## AA1G52xx / AA10G54xx / AA100G32xx-64xx

GRE Encapsulate

Overview:

When a packet is encapsulated with a GRE header the original Ethernet II segment is removed from the packet and the new GRE header segments are added. The GRE header segments consists of Ethernet II, VLAN, IPv4 and GRE as shown below.

Original Packet

ETH II	IPv4	Packet Data

GRE Encapsulated Packet

ETH II	VLAN	IPv4	GRE	IPv4	Packet Data
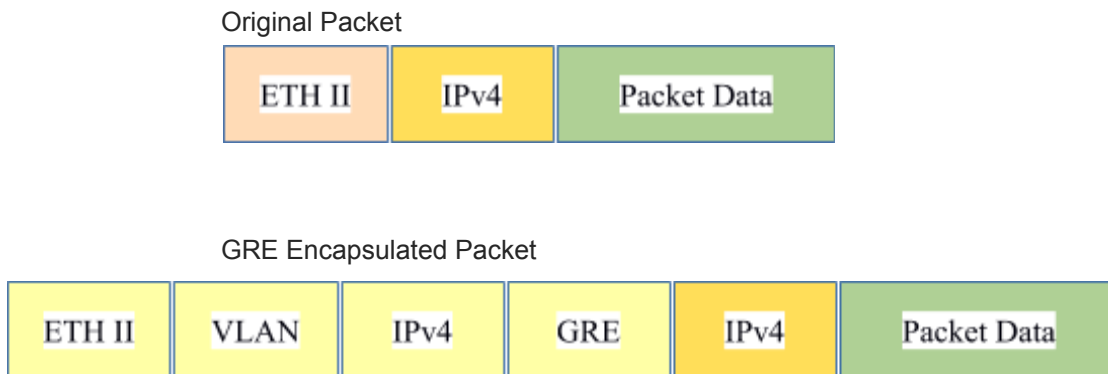
Encapsulating a packet with a GRE header involves three configuration processes.
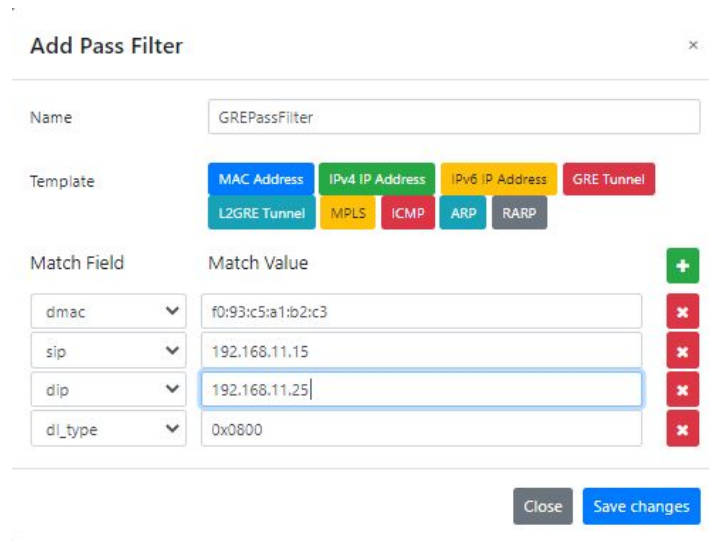
1. Create a Pass Filter

2. Create a GRE Tunnel Port

3. Create a Mapping Rule

1. Create a Pass Filter

The pass filter defines which packets will be encapsulated with a GRE 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 GRE Tunnel template. When GRE 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 GRE Tunnel Port

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

1. Select Port Groups.

2. Select Tunnel Ports.

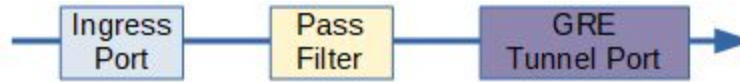3. Select the GREEN + to create a new GRE tunnel port.

> The Add Tunnel Port panel will appear.

4. Select the Tunnel Port Type GRE.

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

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

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

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

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

10. Select the Egress Port.

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

12. Select Save Changes.

3. Create a Mapping Rule

The Mapping Rule defines the ingress port, pass filter and GRE 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. If Match Mode is disabled the range 1-1000. If Match Mode is enabled the range L2-L4 Mode 1000-20000. 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 GRE tunnel port.

7. Select the Pass Filter. The pass filter defines which packets are encapsulated with a GRE header.

8. Select Save Changes.

AA1G52xx / AA10G54xx / AA100G32xx-64xx

GRE Decapsulate

Overview:

When a GRE packet is decapsulated the GRE header segments are removed from the packet and a new Ethernet II segment is added as shown below.

GRE Encapsulated Packet

ETH II	VLAN	IPv4	GRE	IPv4	Packet Data

GRE Decapsulated Packet

ETH II	IPv4	Packet Data
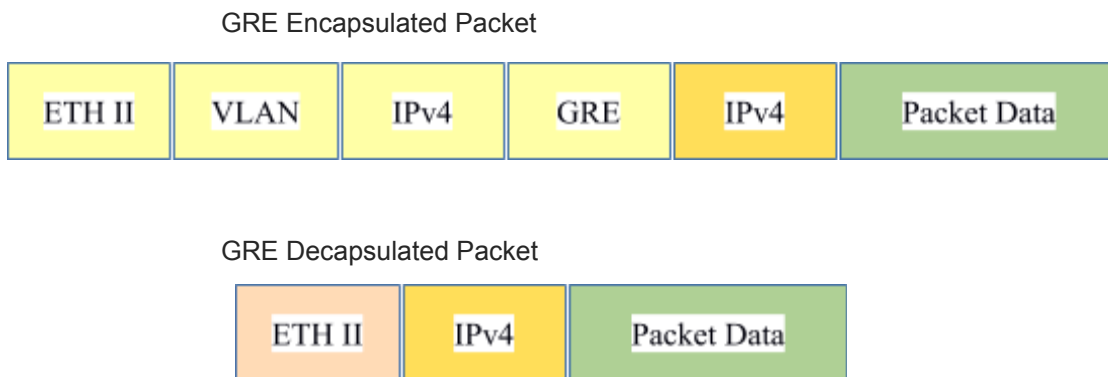
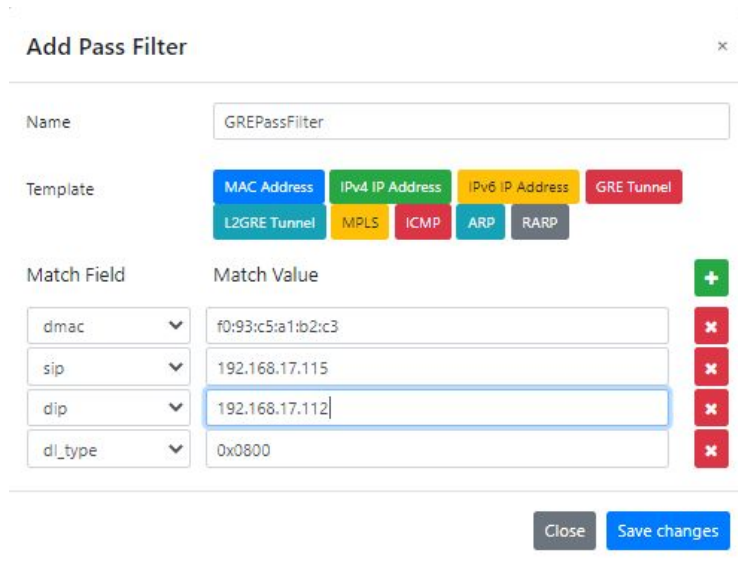Decapsulating the GRE header from a packet involves three configuration processes.

1. Create a Pass Filter

2. Create an Action

3. Create a Mapping Rule

1. Create a Pass Filter

The pass filter defines which GRE 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.
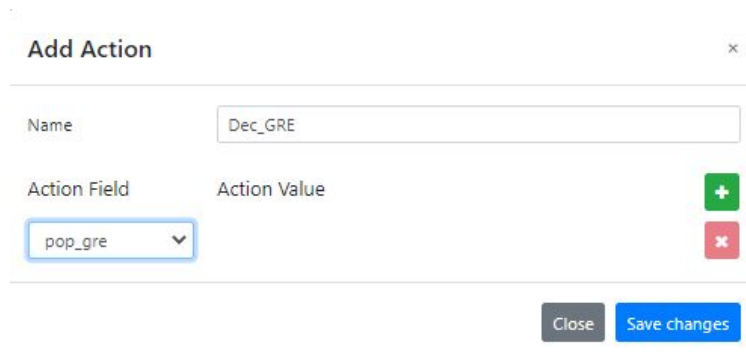
> The Add Pass Filter panel will appear.

4. Select the GRE Tunnel template. When GRE 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 GRE header segment of the packet to be decapsulated.

7. Enter the Source IP found in the IPv4 GRE 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 GRE 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. Select Save Changes.

2. Create an Action

The action provides the ability for the GRE 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_gre.

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. If Match Mode is disabled the range 1-1000. If Match Mode is enabled the range L2-L4 Mode 1000-20000. 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 GRE packets are decapsulated.

8. Select the Action. (pop_gre)

9. Select Save Changes.