure to create a TAP Group is discussed in the TAP Group section.

Create a Flow

1. Select TAP Management.
2. Select Flow.

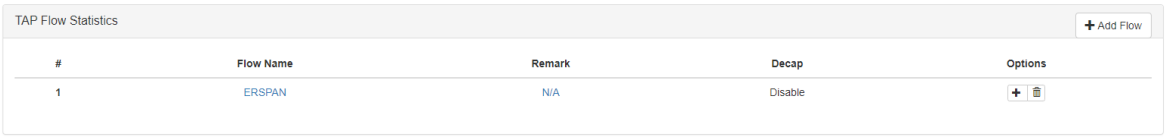
3. Select + Add Flow.

The Add Flow panel will appear.



4. Enter the Flow Name.
5. Select Add Flow.

The flow will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule Options

7. Select permit for the Action.
8. Select gre for the IP Protocol Number.
9. Select any other desired options and enter the desired values to define which ERSPAN packets will be decapsulated. The defaults may be used to decapsulate all ERSPAN packets.

Flow Action Options

10. Enable Strip-header.
11. Enable Strip-position.
12. Select L4 for the Type.
13. Enable Strip-offset.
14. Enter 20 for the Value.
15. Enable Edit packet.
16. Enable Edit-macda.
17. Enter the Dst-mac. This defines the destination MAC address for the new L2 segment added to the packet.
18. Enable Edit-macsa.
19. Enter the Src-mac. This defines the source MAC address for the new L2 segment added to the packet.
20. Select OK.
21. Select the flow name to display the attributes.

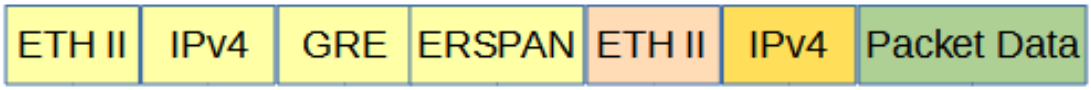
The Flow Entry panel will be displayed

Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

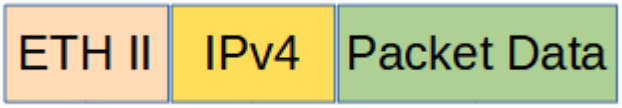
Decapsulate (Original Packet Retained)

When this method is used to decapsulate an ERSPAN Type 2 packet the ERSPAN Type 2 header segments are removed from the packet. The original packet is not modified as shown below.

ERSPAN Type 2 Encapsulated Packet



ERSPAN Type 2 Decapsulated Packet



Decapsulating the ERSPAN Type 2 header from a packet(s) involves two configuration procedures.

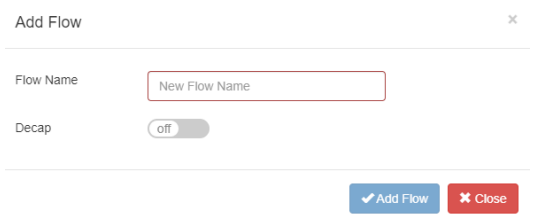
- Create a flow to strip the ERSPAN Type 2 header
- Create a TAP Group

  This section discusses the procedure to create a flow to strip the ERSPAN Type 2 header. The procedure to create a TAP Group is discussed in the TAP Group section.

Create a Flow

1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

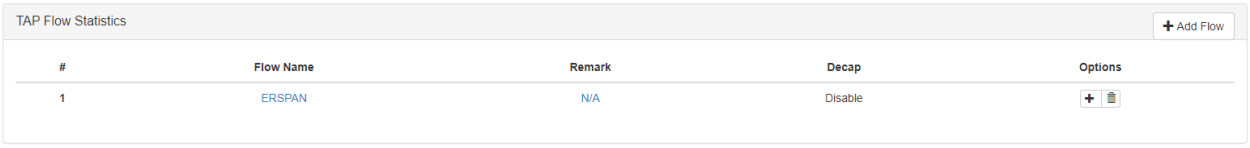
   The Add Flow panel will appear.



4. Enter the Flow Name.

5. Select Add Flow.

The flow will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule Options

7. Select permit for the Action.
8. Select any for the IP Protocol Number.
9. Select any other desired options and enter the desired values to define which ERSPAN packets will be decapsulated. The defaults may be used to decapsulate all ERSPAN packets.

Flow Action Options

10. Enable Strip-header.
11. Enable Strip-position.
12. Select L4 for the Type.
13. Enable Strip-offset.
14. Enter 20 for the Value.

15. Select OK.

16. Select the flow name to display the attributes.

The Flow Entry panel will be displayed

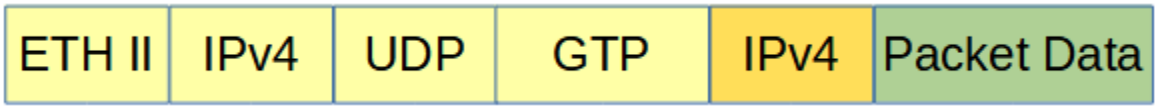
Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

GTP

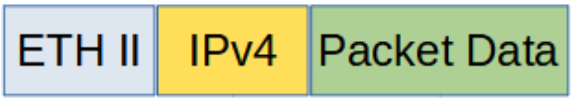
Decapsulate

When a GTP packet is decapsulated the GTP header segments are removed from the packet. A new L2 segment is added as shown below.

GTP Encapsulated Packet



GTP Decapsulated Packet



Decapsulating GTP packet(s) involves two configuration procedures.

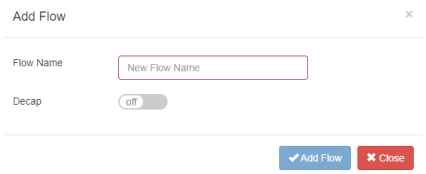
- Create a flow to strip the GTP header
- Create a TAP Group

  This section discusses the procedure to create a flow to strip all GTP headers. The procedure to create a TAP Group is discussed in the TAP Group section.

Create a Flow

1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

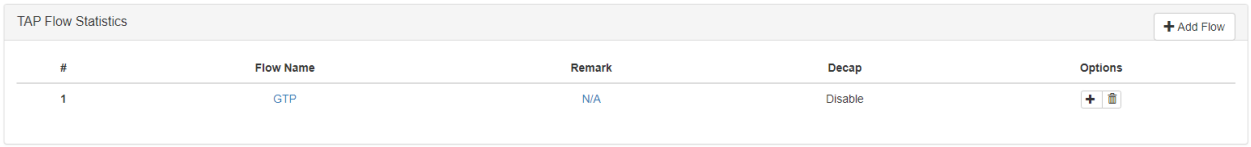
The Add Flow panel will appear.



4. Enter the Flow Name.

5. Select Add Flow.

The flow will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule Options

7. Select permit for the Action.

8. Select udp for the IP Protocol Number.

9. Enable Src-port.

10. Select eq for the Type.
11. Enter 2152 for the Port.
12. Enable Dst-port.
13. Select eq for the Type.
14. Enter 2152 for the Port.

Flow Action Options

15. Enable Strip-header.

16. Enable Strip-position.
17. Select L4 for the Type.
18. Enable Strip-offset.
19. Enter 16 for the Value.
20. Enable Edit packet.
21. Enable Edit-macda.
22. Enter the Dst-mac. This defines the destination MAC address for the new L2 segment added to the packet.
23. Enable Edit-macsa.
24. Enter the Src-mac. This defines the source MAC address for the new L2 segment added to the packet.
25. Select OK.
26. Select the flow name to display the attributes.

The Flow Entry panel will be displayed.

Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

IPIP

Decapsulate

When an IPIP packet is decapsulated the outer L3 header segment is removed from the packet and a new L2 segment is added as shown below.

IPIP Encapsulated Packet

IPIP Decapsulated Packet

Decapsulating the IPinIP header from a packet(s) involves two configuration procedures.

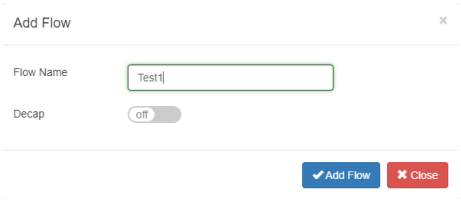
- Create a flow to strip the IPinIP header
- Create a TAP Group

This section discusses the procedure to create a flow to strip the IPIP header. The procedure to create a TAP Group is discussed in the TAP Group section.

Create a Flow

1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

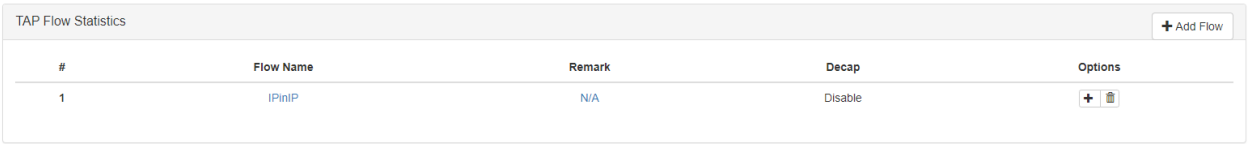
The Add Flow panel will appear.



4. Enter the flow name.

5. Select Add Flow.

The flow will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied
- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule Options

7. Select permit for the Action.

8. Select ipip for the IP Protocol Number.
9. Select any other desired options and enter the desired values to define which IPinIP packets will be decapsulated. The defaults may be used to decapsulate all IPinIP packets.

Flow Action Options

10. Enable Strip-header.
11. Enable Edit packet.
12. Enable Edit-macda.
13. Enter the Dst-mac. This defines the destination MAC address for the new L2 segment added to the packet.
14. Enable Edit-macsa.
15. Enter the Src-mac. This defines the source MAC address for the new L2 segment added to the packet.

16. Select OK.
17. Select the flow name to display the attributes.

The Flow Entry panel will be displayed

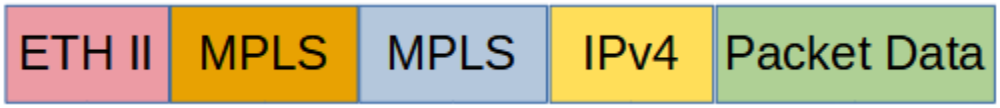
Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

MPLS

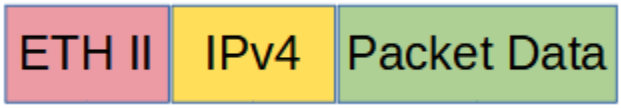
Strip MPLS Labels

When the MPLS label(s) are removed from a packet, the packet maintains the original L2, L3 and packet data as shown below.

MPLS Packet



MPLS Packet – Labels Removed



The Advanced Features MPLS abilities include:

- Strip up to 9 MPLS labels
- Filter on up to 3 MPLS Labels

Stripping and/or filtering MPLS labels on packets involves two configuration procedures.

- Create a flow
  - Strip MPLS labels from packets based on IP Protocol number
  - Strip MPLS labels based on filtering up to 3 MPLS Labels, 1st, 2nd and 3rd
  - Filter MPLS packets based on filtering up to 3 MPLS Labels, 1st, 2nd and 3rd

- Filter MPLS packets based on IP Protocol
- Filter MPLS packets based on Ether Type

- Create a TAP Group

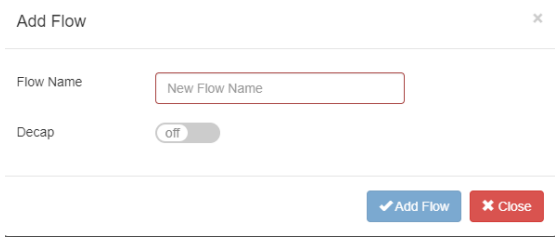
This section discusses the procedure to create MPLS flows. The procedure to create a TAP Group is discussed in the TAP Group section.

Create a Flow

1. Select TAP Management.
2. Select Flow.

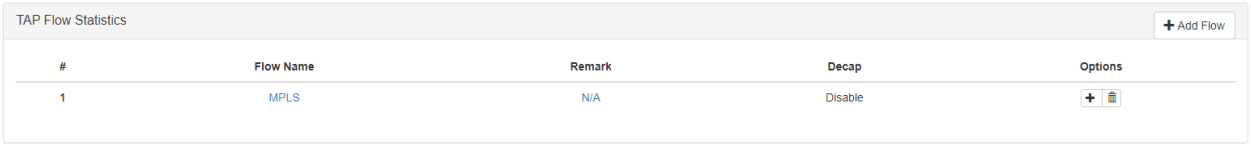
3. Select + Add Flow.

The Add Flow panel will appear.



4. Enter the Flow Name.
5. Select Add Flow.

The flow will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied

- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

  Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Strip MPLS Labels (IP Protocol)

This flow may be used to strip all the MPLS labels from packets without specifying the number of MPLS labels or using filtering to determine which MPLS packets are affected.

Flow Match Rule Options

1. Select permit for the Action.

2. Select mpls for the IP Protocol Number.

3. Enable Mpls enable.

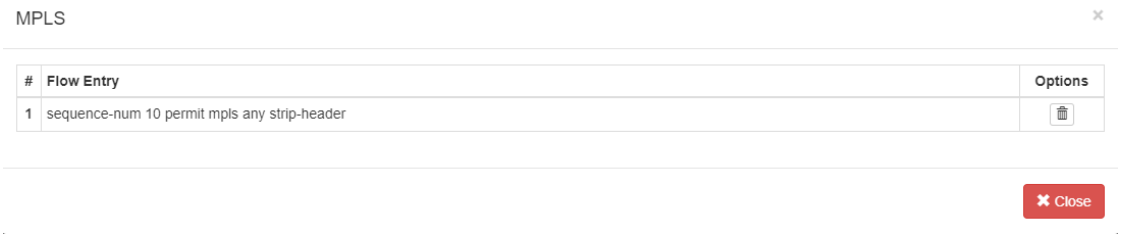
Flow Action Options

4. Enable Strip-header.

5. Select OK.

6. Select the flow name to display the attributes.

   The Flow Entry panel will be displayed



Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

Strip MPLS Labels (Strip 1-9 Labels and Filter on 1st, 2nd and 3rd)

This flow may be used to strip all the MPLS labels from packets by specifying the packets that meet the number of MPLS labels and using filtering to determine which MPLS packets are affected.

Flow Match Rule Options

1. Select permit for the Action.

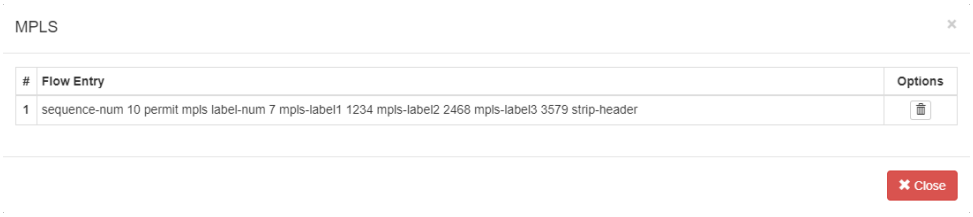
2. Select mpls for the IP Protocol Number.

3. Enable Mpls enable.
4. Select the desired Number. The MPLS labels will only be stripped from the packets that match the number selected. If 7 is selected, packets with 1-6 or 8-9 MPLS labels will not be affected.
5. Select num for label1.
6. Enter the desired label1_number.
7. Select num for label2.
8. Enter the desired label2_number.
9. Select num for label3.
10. Enter the desired label3_number.

Flow Action Options

11. Enable Strip-header .
12. Select OK.
13. Select the flow name to display the attributes.

The Flow Entry panel will be displayed



Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

Filter MPLS Packets (Filter on 1st, 2nd and 3rd)

This flow may be used to filter MPLS packets based on the 1st, 2nd and 3rd MPLS label number.

Flow Match Rule Options

1. Select permit for the Action.
2. Select mpls for the IP Protocol Number.
3. Enable Mpls enable.
4. Select the desired Number. Packets that match the MPLS label number will be permitted. If 7 is selected, packets with 1-6 or 8-9 MPLS labels will be denied.

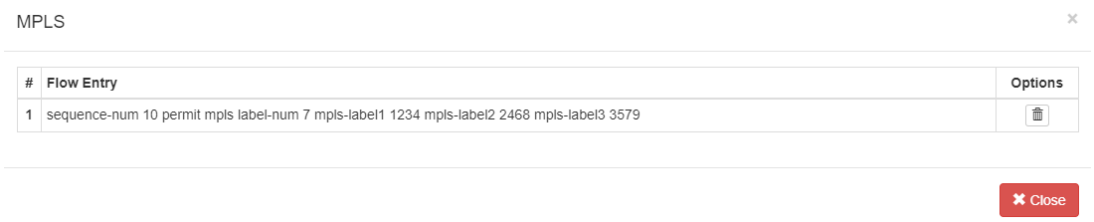
5. Select num for the label1 option.
6. Enter the desired label1_number.
7. Select num for the label2 option.
8. Enter the desired label2_number.
9. Select num for the label3 option.
10. Enter the desired label3_number.

Flow Action Options

11. Select OK.

12. Select the flow name to display the attributes.

The Flow Entry panel will be displayed



Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

Filter MPLS Packets (Filter on IP Protocol)

This flow may be used to filter MPLS packets based on IP Protocol only.

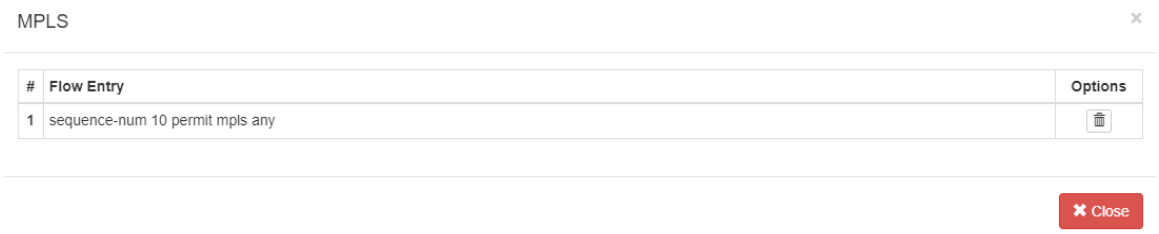
Flow Match Rule Options

1. Select permit for the Action.
2. Select mpls for the IP Protocol Number.
3. Enable Mpls enable.

Flow Action Options

4. Select OK.
5. Select the flow name to display the attributes.

The Flow Entry panel will be displayed



Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

Filter MPLS Packets (Filter on Ether Type)

This flow may be used to filter MPLS packets based on Ether Type only.

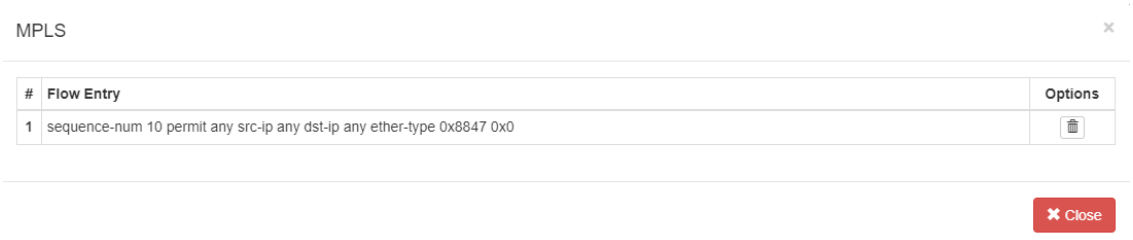
Flow Match Rule Options

1. Select permit for the Action.
2. Select mpls for the IP Protocol Number.
3. Enable Mpls enable.
4. Enable Ether Type
5. Enter 0x8847 for the Value.
6. Enter 0x0 for the Wildcard.

Flow Action Options

7. Select OK.
8. Select the flow name to display the attributes.

The Flow Entry panel will be displayed.



Additional entries may be created for the flow. Entries may be deleted by selecting the

Trash

Can. Entries may not be modified.

PPPoE

Decapsulate

Decapsulating the PPPoE header from a packet(s) involves two configuration procedures.

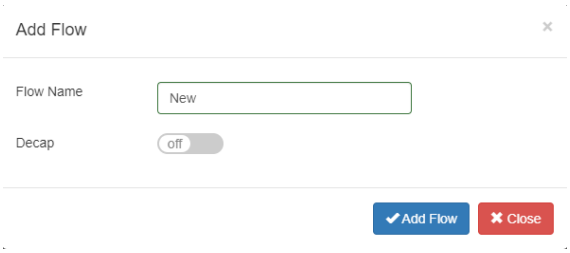
- Create a flow to strip the IPv4 or IPv6 PPPoE header
- Create a TAP Group

  This section discusses the procedure to create a flow to strip the PPPoE header. The procedure to create a TAP Group is discussed in the TAP Group section.

Create a Flow

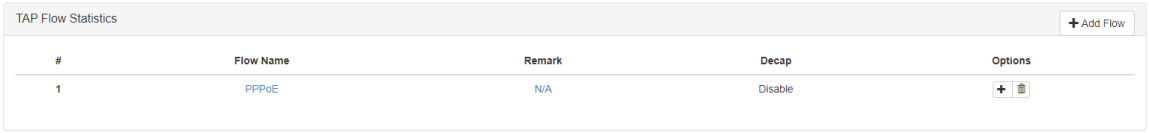
1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

   The Add Flow panel will appear.



4. Enter the flow name.
5. Select Add Flow.

   The flow will be displayed.



6. Select the + in the Options column to define the attributes.

The Add Flow Entry panel will be displayed.

The Add Flow Entry panel is divided into two sections, match rule and action.

Match Rule Section

- Defines whether the packets are permitted or denied

- Determines the permitted or denied packet filter criteria
- Determines which permitted packets will be modified by any action(s) selected and defined in the action section

Action Section

- The action section is used to define the modification(s) that will be performed on any packet(s) that is permitted by the match rule section

Flow Match Rule Options

7. Select permit for the Action.
8. Select pppoe for the IP Protocol Number.
9. Enable PPPOE enable.
10. Select the pppoe type.
11. Select the Protocol Version.
12. Select any other desired options and enter the desired values to define which IPinIP packets will be decapsulated. The defaults may be used to decapsulate all IPinIP packets.

Flow Action Options

13. Enable Strip-header.
14. Enter the pppoe-add-dst-mac. This defines the destination MAC for the new L2 segment added to the packet.
15. Enter the pppoe-add-src-mac. This defines the source MAC for the new L2 segment added to the packet.
16. Select OK.
17. Select the flow name to display the attributes.

The Flow Entry panel will be displayed

Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

TAP Statistics

The tap statistics feature provides the Advanced Features the ability to view traffic statistics based on:

- Per ingress port
  - Per flow statistics
    - Per flow entry
  - Per de-duplicate statistics

The tap statistics features are supported if the following items are configured:

- Flow Statistics
  - When a tap group is created, a flow with at least one entry must be selected for the ingress port(s).
- De-duplicate Statistics
  - The global de-duplicate feature must be enabled and configured under TAP Management/TAP Group Table/de-duplicate
  - When a tap group is created, a flow with at least one entry that has De-duplicate enabled must be selected for the ingress port(s)

Consider that the following flow example shown in Figure 1 is used when a tap group is created. The flow accomplishes the following:

1. If a traffic packet has an IPv4 source IP address of 10.10.10.10 it will pass. This entry will provide tap statistics but will not provide de-duplicate statistics.
2. If a traffic packet has an IPv4 source IP address of 10.10.10.11 it will pass. This entry will provide tap statistics and de-duplicate statistics.

Figure 1

View TAP

Statistics

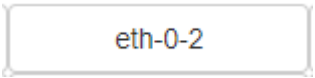
1. Select TAP Management.
2. Select TAP Statistics.

   The Port List panel will be displayed.

3. Select the desired port that can display the tap statistics. Available port(s) are displayed as shown in Figure 2. Unavailable port(s) are displayed as shown in Figure 3.

Figure 2

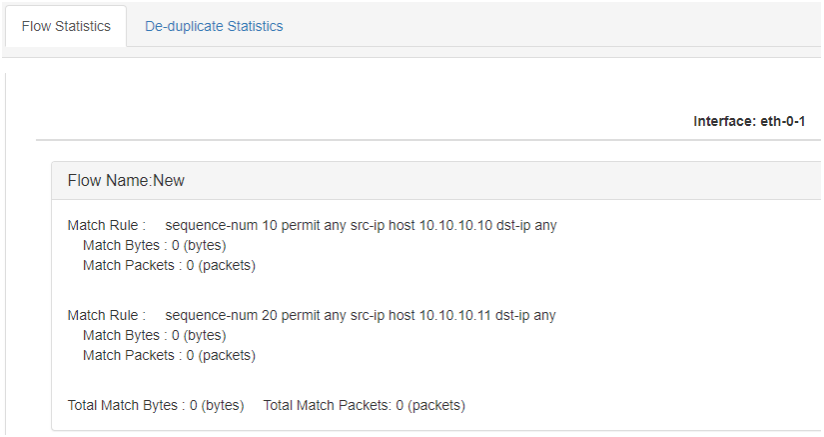
Figure 3



4. Select Update Flow Statistics.

   The statistics will be displayed for the port. Statistics are displayed for each entry within the flow as shown in Figure 4.

Figure 4

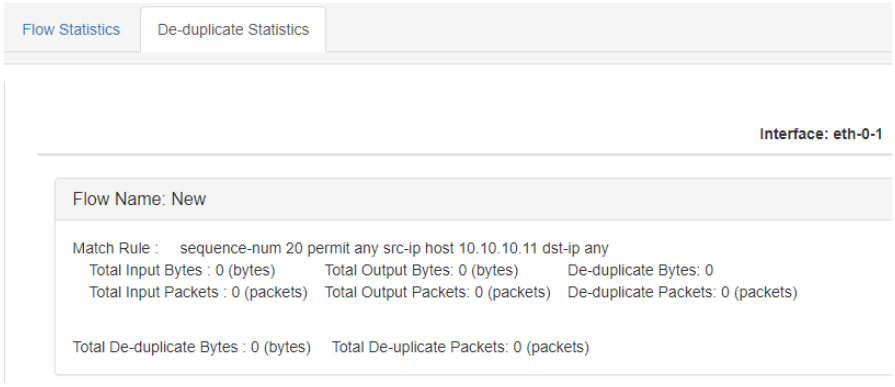


5. Select Update Flow Statistics to update the stats.
6. Select Clear Flow Statistics to clear the stats.
7. Select OK.

8. Select the De-duplicate Statistics tab to display the stats.

The statistics will be displayed for the port as shown in Figure 5.

Figure 5



9. Select Update Flow Statistics to update the stats.
10. Select Clear Flow Statistics to clear the stats.
11. Select OK.

RPC-API

The RPC-API may be configured to use two options:

- JSON over HTTP
- JSON over HTTPS

The RPC-API service is disabled by default. If enabled, the default port number is 80. If it is desired to configure the RPC-API as JSON over HTTP, then the RPC-API port number must be configured to a different port number other than 80 so as not to conflict with HTTP. If it is desired to configure the RPC-API as JSON over HTTPS, then the RPC-API default port number 80 is acceptable due to the HTTPS port number 443. However, the RPC-API port number may be modified in this case as well. The HTTP and HTTPS services may not be enabled simultaneously.

Connect to the Advanced Features

Connect to the Advanced Features unit. A connection to the unit may be established using two options:

- Directly connected to the Console Interface to COM Port using Putty/Serial connection
- Connected via the IP Management Interface using Putty/SSH connection

Display the Default Services

The default services configuration are displayed via the console interface. Use the following procedure to display the default services configuration.

1. Press the Return key.
2. Enter enable.
3. Enter the following command to display the default services configuration.

```
Switch# show services
Networking services configuration:
```

```
Service Name     Status        Port       Protocol   Service ACL
---------------+-------------+----------+----------+------------
http             enable        80         TCP        -
https            disable       443        TCP        -
rpc-api          disable       -          TCP        -
telnet           disable       23         TCP        -
ssh              enable        22         TCP        -
snmp             disable       161        UDP        -
```

Configure RPC-API over HTTP

The HTTP service is enabled by default and is configured to use port 80.

This procedure requires:

Enable the RPC-API service

In this example the RPC-API port number will be configured to use port 2000.

1. Press the Return key.
2. Enter enable.
3. Enter the following commands to enable the RPC-API service and display the services.

```
Switch# configure terminal
Switch(config)# service rpc-api enable port 2000
Switch(config)# exit
Switch# show services
Networking services configuration:
Service Name     Status        Port       Protocol   Service ACL
---------------+-------------+----------+----------+------------
http             enable        80         TCP        -
https            disable       443        TCP        -
rpc-api          enable        2000       TCP        -
telnet           disable       23         TCP        -
ssh              enable        22         TCP        -
snmp             disable       161        UDP        -
```

Configure RPC-API over HTTPS

The HTTPS service is disabled by default and is configured to use port 443.

This procedure requires:

- Disable the HTTP service
- Enable the HTTPS service
- Enable the RPC-API service

  In this example the RPC-API port number will be configured to use port 2000.

1. Press the Return key.
2. Enter enable.

3. Enter the following commands to disable the HTTP service, enable the HTTPS service, enable the RPC-API service and display the services.

```
Switch# configure terminal
Switch(config)# service http disable
Switch(config)# service https enable
Switch(config)# service rpc-api enable port 2000
Switch(config)# exit
Switch# show services
Networking services configuration:
Service Name     Status        Port       Protocol   Service ACL
---------------+-------------+----------+----------+------------
http             disable       80         TCP        -
https            enable        443        TCP        -
rpc-api          enable        2000       TCP        -
telnet           disable       23         TCP        -
ssh              enable        22         TCP        -
snmp             disable       161        UDP        -
```

Log Threshold

Log threshold notifications may be applied to any port. A port may be an ingress port, egress port, member of a port group or member of a link aggregation group. The notifications are presented via Syslog messages. Syslog must be configured on the Advanced Features unit to support log thresholds. The Advanced Features unit polls each port in 5-minute intervals when log threshold is enabled.

Log threshold notifications may be configured as:

- log-threshold output-discard
- log-threshold output-rate xx resume-rate xx
- log-threshold input-rate xx resume-rate xx

Connect to the Advanced Features

Connect to the Advanced Features unit. A connection to the unit may be established using two options:

- Directly connected to the Console Interface to COM Port using Putty/Serial connection
- Connected via the IP Management Interface using Putty/SSH connection

Log-Threshold Output Discard

1. Press the Return key.
2. Enter enable.
3. Enter configure terminal.
4. Enter the following commands to enable log-threshold output discard.

```
Switch(config)# interface eth-0-X
```

X = Port Number

```
Switch(config-if-eth-0-X)# log-threshold output-discard X interval Y
```

X = Packets (100 to 4294967295)

Y = Interval Minutes (1 to 1440)

5. Enter the following command to disable log-threshold output discard.

```
Switch(config-if-eth-0-X)# no log-threshold output-discard
```

The following are examples of log-threshold output discard messages. The output-discard was configured at 100 and the interval was configured at 1 minute.

```
%INTERFACE-4-DROP_OVERFLOW: Interface eth-0-2 output drop 342353278 packets in 1 minutes
%INTERFACE-4-DROP_RESUME: Interface eth-0-2 output drop resume under 100 packets in 1 minutes
```

Log-Threshold Output-Rate

1. Press the Return key.
2. Enter enable.
3. Enter configure terminal.
4. Enter the following commands to enable log-threshold output rate.

```
Switch(config)# interface eth-0-X
```

X = Port Number

```
Switch(config-if-eth-0-X)# log-threshold output-rate X resume-rate Y
```

X = Bandwidth Utilization Rate Over (1 to 100)

Y = Bandwidth Utilization Rate Resume Under (1 to 100)

5. Enter the following command to disable log-threshold output rate.

```
Switch(config-if-eth-0-X)# no log-threshold output-rate
```

The following are examples of log-threshold output-rate messages. The output-rate was configured at 90 and the resume-rate was configured at 50.

```
%INTERFACE-4-BANDWIDTH_OVERFLOW: Interface eth-0-4 output bandwidth utilization rate over 90
percent
%INTERFACE-4-BANDWIDTH_RESUME: Interface eth-0-4 output bandwidth utilization rate resume under
50 percent
```

Log-Threshold Input-Rate

1. Press the Return key.
2. Enter enable.
3. Enter configure terminal.
4. Enter the following commands to enable log-threshold input rate.

```
Switch(config)# interface eth-0-X
```

X = Port Number

```
Switch(config-if-eth-0-X)# log-threshold input-rate X resume-rate Y
```

X = Bandwidth Utilization Rate Over (1 to 100)

Y = Bandwidth Utilization Rate Resume Under (1 to 100)

5. Enter the following command to disable log-threshold input rate.

```
Switch(config-if-eth-0-X)# no log-threshold input-rate
```

The following are examples of log-threshold input-rate messages. The input-rate was configured at 90 and the resume-rate was configured at 50.

```
%INTERFACE-4-BANDWIDTH_OVERFLOW: Interface eth-0-1 input bandwidth utilization rate over 90
percent
```

```
%INTERFACE-4-BANDWIDTH_RESUME: Interface eth-0-1 input bandwidth utilization rate resume under 50
percent
```

Link Flap

Link-Flap is enabled on all ports by default. The following commands provide the ability to enable/disable or control the Link-Flap function.

Connect to the Advanced Features

Connect to the Advanced Features unit. A connection to the unit may be established using two options:

- Directly connected to the Console Interface to COM Port using Putty/Serial connection
- Connected via the IP Management Interface using Putty/SSH connection

1. Press the Return key.
2. Enter enable.
3. Enter configure terminal.

Errdisable Detect

Use the following command to disable the port link error status detection function.

```
Switch(config)# no errdisable detect reason link-flap
```

Use the no form of the command to restore to the default, enabled.

```
Switch(config)# errdisable detect reason link-flap
```

Errdisable Recovery Interval

Use this command to set the recovery time of a port from the error state. The range is 30-86,400 seconds.

```
Switch(config)# errdisable recover interval XX
```

Use this command to set the recovery time of a port from the error state to the default value, 300 seconds.

```
Switch(config)# no errdisable recover interval
```

Errdisable Recovery Reason

Use this command to enable the error recovery function for a specified reason.

```
Switch(config)# errdisable recover reason link-flap
```

Use this command to disable the error recovery function for a specified reason.

```
Switch(config)# no errdisable recover interval
```

Errdisable Flap

There are two parameters used in link flap error detection, one is the flap count and the other is the flap time. If the flap count is reached within the flap time specified, the port will enter the errdisable state.

Use this command to set the link flap oscillation parameters.
XX = The maximum link flaps before setting the port to errdisable. Range, 1 – 100. Default=10.
YY = The maximum flap time before setting the port to errdisable. Range, 1 – 120. Default=10.

```
Switch(config)# errdisable flap reason link-flap xx yy
```

Use this command to restore the link flap oscillation parameters to the default values, 10,10.

```
Switch(config)# no errdisable flap reason link-flap
```

Show Errdisable Detect

Use this command to display the error detection status.

```
Switch# show errdisable detect
```

Show Errdisable Recovery

Use this command to display the error recovery status.

```
Switch# show errdisable recovery
```

Show Errdisable Flap

Use this command to display the link oscillation error detection parameters.

```
Switch# show errdisable flap
```

sFlow

sFlow, short for "sampled flow", is an industry standard for packet export at Layer 2 of the OSI model. sFlow was originally developed by InMon Corp. It provides a means for exporting truncated packets, together with interface counters for the purpose of network monitoring. Maintenance of the protocol is performed by the sFlow.org consortium, the authoritative source of the sFlow protocol specifications.

In this example sFlow will be enabled for Port Eth-0-1. Use this same procedure for any other port desired.

Connect to the Advanced Features

Connect to the Advanced Features unit. A connection to the unit may be established using two options:

- Directly connected to the Console Interface to COM Port using Putty/Serial connection
- Connected via the IP Management Interface using Putty/SSH connection

1. Press the Return key.

2. Enter enable.

3. Enter configure terminal.

Configure sFlow

1. Enter the following commands to enable sFlow.

```
Switch(config)# sflow enable
Switch(config)# sflow agent ip xxx.xxx.xxx.xxx   Advanced Features IP Address)
Switch(config)# sflow collector mgmt-if xxx.xxx.xxx.xxx 6343  (Laptop or PC)
Switch(config)# sflow counter interval 10
Switch(config)# interface eth-0-1            (Advanced Features port)
Switch(config-if-eth-0-1)# sflow counter-sampling enable
Switch(config-if-eth-0-1)# sflow flow-sampling rate 32768
Switch(config-if-eth-0-1)# sflow flow-sampling enable both
Switch(config-if-eth-0-1)# exit
Switch(config)# exit
Switch#
```

Display sFlow

1. Enter the following command to display sFlow.

```
Switch# show sflow
```

IPFix

This document describes the IPFix configuration options supported by the Advanced Features units. IPFix must be configured using CLI commands. Refer to the Advanced Features CLI Guide for parameter defaults and specific details. When IPFix is enabled, 128 flows are reserved.

Connect to the Advanced Features

Connect to the Advanced Features unit. A connection to the unit may be established using two options:

- Directly connected to the Console Interface to COM Port using Putty/Serial connection
- Connected via the IP Management Interface using Putty/SSH connection

1. Press the Return key.

2. Enter enable.

3. Enter configure terminal.

Enable IPFix

```
Switch(config)# ipfix enable
```

Create the IPFix Recorder

```
Switch(config)# ipfix recorder recordername
```

Collect

```
Switch(config-ipfix-recorder-recordername)# collect counter
Switch(config-ipfix-recorder-recordername)# collect flow
Switch(config-ipfix-recorder-recordername)# collect timestamp
Switch(config-ipfix-recorder-recordername)# collect ttl
```

Description

```
Switch(config-ipfix-recorder-recordername)# description
```

Do

```
Switch(config-ipfix-recorder-recordername)# do boot
Switch(config-ipfix-recorder-recordername)# do cd
Switch(config-ipfix-recorder-recordername)# do clear
Switch(config-ipfix-recorder-recordername)# do configure
Switch(config-ipfix-recorder-recordername)# do copy
Switch(config-ipfix-recorder-recordername)# do debug
Switch(config-ipfix-recorder-recordername)# do delete
```

```
Switch(config-ipfix-recorder-recordername)# do dir
Switch(config-ipfix-recorder-recordername)# do disable
Switch(config-ipfix-recorder-recordername)# do enable
Switch(config-ipfix-recorder-recordername)# do logging
Switch(config-ipfix-recorder-recordername)# do logout
Switch(config-ipfix-recorder-recordername)# do ls
Switch(config-ipfix-recorder-recordername)# do md5sum
Switch(config-ipfix-recorder-recordername)# do mkdir



Switch(config-ipfix-recorder-recordername)# do more
Switch(config-ipfix-recorder-recordername)# do no
Switch(config-ipfix-recorder-recordername)# do ping
Switch(config-ipfix-recorder-recordername)# do pwd
Switch(config-ipfix-recorder-recordername)# do re-activate
Switch(config-ipfix-recorder-recordername)# do reboot
Switch(config-ipfix-recorder-recordername)# do reload
Switch(config-ipfix-recorder-recordername)# do remane
Switch(config-ipfix-recorder-recordername)# do reset
Switch(config-ipfix-recorder-recordername)# do rmdir
Switch(config-ipfix-recorder-recordername)# do set
Switch(config-ipfix-recorder-recordername)# do show
Switch(config-ipfix-recorder-recordername)# do source
Switch(config-ipfix-recorder-recordername)# do ssh
Switch(config-ipfix-recorder-recordername)# do start
Switch(config-ipfix-recorder-recordername)# do telnet
Switch(config-ipfix-recorder-recordername)# do terminal
Switch(config-ipfix-recorder-recordername)# do traceroute
Switch(config-ipfix-recorder-recordername)# do write
```

End

```
Switch(config-ipfix-recorder-recordername)# end
```

Exit

```
Switch(config-ipfix-recorder-recordername)# exit
```

Help

```
Switch(config-ipfix-recorder-recordername)# help
```

Match

```
Switch(config-ipfix-recorder-recordername)# match cos
Switch(config-ipfix-recorder-recordername)# match flow
Switch(config-ipfix-recorder-recordername)# match interface
Switch(config-ipfix-recorder-recordername)# match ipv4
Switch(config-ipfix-recorder-recordername)# match ipv6
Switch(config-ipfix-recorder-recordername)# match mac
Switch(config-ipfix-recorder-recordername)# match packet
Switch(config-ipfix-recorder-recordername)# match transport
Switch(config-ipfix-recorder-recordername)# match vlan
Switch(config-ipfix-recorder-recordername)# match vxlan-vni
Switch(config-ipfix-recorder-recordername)# match nvgre-key
```

No

```
Switch(config-ipfix-recorder-recordername)# no collect
Switch(config-ipfix-recorder-recordername)# no description
Switch(config-ipfix-recorder-recordername)# no match
Switch(config-ipfix-recorder-recordername)# no tunnel-aware
```

Quit

```
Switch(config-ipfix-recorder-recordername)# quit
```

Show

```
Switch(config-ipfix-recorder-recordername)# show history
Switch(config-ipfix-recorder-recordername)# show running-config
Switch(config-ipfix-recorder-recordername)# show this
```

Tunnel-Aware

```
Switch(config-ipfix-recorder-recordername)# tunnel-aware inner-outer-merge
```

Create the IPFix Exporter

```
Switch(config)# ipfix exporter exportername
```

Description

```
Switch(config-ipfix-exporter-exportername)# description
```

Destination

```
Switch(config-ipfix-exporter-exportername)# destination mgmt-if ipv4
 xxx.xxx.xxx.xxx
```

Do

```
Switch(config-ipfix-exporter-exportername)# do boot
Switch(config-ipfix-exporter-exportername)# do cd
Switch(config-ipfix-exporter-exportername)# do clear
Switch(config-ipfix-exporter-exportername)# do configure
Switch(config-ipfix-exporter-exportername)# do copy
Switch(config-ipfix-exporter-exportername)# do debug
Switch(config-ipfix-exporter-exportername)# do delete
Switch(config-ipfix-exporter-exportername)# do dir
Switch(config-ipfix-exporter-exportername)# do disable
Switch(config-ipfix-exporter-exportername)# do enable
Switch(config-ipfix-exporter-exportername)# do logging
Switch(config-ipfix-exporter-exportername)# do logout
Switch(config-ipfix-exporter-exportername)# do ls
Switch(config-ipfix-exporter-exportername)# do md5sum
Switch(config-ipfix-exporter-exportername)# do mkdir
Switch(config-ipfix-exporter-exportername)# do more
Switch(config-ipfix-exporter-exportername)# do no
Switch(config-ipfix-exporter-exportername)# do ping
Switch(config-ipfix-exporter-exportername)# do pwd
Switch(config-ipfix-exporter-exportername)# do re-activate
Switch(config-ipfix-exporter-exportername)# do reboot
Switch(config-ipfix-exporter-exportername)# do reload
Switch(config-ipfix-exporter-exportername)# do remane
```

```
Switch(config-ipfix-exporter-exportername)# do reset
Switch(config-ipfix-exporter-exportername)# do rmdir
Switch(config-ipfix-exporter-exportername)# do set
Switch(config-ipfix-exporter-exportername)# do show
Switch(config-ipfix-exporter-exportername)# do source
Switch(config-ipfix-exporter-exportername)# do ssh
Switch(config-ipfix-exporter-exportername)# do start
Switch(config-ipfix-exporter-exportername)# do telnet
Switch(config-ipfix-exporter-exportername)# do terminal



Switch(config-ipfix-exporter-exportername)# do traceroute
Switch(config-ipfix-exporter-exportername)# do write
```

Domain-ID

```
Switch(config-ipfix-exporter-exportername)# domain-id
```

DSCP

```
Switch(config-ipfix-exporter-exportername)# dscp
```

End

```
Switch(config-ipfix-exporter-exportername)# end
```

Event

```
Switch(config-ipfix-exporter-exportername)# event flow start
Switch(config-ipfix-exporter-exportername)# event flow end
```

Exit

```
Switch(config-ipfix-exporter-exportername)# exit
```

Flow

```
Switch(config-ipfix-exporter-exportername)# flow data flush
Switch(config-ipfix-exporter-exportername)# flow data timeout
```

Help

```
Switch(config-ipfix-exporter-exportername)# help
```

No

```
Switch(config-ipfix-exporter-exportername)# no description
Switch(config-ipfix-exporter-exportername)# no destination
Switch(config-ipfix-exporter-exportername)# no domain-id
Switch(config-ipfix-exporter-exportername)# no dscp
Switch(config-ipfix-exporter-exportername)# no event
Switch(config-ipfix-exporter-exportername)# no flow
Switch(config-ipfix-exporter-exportername)# no template
Switch(config-ipfix-exporter-exportername)# no transport
Switch(config-ipfix-exporter-exportername)# no ttl
```

Quit

```
Switch(config-ipfix-exporter-exportername)# quit
```

Show

```
Switch(config-ipfix-exporter-exportername)# show history
Switch(config-ipfix-exporter-exportername)# show running-config
```

Template

```
Switch(config-ipfix-exporter-exportername)# template data timeout
```

Transport

```
Switch(config-ipfix-exporter-exportername)# transport protocol udp port
```

TTL

```
Switch(config-ipfix-exporter-exportername)# ttl
```

Create the IPFix Sampler

```
Switch(config)# ipfix sampler samplername
```

1 Out Of

```
Switch(config-ipfix-sampler-samplername)# 1 out of
```

Description

```
Switch(config-ipfix-sampler-samplername)# description
```

Do

```
Switch(config-ipfix-sampler-samplername)# do boot
Switch(config-ipfix-sampler-samplername)# do cd
Switch(config-ipfix-sampler-samplername)# do clear
Switch(config-ipfix-sampler-samplername)# do configure
Switch(config-ipfix-sampler-samplername)# do copy
Switch(config-ipfix-sampler-samplername)# do debug
Switch(config-ipfix-sampler-samplername)# do delete
Switch(config-ipfix-sampler-samplername)# do dir
Switch(config-ipfix-sampler-samplername)# do disable
Switch(config-ipfix-sampler-samplername)# do enable
Switch(config-ipfix-sampler-samplername)# do logging
Switch(config-ipfix-sampler-samplername)# do logout
Switch(config-ipfix-sampler-samplername)# do ls
Switch(config-ipfix-sampler-samplername)# do md5sum
Switch(config-ipfix-sampler-samplername)# do mkdir
Switch(config-ipfix-sampler-samplername)# do more
Switch(config-ipfix-sampler-samplername)# do no
Switch(config-ipfix-sampler-samplername)# do ping
Switch(config-ipfix-sampler-samplername)# do pwd
Switch(config-ipfix-sampler-samplername)# do re-activate
Switch(config-ipfix-sampler-samplername)# do reboot
Switch(config-ipfix-sampler-samplername)# do reload
Switch(config-ipfix-sampler-samplername)# do remane
Switch(config-ipfix-sampler-samplername)# do reset
Switch(config-ipfix-sampler-samplername)# do rmdir
Switch(config-ipfix-sampler-samplername)# do set
Switch(config-ipfix-sampler-samplername)# do show
Switch(config-ipfix-sampler-samplername)# do source
Switch(config-ipfix-sampler-samplername)# do ssh
Switch(config-ipfix-sampler-samplername)# do start
```

```
Switch(config-ipfix-sampler-samplername)# do telnet
Switch(config-ipfix-sampler-samplername)# do terminal
Switch(config-ipfix-sampler-samplername)# do traceroute
Switch(config-ipfix-sampler-samplername)# do write
```

End

```
Switch(config-ipfix-sampler-samplername)# end
```

Exit

```
Switch(config-ipfix-sampler-samplername)# exit
```

Help

```
Switch(config-ipfix-sampler-samplername)# help
```

Mode

```
Switch(config-ipfix-sampler-samplername)# mode flow
Switch(config-ipfix-sampler-samplername)# mode random
Switch(config-ipfix-sampler-samplername)# mode determinate
```

No

```
Switch(config-ipfix-sampler-samplername)# no description
```

Quit

```
Switch(config-ipfix-sampler-samplername)# quit
```

Show

```
Switch(config-ipfix-sampler-samplername)# show history
Switch(config-ipfix-sampler-samplername)# show running-config
Switch(config-ipfix-sampler-samplername)# show this
```

Create the IPFix Monitor

```
Switch(config)# ipfix monitor monitorname
```

Description

```
Switch(config-ipfix-monitor-monitorname)# description
```

Do

```
Switch(config-ipfix-monitor-monitorname)# do boot
Switch(config-ipfix-monitor-monitorname)# do cd
Switch(config-ipfix-monitor-monitorname)# do clear
Switch(config-ipfix-monitor-monitorname)# do configure
Switch(config-ipfix-monitor-monitorname)# do copy
Switch(config-ipfix-monitor-monitorname)# do debug
Switch(config-ipfix-monitor-monitorname)# do delete
Switch(config-ipfix-monitor-monitorname)# do dir
Switch(config-ipfix-monitor-monitorname)# do disable
Switch(config-ipfix-monitor-monitorname)# do enable
Switch(config-ipfix-monitor-monitorname)# do logging
```

```
Switch(config-ipfix-monitor-monitorname)# do logout
Switch(config-ipfix-monitor-monitorname)# do ls
Switch(config-ipfix-monitor-monitorname)# do md5sum
Switch(config-ipfix-monitor-monitorname)# do mkdir
Switch(config-ipfix-monitor-monitorname)# do more
Switch(config-ipfix-monitor-monitorname)# do no
Switch(config-ipfix-monitor-monitorname)# do ping
Switch(config-ipfix-monitor-monitorname)# do pwd
Switch(config-ipfix-monitor-monitorname)# do re-activate
```

```
Switch(config-ipfix-monitor-monitorname)# do reboot
Switch(config-ipfix-monitor-monitorname)# do reload
Switch(config-ipfix-monitor-monitorname)# do remane
Switch(config-ipfix-monitor-monitorname)# do reset
Switch(config-ipfix-monitor-monitorname)# do rmdir
Switch(config-ipfix-monitor-monitorname)# do set
Switch(config-ipfix-monitor-monitorname)# do show
Switch(config-ipfix-monitor-monitorname)# do source
Switch(config-ipfix-monitor-monitorname)# do ssh
Switch(config-ipfix-monitor-monitorname)# do start
Switch(config-ipfix-monitor-monitorname)# do telnet
Switch(config-ipfix-monitor-monitorname)# do terminal
Switch(config-ipfix-monitor-monitorname)# do traceroute
Switch(config-ipfix-monitor-monitorname)# do write
```

End

```
Switch(config-ipfix-monitor-monitorname)# end
```

Exit

```
Switch(config-ipfix-monitor-monitorname)# exit
```

Exporter

```
Switch(config-ipfix-monitor-monitorname)# exporter exportername
```

Help

```
Switch(config-ipfix-monitor-monitorname)# help
```

No

```
Switch(config-ipfix-monitor-monitorname)# no description
Switch(config-ipfix-monitor-monitorname)# no exporter
Switch(config-ipfix-monitor-monitorname)# no recorder
```

Quit

```
Switch(config-ipfix-monitor-monitorname)# quit
```

Recorder

```
Switch(config-ipfix-monitor-monitorname)# recorder recordername
```

Show

```
Switch(config-ipfix-monitor-monitorname)# show history
Switch(config-ipfix-monitor-monitorname)# show running-config
Switch(config-ipfix-monitor-monitorname)# show this
```

Create the IPFix Interface

```
Switch(config)# interface eth-0-X
Switch(config-if-eth-0-X)# ipfix IPFIX monitor input monitorname sampler
                            samplername
Switch(config-if-eth-0-X)# ipfix IPFIX monitor output monitorname sampler
                            samplername
Switch(config-if-eth-0-X)# ipfix IPFIX tunnel-aware inner



Switch(config-if-eth-0-X)# ipfix IPFIX tunnel-aware inner-outer-merge
Switch(config-if-eth-0-X)# no shutdown
Switch(config-if-eth-0-X)# exit
```

Configure the IPFix Global Options

```
Switch(config)# ipfix global
```

Do

```
Switch(config-ipfix-global)# do boot
Switch(config-ipfix-global)# do cd
Switch(config-ipfix-global)# do clear
Switch(config-ipfix-global)# do configure
Switch(config-ipfix-global)# do copy
Switch(config-ipfix-global)# do debug
Switch(config-ipfix-global)# do delete
Switch(config-ipfix-global)# do dir
Switch(config-ipfix-global)# do disable
Switch(config-ipfix-global)# do enable
Switch(config-ipfix-global)# do logging
Switch(config-ipfix-global)# do logout
Switch(config-ipfix-global)# do ls
Switch(config-ipfix-global)# do md5sum
Switch(config-ipfix-global)# do mkdir
Switch(config-ipfix-global)# do more
Switch(config-ipfix-global)# do no
Switch(config-ipfix-global)# do ping
Switch(config-ipfix-global)# do pwd
Switch(config-ipfix-global)# do re-activate
Switch(config-ipfix-global)# do reboot
Switch(config-ipfix-global)# do reload
Switch(config-ipfix-global)# do remane
Switch(config-ipfix-global)# do reset
Switch(config-ipfix-global)# do rmdir
Switch(config-ipfix-global)# do set
Switch(config-ipfix-global)# do show
Switch(config-ipfix-global)# do source
Switch(config-ipfix-global)# do ssh
Switch(config-ipfix-global)# do start
Switch(config-ipfix-global)# do telnet
Switch(config-ipfix-global)# do terminal
Switch(config-ipfix-global)# do traceroute
Switch(config-ipfix-global)# do write
```

End

```
Switch(config-ipfix-global)# end
```

Exit

```
Switch(config-ipfix-global)# exit
```

Flow

```
Switch(config-ipfix-global)# flow aging
Switch(config-ipfix-global)# flow export
```

Help

```
Switch(config-ipfix-global)# help
```

No

```
Switch(config-ipfix-global)# no flow aging
Switch(config-ipfix-global)# no flow export
```

Quit

```
Switch(config-ipfix-global)# quit
```

Show

```
Switch(config-ipfix-global)# show history
Switch(config-ipfix-global)# show running-config
Switch(config-ipfix-global)# show this
```

Monitor Capture

Monitor Capture is a tool that can assist with verifying new traffic configurations or assist in trouble shooting.

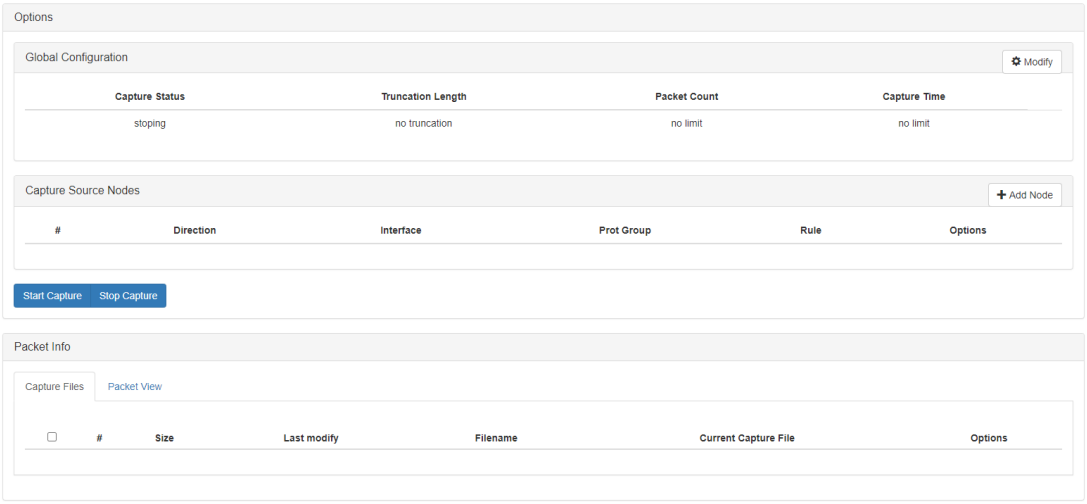
- The Monitor Capture tool supports the following capabilities:
- The monitor capture tool requires a TAP Group to be created
- Supports truncation, 64 to 144 bytes
- Supports packet count
- Support capture time
- Ingress packet capture options
  - A flow may be applied to filter the captured packets
  - A single port or group of ports may be selected
  - A link aggregation group may be selected
  - A port group may be selected.
- Egress packet capture options
  - An ACL may be applied to filter the captured packets
  - A single port or group of ports may be selected
  - A link aggregation group may be selected
- The monitor capture tool must be manually started
- The monitor capture tool must be manually stopped
- A txt file is created to view the last 1000 captured packets
- A pcap file may be created from the txt file

Monitor Capture Configuration

1. Select tools.

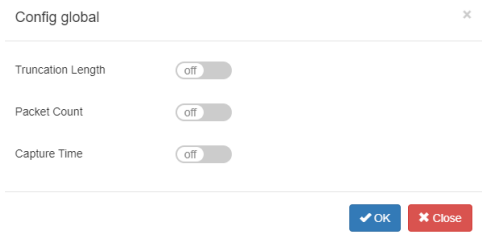
2. Select Monitor Capture.

The Options panel will be displayed.



3. Select the Global Configuration Modify.

The Config global panel will be displayed. The defaults may be used if desired.



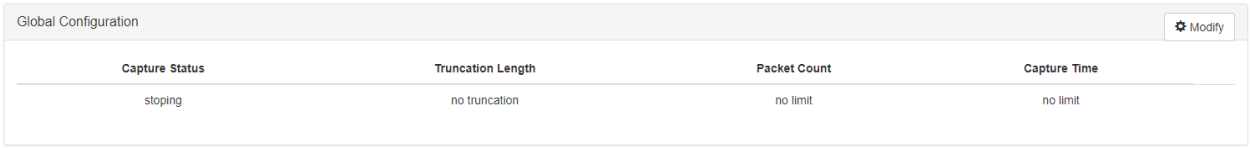
4. Truncation Length may be enabled. If so, enter the value.

5. Packet Count may be enabled, If so, enter the value.

6. Capture Time may be enabled. If so, enter the value.

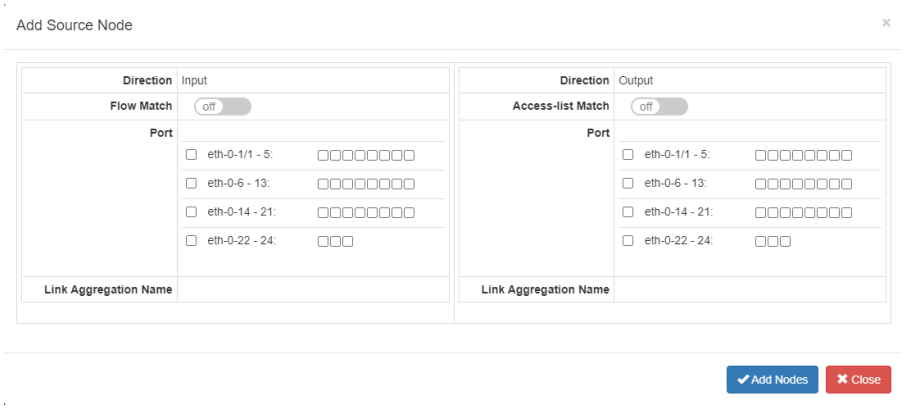
7. Select OK.

The Global Configuration options will be displayed



8. Select the Capture Source Nodes + Add Node.

The Add Source Node panel will be displayed



Direction Input

9. Flow Match may be enabled. If so, select the desired flow.

10. Select the desired Port(s). A TAP group must be previously created.

11. Select Link Aggregation name. The link aggregation group must be previously created.

Direction Output

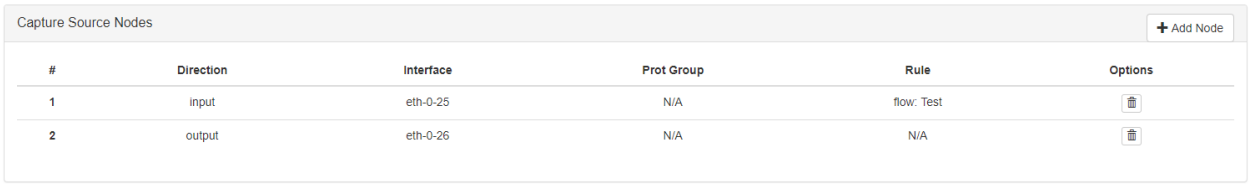
12. Access-list Match may be enabled. If so, select the desired ACL.

13. Select the desired Port(s). A TAP group must be previously created.

14. Select Link Aggregation name. The link aggregation group must be previously created.

15. Select Add Nodes.

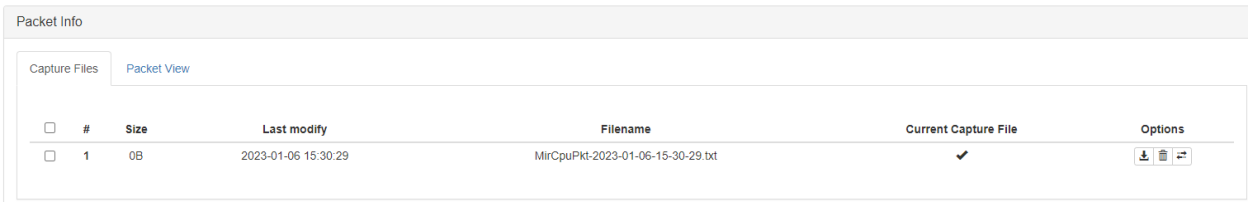
The Capture Source Nodes will be displayed



16. Select the Trash Can in the Options column to delete a node.

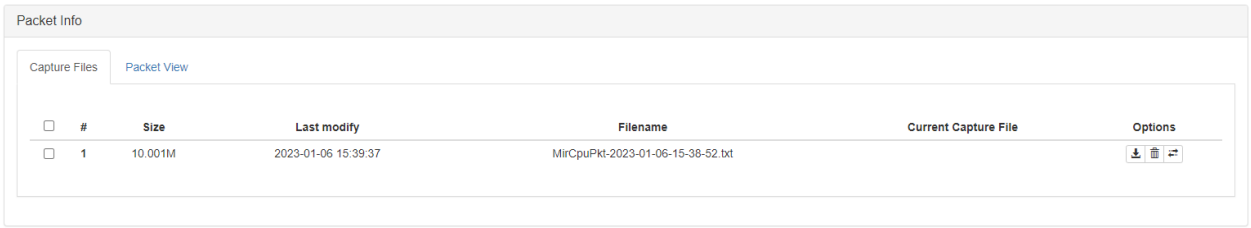
17. Select Start Capture.

The Packet Info panel will display the txt file. A (check) will be displayed indicating the Current Capture File



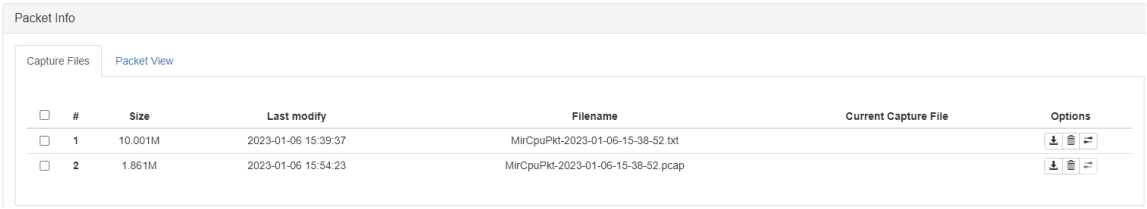
18. Select Stop Capture.

The Packet Info panel will display the txt file. A (check) will not be displayed indicating the Current Capture File



19. Select Download in the Options column to download the txt file.
20. Select Trash Can in the Options column to delete the txt file.
21. Select Convert to pcap in the Options column to create a pcap file.

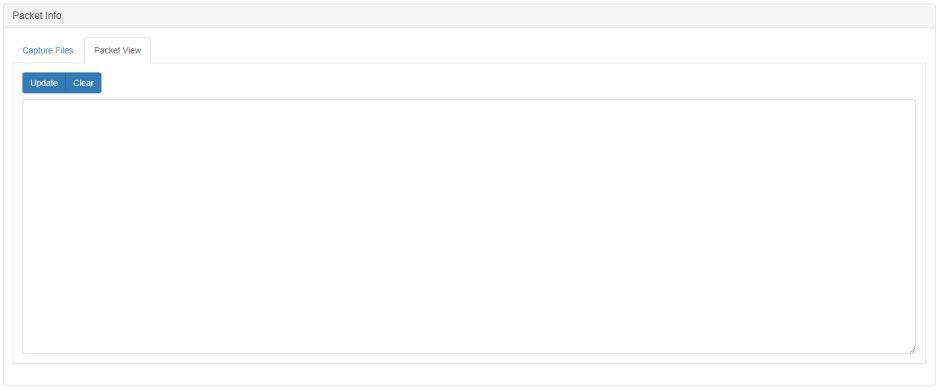
The Packet Info panel will display the pcap file.



22. Select Download in the Options column to download the pcap file.
23. Select Trash Can in the Options column to delete the pcap file.

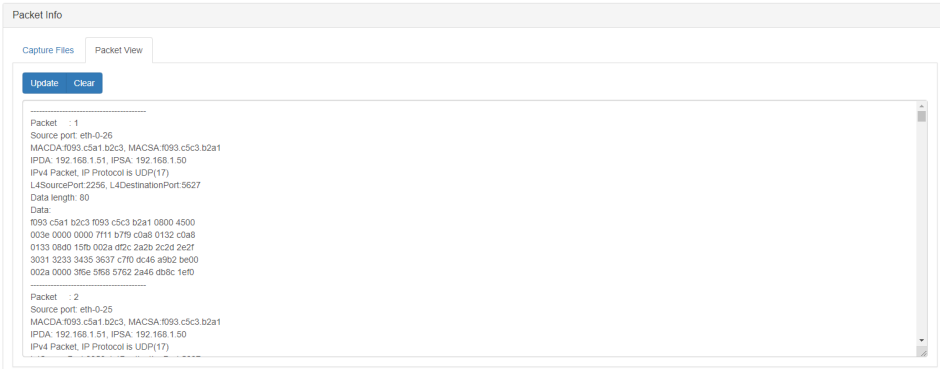
24. Select Packet View Tab.

The Packet View panel will be displayed.



25. Select Update.

The Packet View panel will display the latest packets.



26. Select Clear to clear the packet information.