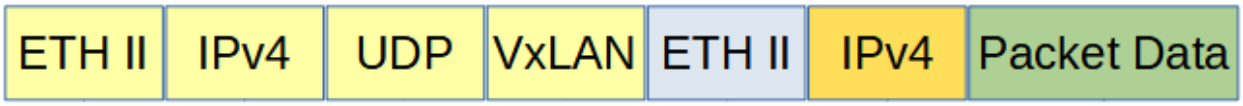
Encapsulate

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.

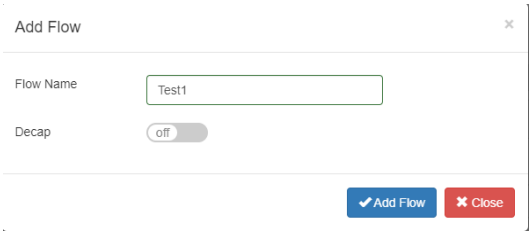
- Create a flow to add the VxLAN header
- Create a TAP Group

This document 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 Guide.

Create a Flow

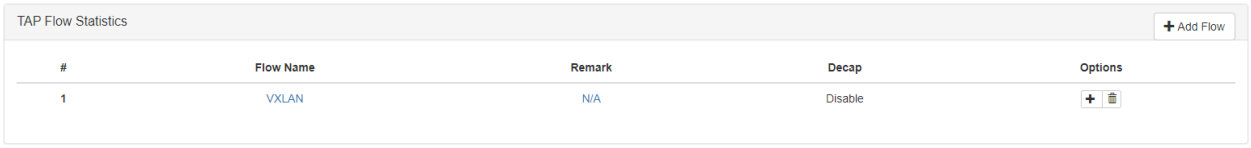
1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

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. Action permit

8. IP Protocol Number any

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. Add Vxlan enable

11. Vxlan-dest-mac Enter the desired address. This defines the destination MAC in the L2 segment of the VXLAN header.

12. Vxlan-src-ip Enter the desired address. This defines the source IP in the L3 segment of the VXLAN header.

13. Vxlan-dest-ip Enter the desired address. This defines the destination IP in the L3 segment of the VXLAN header.

14. Vxlan-dst-port Enable to enter the UDP destination port in the VXLAN header other than the default 4789. The system will automatically define the UDP destination port value as 4789.

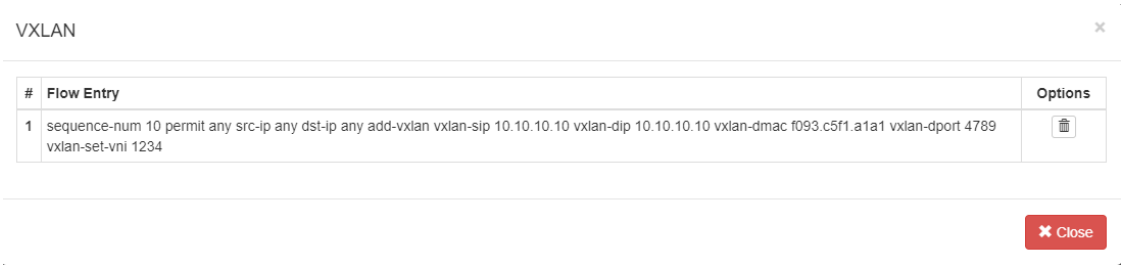
15. Vxlan-src-port Enable to enter the UDP source port in the VXLAN header other than the default 0. The system will automatically define the UDP source port value as 0.

16. Vxlan-vni-num Enter the desired VXLAN VNI number. The range is 1 to 16777215.

17. Select OK.

18. Select the flow name to display the attributes.

The Flow Entry panel will be displayed

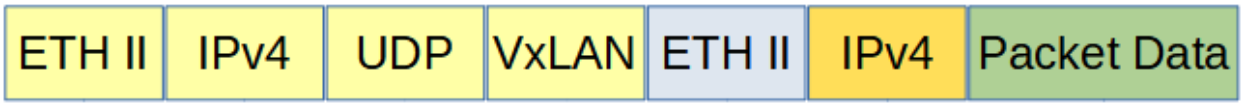


Additional entries may be created for the flow. Entries may be deleted by selecting the Trash Can. Entries may not be modified.

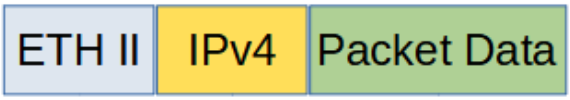
Decapsulate

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

VxLAN Encapsulated Packet



VxLAN Decapsulated Packet



The 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.

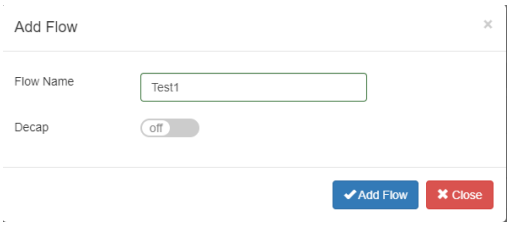
- Create a flow to strip the VxLAN header
- Create a TAP Group

This document 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 Guide.

Create a Flow (Decapsulate VxLAN per VNI)

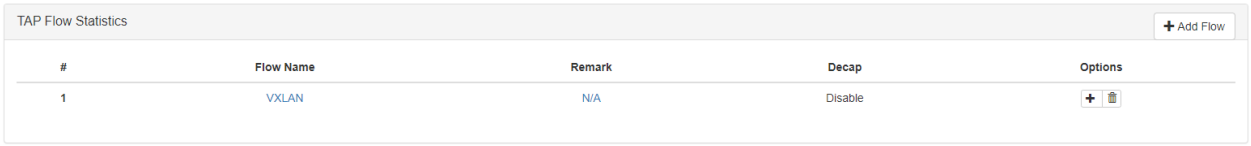
1. Select TAP Management.
2. Select Flow.
3. Select + Add Flow.

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

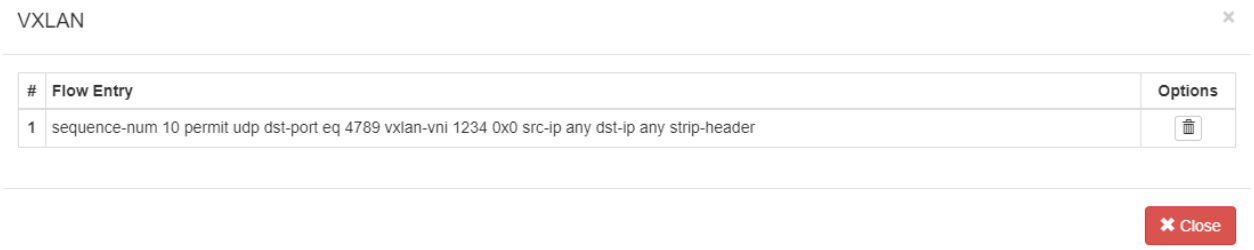
Flow Match Rule Options

7. Action permit
8. IP Protocol Number udp
9. Dst-port enable
10. Type eq
11. Port 4789
12. Vxlan-VNI enable
13. ID VxLAN VNI value
14. Wildcard 0x0
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. Strip-header enable
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)

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.

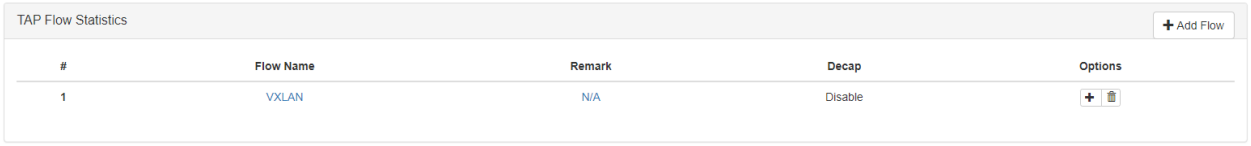
1. Press the Return key.
2. Enter enable.
3. Enter configure terminal.
4. Enter the following commands to create the flow.

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

VXLAN is the flow name.

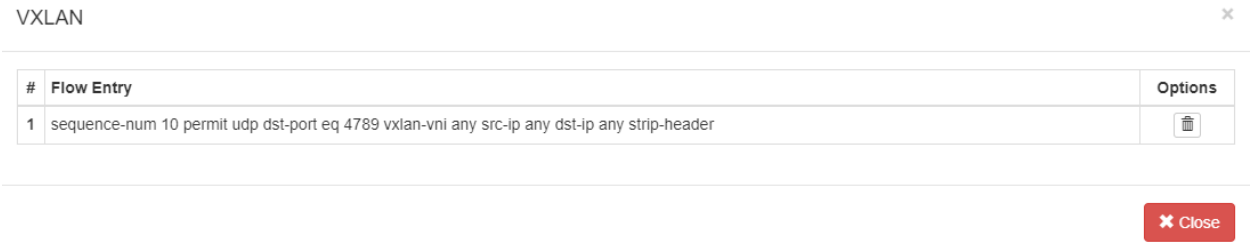
```
Switch(config-flow-VXLAN)# permit udp dst-port eq 4789 vxlan-vni any src-ip any
                           dst-ip any strip-header
```

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.