

AA1G52xx / AA10G54xx / AA100G32xx-64xx

L2GRE Encapsulate

Overview:

When a packet is encapsulated with a L2GRE header the new L2GRE header segments are added to the original packet. The L2GRE header segments consists of Ethernet II, VLAN, IPv4 and L2GRE as shown below. L2GRE Encapsulation is not supported if Match Mode is enabled.

Original Packet



L2GRE Encapsulated Packet



Encapsulating a packet with a L2GRE header involves three configuration processes.

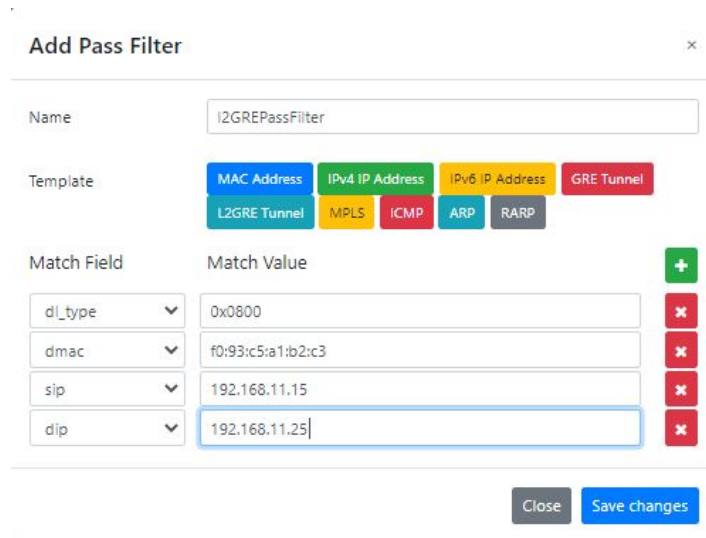
1. Create a Pass Filter
2. Create a L2GRE Tunnel Port
3. Create a Mapping Rule

1. Create a Pass Filter

The pass filter defines which packets will be encapsulated with a L2GRE 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.



Match Field	Match Value
d_type	0x0800
dmac	f0:93:c5:a1:b2:c3
sip	192.168.11.15
dip	192.168.11.25

4. Enter the Name.
5. Using the GREEN + add the following Match Fields. d_l_type, dmac, sip and dip. Do not select the L2GRE Tunnel template.
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 L2GRE Tunnel Port

The L2GRE Tunnel Port defines the L2GRE header attributes and egress port.

1. Select Port Groups.
2. Select Tunnel Ports.
3. Select the GREEN + to create a new L2GRE tunnel port.

The Add Tunnel Port panel will appear.

Add Tunnel Port

Tunnel Port Type: L2GRE

Tunnel Port Num: 1

Remote IP: 192.168.14.57

Local IP: 192.168.14.65

Src MAC: f0:93:c5:a1:a1:a1

Dst MAC/ Dst MAC of First Hop: f0:93:c5:a1:a1:a2

Egress Port: ge-1/1/2

VLAN: 100

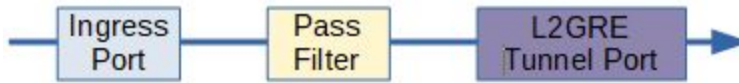
L2GRE Key: 1234

Close Save changes

4. Select the Tunnel Port Type L2GRE.
5. Enter the Tunnel Port Number, (1-1023).
6. Enter the Remote IP. This defines the Destination IP in the IPv4 segment of the L2GRE header.
7. Enter the Local IP. This defines the Source IP in the IPv4 segment of the L2GRE header.
8. Enter the Src MAC. This defines the Source MAC in the Ethernet II segment of the L2GRE header.
9. Enter the Dst MAC. This defines the Destination MAC in the Ethernet II segment of the L2GRE header.
10. Select the Egress Port.
11. Enter the VLAN. This defines the VLAN in the VLAN segment of the L2GRE header.
12. Enter the L2GRE Key, (1-16777215).
13. Select Save Changes.

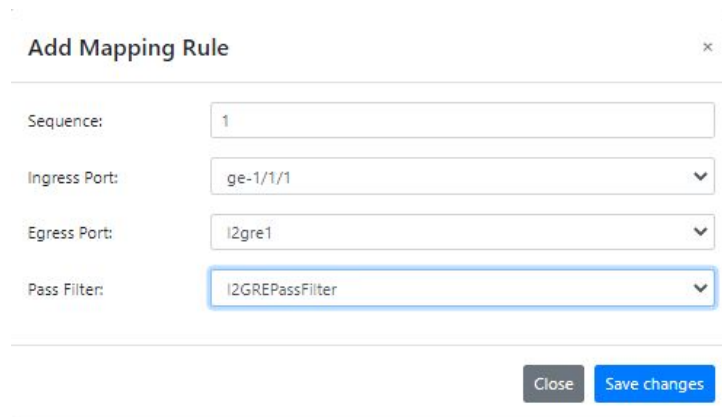
3. Create a Mapping Rule

The Mapping Rule defines the ingress port, pass filter and L2GRE 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.



Add Mapping Rule [x]

Sequence:

Ingress Port:

Egress Port:

Pass Filter:

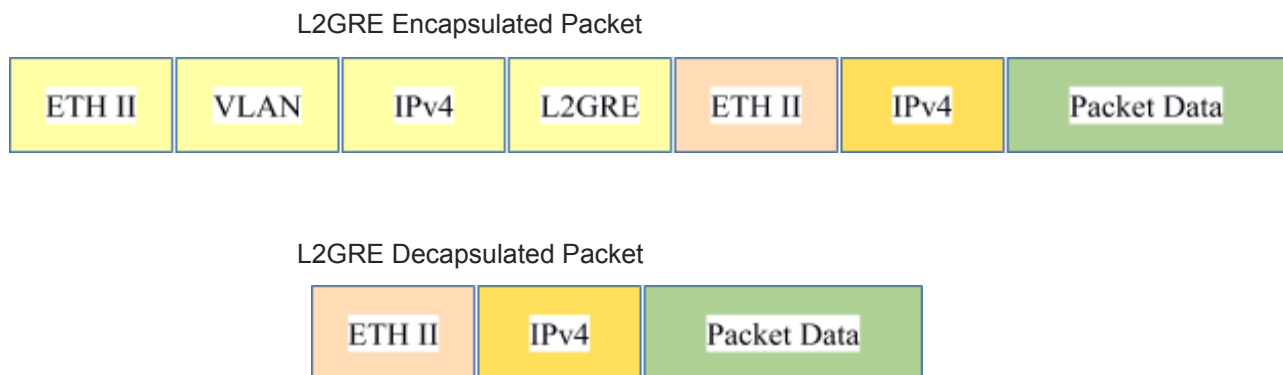
4. Enter the Sequence number. The range 1-1000. The sequence number defines the priority of the mapping rule. The priority is established based on highest number to lowest number.
5. Select the Ingress Port.
6. Select the Egress Port. The L2GRE tunnel port.
7. Select the Pass Filter. The pass filter defines which packets are encapsulated with a L2GRE header.
8. Select Save Changes.

AA1G52xx / AA10G54xx / AA100G32xx-64xx

L2GRE Decapsulate

Overview:

When a L2GRE packet is decapsulated the L2GRE header segments are removed from the packet as shown below. L2GRE Decapsulation is not supported if Match Mode is enabled.



Decapsulating the L2GRE header from a packet involves three configuration processes.

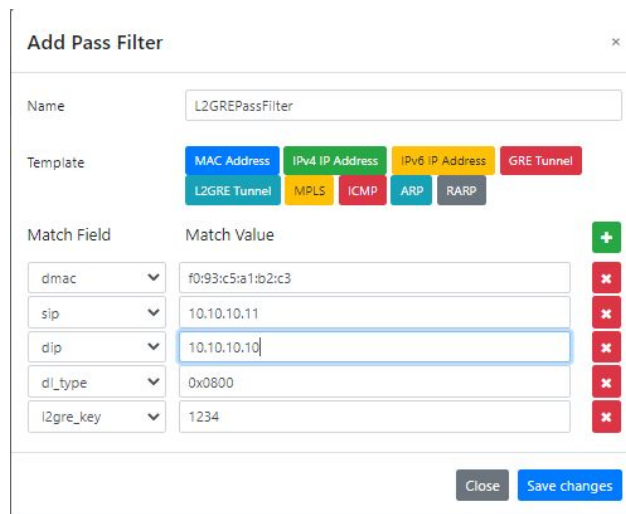
1. Create a Pass Filter
2. Create an Action
3. Create a Mapping Rule

1. Create a Pass Filter

The pass filter defines which L2GRE 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 L2GRE Tunnel template. When L2GRE Tunnel is selected the pass filter will automatically display the required options; dmac, sip, dip, l2gre_key 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 L2GRE header segment of the packet to be decapsulated.
7. Enter the Source IP found in the IPv4 L2GRE 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 L2GRE 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 L2GRE Key found in the L2GRE header segment of the packet to be decapsulated.
10. Select Save Changes.

2. Create an Action

The action provides the ability for the L2GRE 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.



The screenshot shows a modal window titled "Add Action" with a close button (x) in the top right corner. Inside the modal, there is a text input field for "Name" containing the text "L2GRE". Below this, there is a table with two columns: "Action Field" and "Action Value". The "Action Field" column contains a dropdown menu with "pop_l2gre" selected. To the right of the table, there are two buttons: a green button with a plus sign (+) and a red button with a minus sign (-). At the bottom right of the modal, there are two buttons: a grey "Close" button and a blue "Save changes" button.

4. Enter the Name.
5. Select the Action Field, pop_l2gre.
6. Select Save Changes.

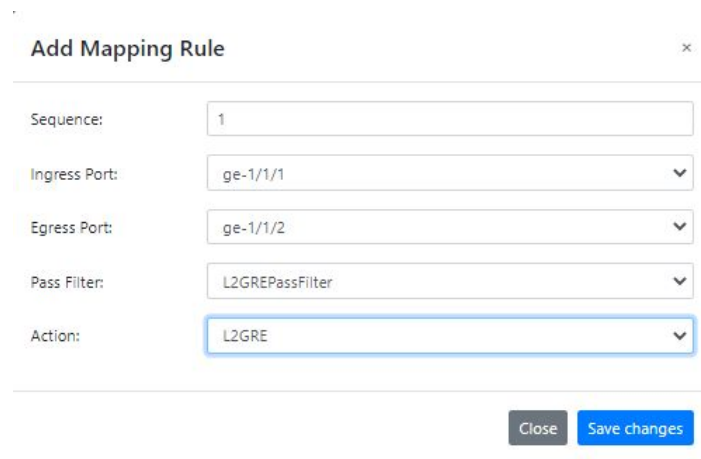
3. Create a Mapping Rule

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.



The screenshot shows a dialog box titled "Add Mapping Rule" with a close button (x) in the top right corner. It contains the following fields:

- Sequence: 1
- Ingress Port: ge-1/1/1
- Egress Port: ge-1/1/2
- Pass Filter: L2GREPassFilter
- Action: L2GRE

At the bottom right, there are two buttons: "Close" and "Save changes".

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 L2GRE packets are decapsulated.
8. Select the Action. (pop_l2gre)
9. Select Save Changes.