AA10G54xx

VXLAN Encapsulate

Overview:

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 Ethernet II, VLAN, Ipv4, UDP and VXLAN as shown below. VXLAN Encapsulation is not supported if Match Mode is enabled.

Original Packet

VXLAN Encapsulated Packet

Encapsulating a packet with a VXLAN header involves three configuration processes.

1. Create a Pass Filter

2. Create a VXLAN Tunnel Port

3. Create a Mapping Rule

1. Create a Pass Filter

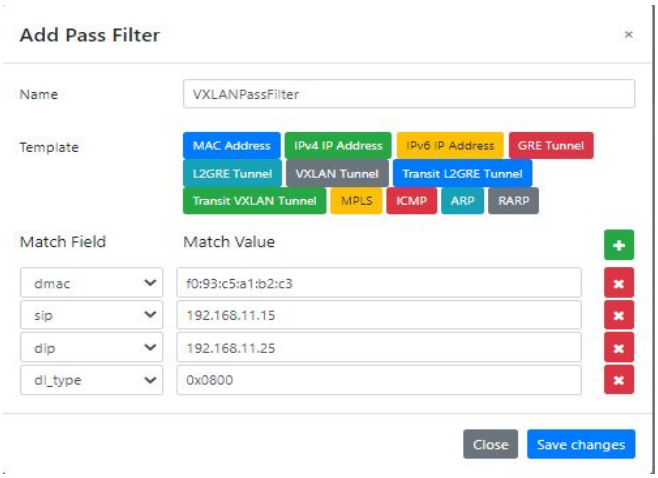
The pass filter defines which packets will be encapsulated with a VXLAN header. Packets that do not meet the pass filter attributes will not be encapsulated. In some cases it may be required to create more than 1 pass filter.

1. Select Mapping.

2. Select Pass Filter.

3. Select the GREEN + to create a new pass filter.

   The Add Pass Filter panel will appear.



4. Select the Transit VXLAN Tunnel template. When Transit VXLAN Tunnel is selected the pass filter will automatically display the required options; dmac, sip, dip and dl_type. The dl_type is already defined as 0x0800.

5. Enter the Name.

6. Enter the Destination MAC found in the Ethernet II segment of the packet to be encapsulated.

7. Enter the Source IP found in the IPv4 segment of the packet to be encapsulated. A mask may be added to the Source IP such as: 1.1.1.1/32, 1.1.1.0/24, 1.1.0.0/16 or 1.0.0.0/8.

8. Enter the Destination IP found in the IPv4 segment of the packet to be encapsulated. A mask may be added to the Destination IP such as: 1.1.1.1/32, 1.1.1.0/24, 1.1.0.0/16 or 1.0.0.0/8.

9. Select Save Changes.

2. Create a VXLAN Tunnel Port

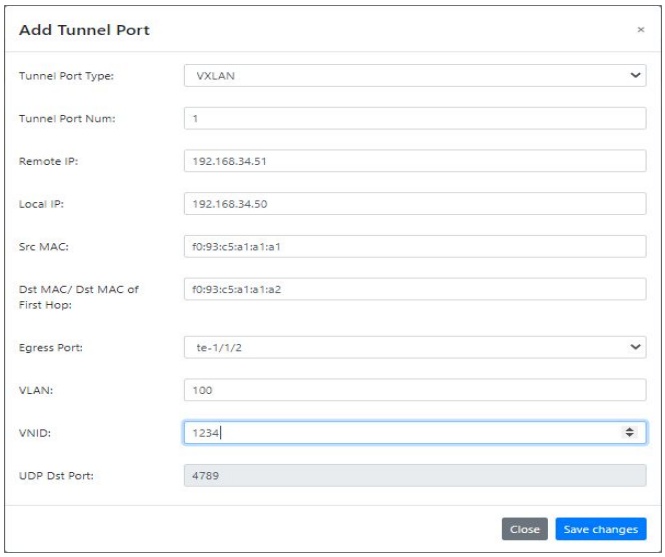
The VXLAN Tunnel Port defines the VXLAN header attributes and egress port.

1. Select Port Groups.

2. Select Tunnel Ports.

3. Select the GREEN + to create a new VXLAN tunnel port.

The Add Tunnel Port panel will appear.



4. Select the Tunnel Port Type VXLAN.

5. Enter the Tunnel Port Number, (1-1023).

6. Enter the Remote IP. This defines the Destination IP in the IPv4 segment of the VXLAN header.

7. Enter the Local IP. This defines the Source IP in the IPv4 segment of the VXLAN header.

8. Enter the Src MAC. This defines the Source MAC in the Ethernet II segment of the VXLAN header.

9. Enter the Dst MAC. This defines the Destination MAC in the Ethernet II segment of the VXLAN header.

10. Select the Egress Port.

11. Enter the VLAN. This defines the VLAN in the VLAN segment of the VXLAN header.

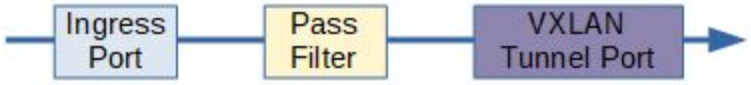
12. Enter the VNID, (1-16777215).

13. The UDP Destination Port is default, 4789 for VXLAN.

14. Select Save Changes.

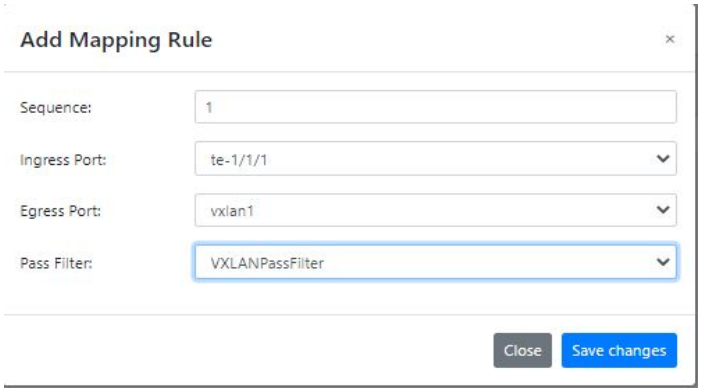
3. Create a Mapping Rule

The Mapping Rule defines the ingress port, pass filter and VXLAN tunnel port.



1. Select Mapping.
2. Select Mapping Rules.
3. Select the GREEN + to create a new mapping rule.

   The Add Mapping Rule panel will appear.



4. Enter the Sequence number. The range 1-1000. The sequence number defines the priority of the mapping rule. The priority is established based on highest number to lowest number.
5. Select the Ingress Port.
6. Select the Egress Port. The VXLAN tunnel port.
7. Select the Pass Filter. The pass filter defines which packets are encapsulated with a VXLAN header.
8. Select Save Changes.

AA10G54xx

VXLAN Decapsulate

Overview:

When a VXLAN packet is decapsulated the VXLAN header segments are removed from the packet as shown below. VXLAN decapsulation is not supported if Match Mode is enabled.

VXLAN Encapsulated Packet

VXLAN Decapsulated Packet

Decapsulating the VXLAN header from a packet involves three configuration processes.

1. Create a Pass Filter

2. Create an Action

3. Create a Mapping Rule

1. Create a Pass Filter

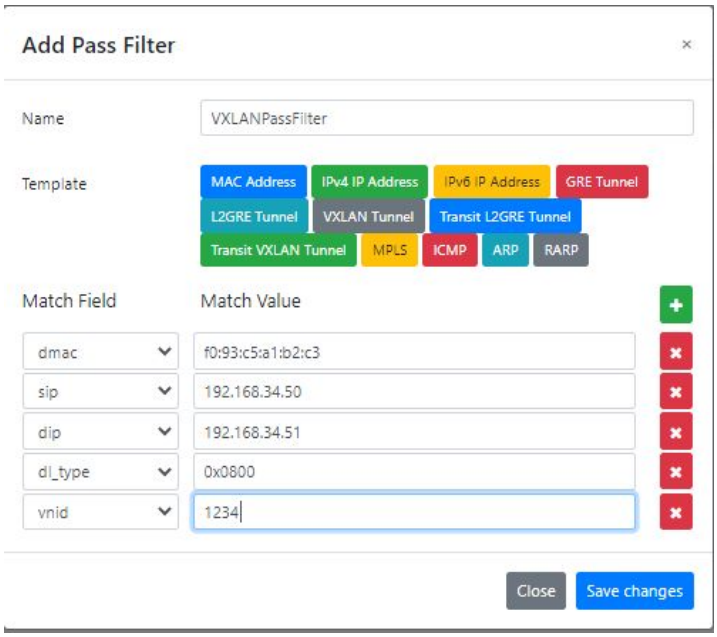
The pass filter defines which VXLAN packets will be decapsulated. Packets that do not meet the pass filter attributes will not be decapsulated. In some cases it may be required to create more than 1 pass filter.

1. Select Mapping.

2. Select Pass Filter.

3. Select the GREEN + to create a new pass filter.

   The Add Pass Filter panel will appear.



4. Select the VXLAN Tunnel template. When VXLAN Tunnel is selected the pass filter will automatically display the required options; dmac, sip, dip, vnid and dl_type. The dl_type is already defined as 0x0800.

5. Enter the Name.

6. Enter the Destination MAC found in the Ethernet II VXLAN header segment of the packet to be decapsulated.

7. Enter the Source IP found in the IPv4 VXLAN header segment of the packet to be decapsulated. A mask may be added to the Source IP such as: 1.1.1.1/32, 1.1.1.0/24, 1.1.0.0/16 or 1.0.0.0/8.

8. Enter the Destination IP found in the IPv4 VXLAN header segment of the packet to be decapsulated. A mask may be added to the Destination IP such as: 1.1.1.1/32, 1.1.1.0/24, 1.1.0.0/16 or 1.0.0.0/8.

9. Enter the VNID found in the VXLAN header segment of the packet to be decapsulated.

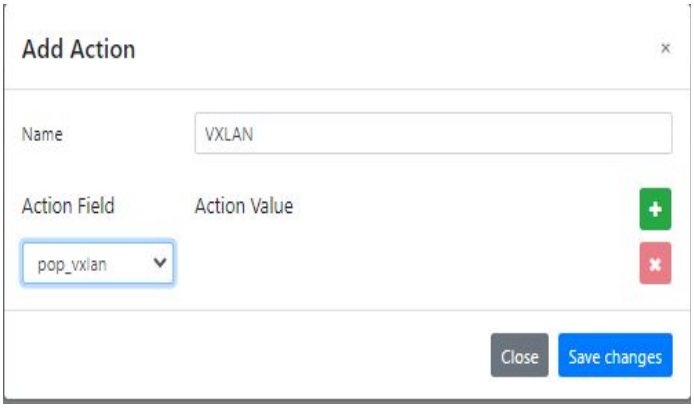
10. Select Save Changes.

2. Create an Action

The action provides the ability for the VXLAN header to be decapsulated from the packets.

1. Select Mapping.
2. Select Action.
3. Select the GREEN + to create an action.

The Add Action panel will appear.



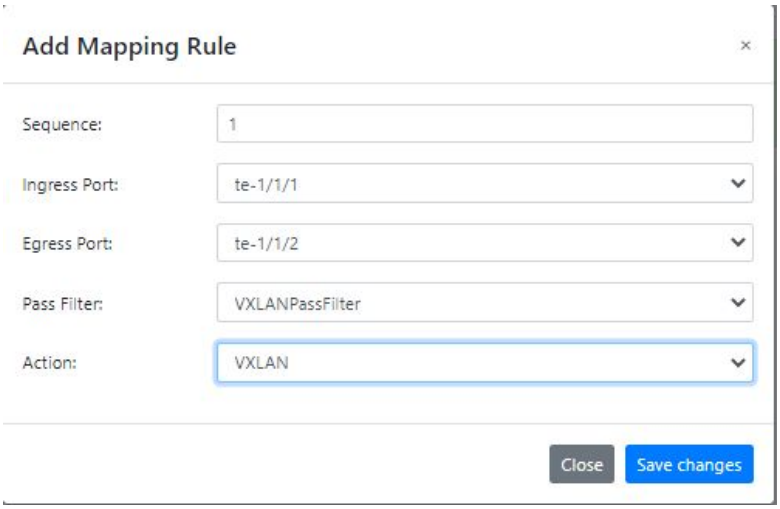
4. Enter the Name.
5. Select the Action Field, pop_vxlan.
6. Select Save Changes.

3. Create a Mapping Rule

The Mapping Rule defines the ingress port, pass filter, action and egress port.

1. Select Mapping.
2. Select Mapping Rules.
3. Select the GREEN + to create a new mapping rule.

   The Add Mapping Rule panel will appear.



4. Enter the Sequence number. The range 1-1000. The sequence number defines the priority of the mapping rule. The priority is established based on highest number to lowest number.
5. Select the Ingress Port.
6. Select the Egress Port.
7. Select the Pass Filter. The pass filter defines which VXLAN packets are decapsulated.
8. Select the Action. (pop_vxlan)
9. Select Save Changes.