Juniper Networks | Engineering Simplicity

Microsegmentation with VXLAN Group-Based Policies in IP Clos Fabric— Juniper Validated Design Extension (JVDE)

Published
2025-06-05

Table of Contents

Microsegmentation with VXLAN Group-Based Policies in IP Clos Fabric— Juniper Validated Design Extension (JVDE)

Juniper Networks Validated Designs provide customers with a comprehensive, end-to-end blueprint for deploying Juniper solutions in their network. These designs are created by Juniper's expert engineers and tested to ensure they meet the customer's requirements. Using a validated design, customers can reduce the risk of costly mistakes, save time and money, and ensure that their network is optimized for maximum performance.

About this Document

Overview

This document focuses on a VXLAN group-based policies (GBP) reference design using a Juniper Mist™-managed Campus Fabric IP Clos. The intent is to demonstrate how VXLAN GBPs can be implemented in a campus fabric to achieve microsegmentation beyond the level of traditional ACL-based designs. As a result of reviewing this JVD, you will learn how to leverage these features in your own network designs.

This document describes the basics of how VXLAN GBPs work and the enhancements Juniper Networks provides to the IETF standards-based approach. Common implementation questions and potential limits are also discussed. We discuss which tests are performed for this JVD. In the appendix section of this JVD, we share details about how you can repeat these tests in your own environment.

Solution Overview

Enterprise networks are undergoing massive transitions to accommodate the growing demand for cloud-ready, scalable, and efficient networks. There's also demand for a plethora of Internet of Things (IoT) and mobile devices. As the number of devices grows, so does network complexity with an ever-greater need for microsegmentation and security. To meet these challenges, you need a network with automation and Artificial Intelligence (AI) for operational simplification. A Juniper Networks Campus Fabric IP Clos supporting microsegmentation with GBPs is a highly scalable, standards-based architecture (https://www.rfc-editor.org/rfc/rfc8365). This architecture delivers consistent and optimized enterprise security requirements managed through the Juniper Mist™ portal.

Solution Benefits

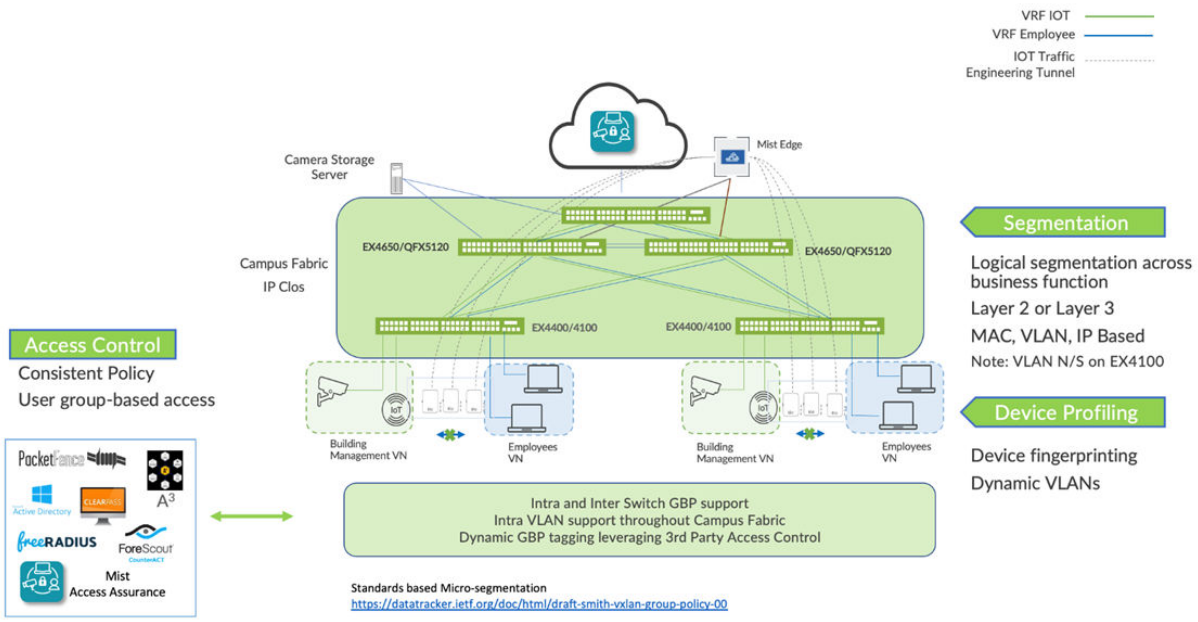
With group-based policies (GBP), you can enable microsegmentation at the access layer within a campus fabric IP Clos and leverage EVPN-VXLAN to provide traffic isolation within and between broadcast domains as well as simplify security policies across a campus fabric. See Figure 1 on page 3.

There are several benefits of microsegmentation with GBP:

Standards based — https://datatracker.ietf.org/doc/html/draft-smith-vxlan-group-policy-05

- Simplified Workflow—GBPs are administered through the Juniper Mist portal and provide a simple and well understood workflow for network wide policy control and enforcement. GBPs also simplify network configuration by avoiding the need for large numbers of firewall filters on all devices to ensure lateral threat protection.
- Consistency—GBPs provide consistent, customer-managed security policies across the enterprise through the Juniper Mist portal.
- Location-agnostic connectivity—GBPs leverage underlying VXLAN technology to provide location-agnostic endpoint access control.
- More granular control—Because GBP can be enforced as a Layer 2 method, it provides tighter control than with traditional ACL-based methods. Using VXLAN with GBP, you can block traffic to and from clients inside the same VLAN.
- Network access Control—GBPs allow for dynamic or static tagging of wired clients.
  - Dynamic GBP tagging works with industry standards-based RADIUS and network access control platforms, including the cloud-based Juniper Mist Access Assurance.
  - Static GBP tagging allows you to assign GBP tags by IP prefix, MAC address, VLAN, and port on all access ports in the fabric.

Figure 1: Solution Overview



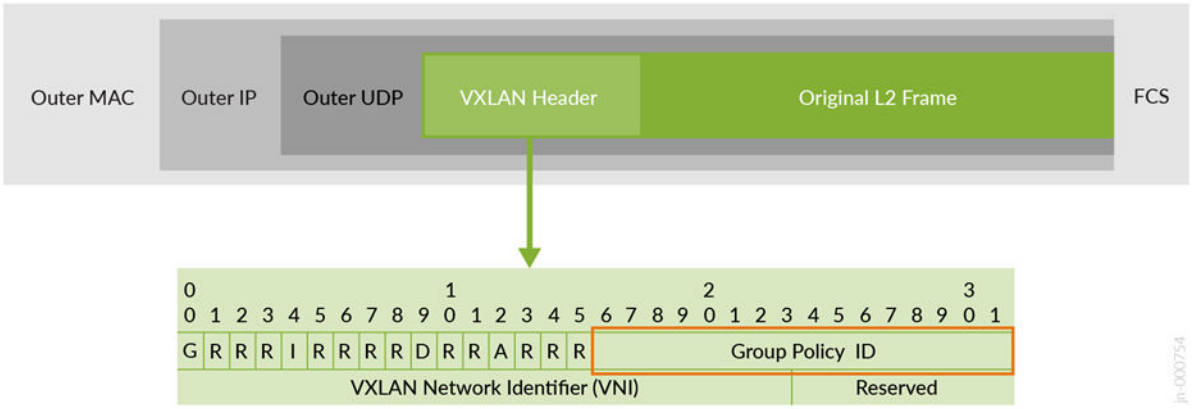
Use Case and Reference Architecture

You can achieve macro and microsegmentation, for example to secure data and assets, in a VXLAN architecture using GBP. GBPs leverage underlying VXLAN technology to provide location-agnostic endpoint access control. GBPs allow you to implement consistent security policies across your enterprise network domains. You can simplify your network configuration by using GBP, avoiding the need to configure large numbers of firewall filters on all your switches. GBPs block lateral threats by ensuring consistent application of security group policies throughout the network, regardless of the location of endpoints or users. VXLAN-GBP works by leveraging a reserved field in the VXLAN header for use as a Scalable Group Tag (SGT). You can use the SGTs as match conditions in firewall filter rules. Using an SGT is more robust than using port or MAC addresses to achieve similar results. Scalable Group Tags can be assigned statically (by configuring the switch on a per-port or per-MAC basis), or they can be configured on the RADIUS server and pushed to the switch through 802.1X when the user is authenticated.

The segmentation enabled by VXLAN-GBP is especially useful in campus VXLAN environments because it gives you a practical way to create network access policies that are independent of the underlying network topology. It simplifies the design and implementation phases of developing network application and endpoint-device security policies.

You can find more detailed information on the VXLAN-GBP standard in the IEEE RFC, I-D.draft-smith-vxlan-group-policy. For the purposes of this example architecture, VXLAN-GBP leverages a reserved field in the VXLAN header as an SGT, as shown in Figure 2 on page 4.

Figure 2: Group Policy ID within VXLAN Header



Starting with Junos OS Release 22.4R1, Juniper Networks switches support VXLAN-GBP in egress and ingress enforcing mode as described below:

- GBP egress enforcement:
  - This is the IETF standards-based approach.
  - The GBP tag is part of the VXLAN data plane and needs to be set as the group policy ID in the VXLAN header.
  - For verification of the destination GBP tag from a remote switch, the packet must be sent to the remote switch every time. The remote switch can then act as an enforcement point for traffic egressing the fabric to the next wired client and can, based on SGT Policy, block the traffic, and discard the packet.
- GBP ingress enforcement:
  - This is a Juniper Networks proprietary enhancement to the Junos GBP and SGT implementations.
  - This enhancement is available starting with Junos OS Release 22.4R1.
  - Here, the GBP tag is an extension of the control plane (MP-BGP extension).
  - The GBP tag information is added through a vendor-specific attribute to the EVPN Type-2 MAC and IP address information that the fabric shares among its nodes. In this case, the group policy ID in the VXLAN header is always left zero as it is not used for enforcement.

- The huge advantage is that the destination GBP tag of a wired client present on a remote switch is already known because it's learned through the control plane. With this enhancement, the SGT on the local switch where the source wired client is attached can pre-emptively block traffic that is not allowed to be sent to a destination client on a remote switch. The enforcement of SGTs always happens at the ingress wired client switch. The need for sending all traffic through the fabric even though it may get discarded by the SGT, as in the standards-based approach, does not happen with this solution.

- This extension makes it easier for administrators to debug GBP-based traffic forwarding decisions. You can review a local switch to know if traffic would be allowed or blocked by a remote switch. Junos OS commands like

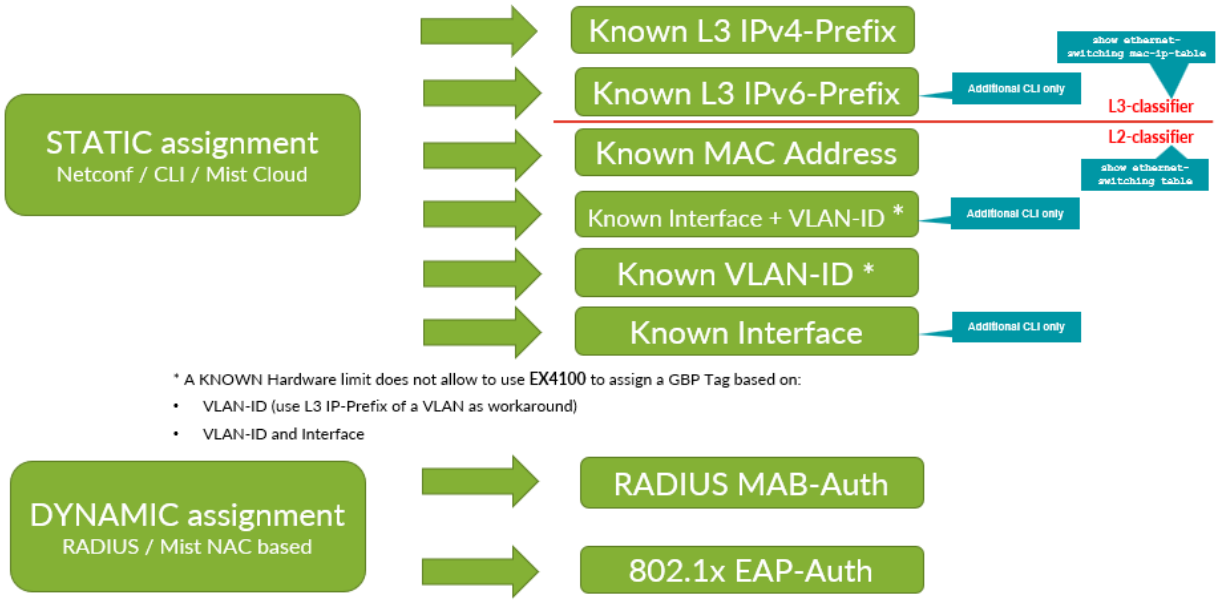
  ```
  show ethernet-switching table
  display
  ```

  GBP tag information of local and remote wired clients.

NOTE: Juniper Mist-managed campus fabrics automatically activate ingress GBP enforcement.

There are different ways you can apply a GBP tag to a wired client to be used by the SGTs to allow or block traffic. See Figure 3 on page 5.

Figure 3: How a GBP tag is typically assigned



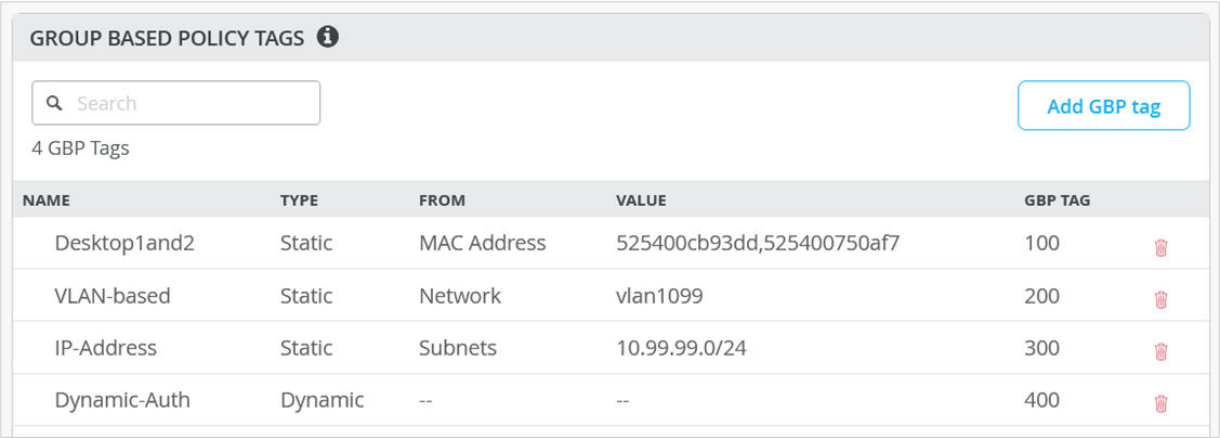
You can assign GBP tags as follows:

- For static GBP tag assignment:
  - You must configure static assignment to identify a wired client and assign the GBP tag to it.
  - Match criteria (depending on Junos OS release version) can be:
    1. Layer 3 IPv4 prefixes and hosts
    2. Layer 3 IPv6 prefixes and hosts
    3. Layer 2 MAC address
    4. Switch interface/port and VLAN ID (not supported on Juniper Networks® EX4100 Switches).
    5. Layer 2 VLAN ID (not supported on EX4100 Switches).
    6. Switch interface/port
- For dynamic GBP tag assignment:
  - The wired client needs to be authenticated at the switch port when entering the fabric.
  - Is based on RADIUS server authorization information which is part of the RADIUS access accept message.
  - The wired client authentication can be:
    - IEEE 802.1X EAP-based
    - MAC Authentication Bypass (MAB)

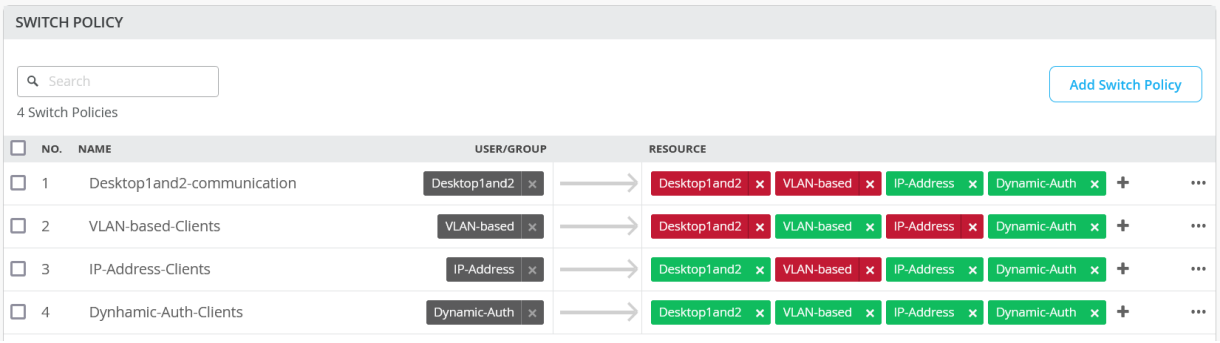
NOTE: There is no prioritization between any static GBP tag and dynamic GBP tag assignment. A port can only be used for one of the two assignment methods at any time. Dynamic GBP tag assignment will override any static GBP assignment should you have a conflict. Currently, there is no support for cascading these methods.Within static GBP tag assignment, there is prioritization among the match criteria, but only for those within the same layer (within Layer 2 or within Layer 3). This is because Juniper Mist cloud automatically activates Layer 2 to Layer 3 tagging propagation, but the classification is done in separate tables. For example, a static classifier for IPv4 does not override a static MAC address classifier because of this separation. However, a MAC address classifier overrides a VLAN-based tag classification because of higher priority.

The Juniper Mist portal simplifies this process and abstracts the switch configuration needed as shown in Figure 4 on page 7.

Figure 4: GBP tags in the Mist GUI



After defining the GBP tag assignment, you need to specify the SGTs as switch policies. Again, the Juniper Mist cloud simplifies and abstracts this process in its portal, allowing you to build an intuitive communication matrix.



NOTE: We strongly recommend using a switch template to configure static or dynamic GBP tag assignments and SGT policies since the templates ease the task of distributing this information across all access switches of an IP Clos fabric.

Validation Framework

IN THIS SECTION

To be able to test VXLAN GBPs you must have the following in place:

- Wired clients with a known MAC address you can configure in the Juniper Mist cloud or on a RADIUS server.
- Wired clients with 802.1X EAP supplicant support.
- The wired clients IP address can be configured either:
  - With a pre-configured static IP address
  - As a DHCP client. In this case, the fabric needs to be configured for:
    - DHCP relay for the fabric towards the DHCP server.
    - A DHCP server attached to hand out the DHCP lease back to the wired client.
- A Juniper Mist-managed campus fabric with IP Clos configuration:
  - Configured as either a 3-stage or 5-stage fabric.
  - Has WAN routers attached to the fabric.
  - That uses EX4100 or Juniper Networks® EX4400 access switches that MUST be running Junos OS Release 24.2R2 or higher.
  - May use optional service block switches.
- RADIUS server:
  - Any third-party RADIUS server that is reachable via the fabric management network.
  - Juniper Mist Access Assurance (NAC) that is reachable via the Internet.
  - A minimum enterprise PKI for the EAP authentications between client (supplicant) and RADIUS server to be performed.

- Wi-Fi access points are optional.

Test Bed

We tested a 5-Stage IP Clos fabric which was managed via Juniper Mist cloud.

The access switches were configured as either:

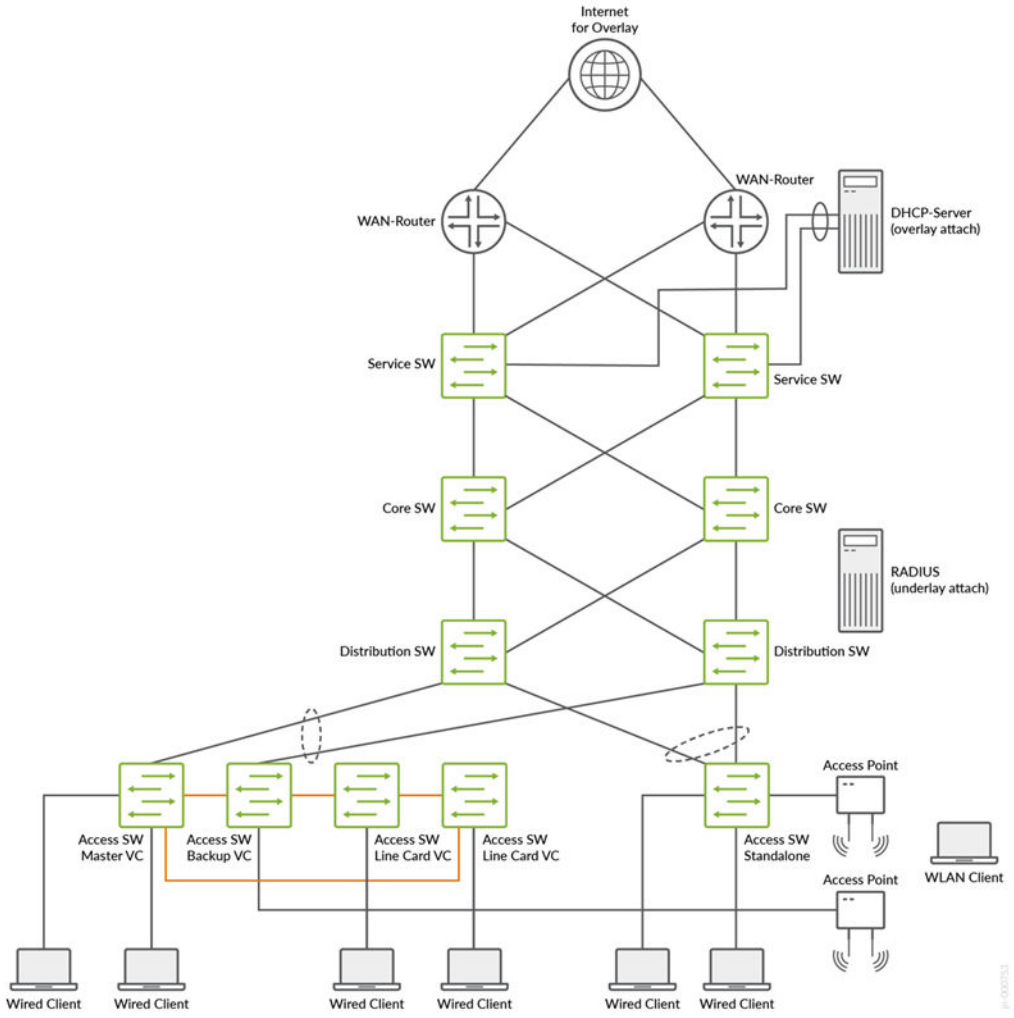
- Virtual Chassis with 4 members
- Standalone switches

The local RADIUS server was a FreeRADIUS virtual machine and Juniper Mist Access Assurance tests were operated via the Juniper Mist auth cloud.

All wired clients were emulated via Spirent testing equipment.

The test bed topology can be seen in Figure 5 on page 10:

Figure 5: 5-Stage IP-Clos with Dedicated Service Block Switches



Platforms / Devices Under Test (DUT)

To review the software versions and platforms on which this JVD was validated by Juniper Networks, see the Validated Platforms and Software section in this document.

Test Bed Configuration

We are sharing information on exactly how some of the tests are performed. For more information, see the appendix section of this document. Contact your Juniper Networks representative to obtain the full archive of the test bed configuration used for this JVD.

Considerations when implementing VXLAN-GBP

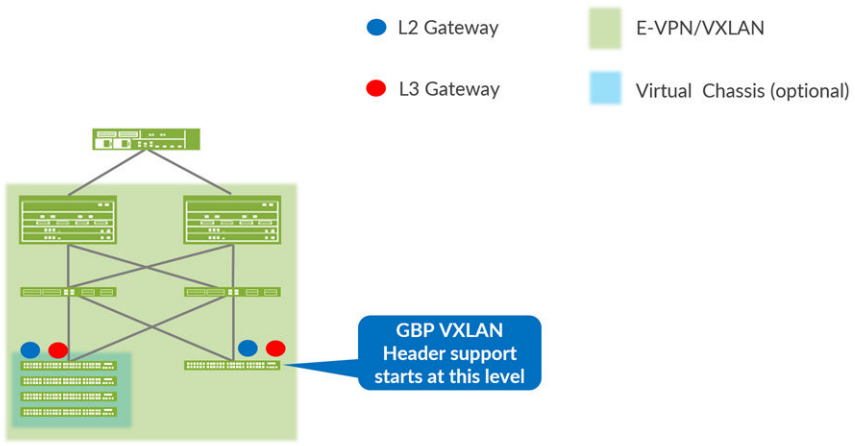
IN THIS SECTION

There are a few areas to consider when testing VXLAN-GBP support as covered in this document.

VXLAN-GBP Needs IP Clos Fabrics

The technology only supports VXLAN-GBP in an IP Clos fabric because this is the only design where the VXLAN Layer 2 VTEP is supported at the access switch layer.

Figure 6: Group-Based Policy Support



	Campus Fabric IP Clos
Technology	End-to-End VPN
Positioning	• Medium/large campus • Intra-campus traffic (E/W) • Recommended when L3 at access
Advantages	• Access layer segmentation • Ideal for mobility and IoT devices

All other fabric types like EVPN multihoming, centrally-routed bridging (CRB), and edge-routed bridging (ERB) do not allow GBP tag management of wired clients because:

- The VXLAN layer starts at the distribution or collapsed core layer, hence, wired clients can communicate uncontrolled to each other locally from port-to-port within the same access switch. Private VLANs do not help in this case because they are created through static Junos OS configuration and won't follow a dynamically assigned GBP tag.
- There is only a standard LAG established between the access switch and upper switches such as distribution or collapsed core. Hence, between these stages of the fabric-only VLANs and MAC addresses play a role, and the GBP tag gets lost in transit. You must start with VXLAN at the lowest stage of the fabric.
- For wired clients performing dynamic RADIUS-based authentication, the wired client gets a GBP tag assigned as part of the authorization process on the access switch it is attached to. Again, there is no additional protocol to pass this information to the upper fabric stage, so this information is unseen by the fabric and cannot be reconstructed by it.

NOTE: You can attach a desktop switch to the fabric's access switch to manage, for example, a VoIP phone and a PC on a campus fabric IP Clos. If you want to perform dynamic authentication,

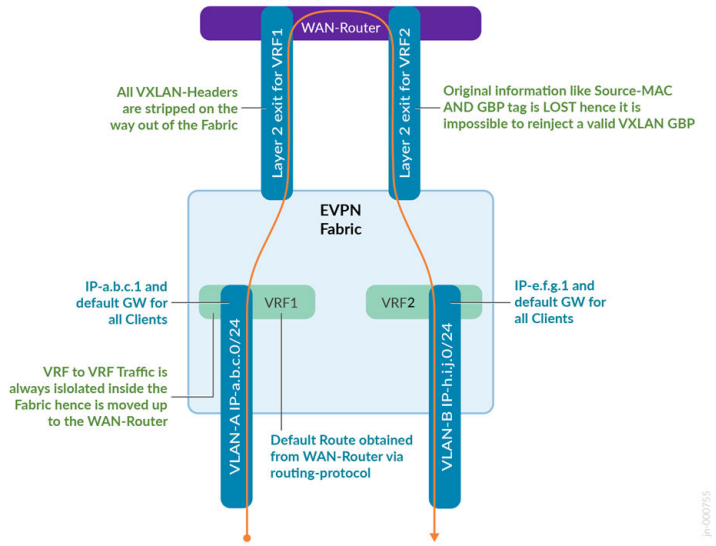
you must perform a second, MAC-based authentication on the fabric's access switch to get synchronized information about which GBP tag to assign. This is because the attached desktop switch does not share its RADIUS-based authorization information with the access switch.

No Support for VRF-to-VRF GBP Tag Distribution

The GBP tag distribution is limited to the VLANs inside the same VRF. This may be applicable if your network has a fabric with more than a single virtual routing and forwarding (VRF) instance. As shown in Figure 7 on page 14, VRF-to-VRF GBP tag distribution does not work due to the following technical reasons:

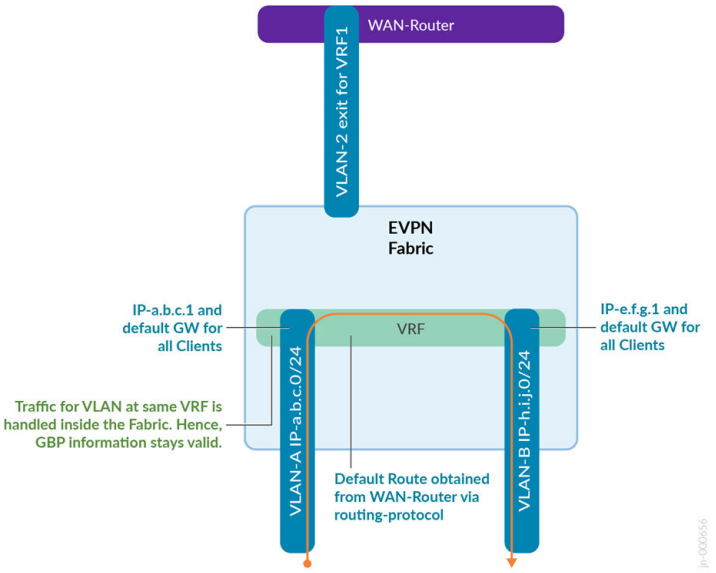
- All Juniper Mist-managed campus fabrics have isolation inside the fabric when traffic is passing between two VRFs. There is no route leaking between VRFs allowed inside the fabric itself for security reasons. Traffic between VRFs must always go south-to-north to the WAN router. The WAN router can then permit or forward the traffic between the VRFs and allow the traffic to flow back through the fabric to the destination VRF and VLAN.
- WAN routers are usually not part of the VXLAN layer of a fabric. They use either a:
  - Layer 2 configuration with VLANs and trunk ports and static routes between the fabric and the WAN router.
  - Layer 3 configuration with point-to-point links and a routing protocol such as OSPF or eBGP between the fabric and the WAN router.
- You encounter a similar situation as in EVPN multihoming of CRB and ERB fabrics mentioned above where traffic between stages uses a different environment and the on-hook information of the VXLAN tunnel gets lost between these stages. It is almost impossible to reconstruct the original information because when the packet gets back into the fabric towards the destination VRF, the original MAC address is lost.

Figure 7: GBP Does Not Work for Traffic Between VRFs



It's better to consider moving the VLANs into the same VRF in the fabric since such traffic will remain inside the fabric as east-west traffic and not be sent through the WAN router. In such a case, GBP-based management remains valid. See Figure 8 on page 14.

Figure 8: GBP Works in a Single-VRF Fabric



NOTE: A single global VRF is recommended to be used in this case. The usage of GBP then mitigates the need for multiple VRFs for security needs.

Known Junos OS Switch Firmware Notes

When **configuring GBP usage for the first time** on an access switch, you need to schedule a maintenance window before it gets activated and used. Junos OS requires a restart of the control plane to include this change:

- On a standalone switch, you could restart the Packet Forwarding Engine (PFE) to achieve the needed control plane restart for GBP inclusion.
- On a Virtual Chassis, you need to issue a complete reboot of the entire Virtual Chassis to achieve the needed control plane restart for GBP activation.

Known Hardware Restrictions

Juniper Networks® EX4100 Switches have the following documented limitations:

- Static interface/port and VLAN ID-based GBP tag assignments are not supported on the EX4100 Switch.
- Static VLAN ID-based GBP tag assignments are not possible on the EX4100 Switch. We suggest you use the IPv4 prefix of the VLAN to achieve similar functionality.

Known Campus Fabric Deployment Functionally

Depending on when you have built your campus fabric IP Clos, the following needs to be checked:

- If the campus fabric IP Clos was created after July 2024, you need to use Junos OS Release 24.2R2 or higher on the access switches for GBP. This is because a fabric created after this date automatically gets EVPN Type 2/5 coexistence configured for larger scale. The first Junos OS release version which supports EVPN Type 2/5 coexistence together with GBP is Junos OS Release 24.2R2.

Known Juniper Mist Portal Restrictions

In the current version, the Juniper Mist portal only supports the following static GBP tag assignments:

- IPv4 prefix-based static GBP tag assignments called **Subnets**.
- MAC address host-based static GBP tag assignments called **MAC Address**.
- VLAN ID-based static GBP tag assignments called **Network**.

Currently, you must use additional Junos OS CLI commands if you want to make use of:

- Switch port-based (interface-based) static GBP tag assignments
- Switch port-based (interface-based) and VLAN ID-based static GBP tag assignments.
- L4 match conditions for policies as documented here.
- Using a default deny option on all communication that does not have an explicit allow policy.

Wireless and Wired Client Segmentation Policies Use Different Sections in the Juniper Mist Portal

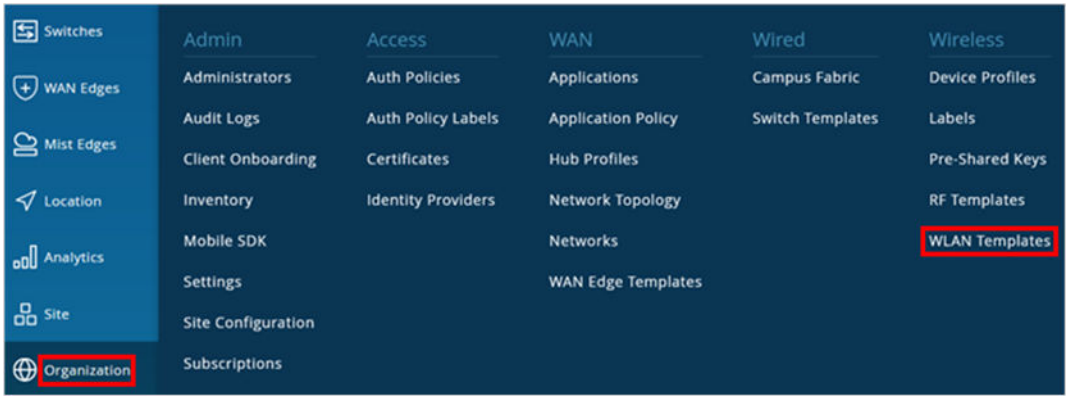
Currently, the microsegmentation of Juniper Mist-managed fabrics is achieved for wired and wireless clients in different sections of the Juniper Mist portal:

- GBP and SGT-based microsegmentation of wired clients should be configured on the **Organization > Switch Templates** page. See Figure 9 on page 16.

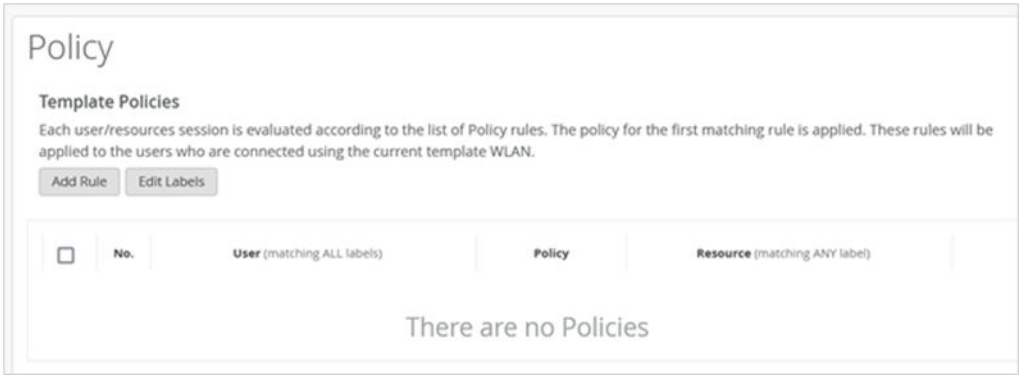
Figure 9: Switch Templates Location in the Juniper Mist Portal

- Policy configuration of microsegmentation for wireless clients should be configured on the **Organization > WLAN Templates** page. See Figure 10 on page 17.

Figure 10: WLAN Templates Location in the Juniper Mist Portal



After you create a new WLAN template, you can start to manage and configure the policies for wireless clients.



Test Objectives

IN THIS SECTION

The objective of the testing performed was to ensure that the features work as designed in the context of a Juniper Mist-managed IP Clos fabric. All configurations of the fabric itself, the GBP tag assignment, and the SGT policy configuration (with a few exceptions) must be performed through the Juniper Mist portal since this is the same as the end user experience. Dynamic GBP tag assignments were performed using a local, third-party RADIUS server and the Juniper Mist Access Assurance solution. Scale testing was also conducted.

Test Goals

The testing for this JVD was intended to achieve the following goals. Review the separate Test Report Brief for more information.

Goals for the tests performed:

- Test everything using ingress GBP enforcement. This is the default configuration of a Juniper Mist-managed fabric. No other options are available.
- Test all Juniper Mist portal static and dynamic GBP tag assignments:
  - IPv4 prefix-based, static GBP tag assignments called **Subnets**.
  - MAC address host-based, static GBP tag assignments called **MAC Address**.
  - VLAN ID-based, static GBP tag assignments called **Network**.
  - Dynamic GBP tag assignments for RADIUS authorization information.
- Limited testing using additional Junos OS CLI configuration was performed to test the following GBP tag assignments:
  - Switch port-based (interface-based) static GBP tag assignments.
- Dynamic GBP tag assignments for RADIUS authorization information utilizing different RADIUS servers:
  - A third-party RADIUS server local to the test bed.
  - Juniper Mist Access Assurance solution as a cloud-based authentication service.
  - MAC-based GBP tag assignments based on RADIUS authentication for both of the above servers.
  - 802.1X EAP-based GBP tag assignments based on RADIUS authentication for both of the above servers.
- Testing the hierarchy of static GBP tag assignments was performed within Layer 2 classifiers.
- Testing that a dynamic GBP tag assignment overrides a static GBP tag assignment was performed.

- Testing of wired clients towards wireless clients was performed when the APs directly breakout wireless client traffic at the AP. That traffic can then be identified at a trunk port of the access switch, where the AP is attached, via static assignments such as VLAN or IP address.
- Scale testing was performed, and the details are shared in the test report.
- A minimum of 3 GBP tags were used which allowed us to test different permutations of allowed and blocked traffic through SGT policy.
- Table 1 on page 19 shows the matrix that was used in respect to location of a wired client on an access switch.

Table 1: Wired Client Testing

Wired Client to Wired Client testing				
	Wired Client1	Wired Client2	Wired Client3	Wired Client4
Location on access switch	Located on a VC member	Same VC member as Client1 but different port	Different VC Member than Client1	Different switch than Client1
Same VLAN for all clients	GBP tag1	GBP tag1	GBP tag1	GBP tag1
Same VLAN for all clients	GBP tag1	GBP tag2	GBP tag2	GBP tag2
Same VLAN for all clients	GBP tag1	GBP tag3	GBP tag3	GBP tag3

NOTE: Review the separate Test Report for detailed information.

Test Non-Goals

The following tests were not performed for this JVD for various reasons:

- Testing without a fabric managed by Juniper Mist cloud was not a goal of this JVD. Even though it's possible to build a fabric based on Junos CLI commands without it being managed by the Juniper

Mist cloud, the goal was to utilize the Juniper Mist portal to manage the fabric and configure GBP tag assignments and SGT through the Juniper Mist portal.

- Testing with Juniper Apstra configuration management was not performed.
- Testing any other Juniper switches supporting VXLAN GBP such as EX4650, QFX5120-48Y, and QFX5120-32C was not performed since these switches are not supported in a Juniper Mist-managed fabric as access switches.
- Testing egress enforcement was not performed. The test cases focus on ingress enforcement since the Juniper Mist cloud uses this configuration as the default.
- Juniper Mist™ Edge integration testing was not performed. It will be added later.
- Testing with the new GBP Layer 4 static assignment features introduced in Junos OS Release 23.2R1 was not performed:
  - The current version of the Juniper Mist portal does not allow configuring the Layer 4 static GBP tag assignments, so this test would have required us to use the additional CLI function.
- Testing with more than one third-party RADIUS server vendor was not performed. It was assumed that if one third-party RADIUS server worked, all others should work as well. If any third-party RADIUS server vendor does not have a definition for the Juniper RADIUS dictionary, add a vendor-specific dictionary and use the Juniper vendor ID 2636. You must also configure the RADIUS authorization attribute “Juniper-switching-filter” value 48 as a string. Support for custom RADIUS dictionaries is a common thing with all production-grade RADIUS servers.

Recommendations

The following simple guidelines will help you to successfully implement a campus fabric using VXLAN-based GBPs in your network:

- Consider building and managing the fabric using the Juniper Mist portal as part of what is tested in this JVD.
- The only supported fabric type for VXLAN-based GBPs is IP Clos.
- The only supported switch types for access switches are the EX4400 and EX4100 Switches.
- When you intend to do static GBP tag assignments via VLAN ID, it is better to use the IP prefix of a VLAN since the IP prefix would also be recognized by EX4100 Switches.

- Dynamic assignments via third-party RADIUS servers should be easy to implement once you have configured the RADIUS dictionaries to support the vendor attribute “Juniper-switching-filter” with the right string value.
- If your wired clients are in different VRFs of the same fabric, consider configuring the segmentation in the WAN router for controlling the forwarding between the two VRFs.
- If you attach a desktop switch at the access switch then you may need to do a second authentication at the access switch before entering the fabric.
- Microsegmentation of wired and wireless clients is managed using the Juniper Mist portal but in different sections of the portal.
- Always use a switch template for all switches in the fabric to sync all changes you do in regards to GBP tag assignments and SGT Policies. Do not configure each switch individually. Switch templates help applying consistent policies across the network and any CRUD operations performed will be uniformly applied.
- When configuring GBP for the first time, you need to schedule a maintenance window for your access switches to restart the PFE for a standalone switch or a reboot of a Virtual Chassis before your GBP configuration gets activated.
- **All deployments must be done with Junos OS Release 24.2R2 or higher** as only this guarantee syncing between Layer 2 and Layer 3 GBP tag internal tables. Also check that the Juniper Mist fabric pushes the `set forwarding-options evpn-vxlan gbp mac-ip-inter-tagging` Junos OS command to each switch activating this sync. If this is missing, add it as an additional CLI command to your access switch template. Campus fabrics deployed after June 2024 also need Junos OS Release 24.2R2 since you need GBP support for EVPN Type 2/5 coexistence configured on the fabric.
- When using static classifiers, it is recommended to avoid overlapping assignments where different GBP tags can be assigned to the same client based on different classifiers. This avoids confusion on needing to know about tag hierarchy and when it takes place or not. You will find more information about the expected behaviour via this link.

Recommended installation and activation procedure for GBP in IP Clos campus fabrics.

1. Schedule a maintenance window for the entire fabric.
2. Download the recommended Junos OS Release (currently 24.2R2) to all standalone access and Virtual Chassis switches.
3. Reboot all standalone access and Virtual Chassis switches so that they have the recommended Junos OS release version running.
4. Using switch template:
    a. Have at least one initial GBP tag assignment created.

   b. Have at least one initial switch policy created.

   c. Save the template.

5. Juniper Mist cloud will then deploy the global tags and policy onto all access switches.

   a. Standalone switches will automatically reboot the PFE when the first GBP configuration is populated by Juniper Mist cloud.

   b. The Virtual Chassis will need to be rebooted manually in step 7.

6. Go to the access switches and check they all received the initial GBP configuration.

   a. Use a remote shell and use the CLI `show configuration | display set | match gbp` to review.

   b. Ensure that needed commands like `set forwarding-options evpn-vxlan gbp mac-ip-inter-tagging` are part of the configuration on each access switch.

7. Manually reboot all Virtual Chassis access switches now as they must have the GBP configuration when they start to reserve the needed resources.

8. After Virtual Chassis access switches are up again you can close the maintenance window of the campus fabric and start using it again.

9. You can now start to test GBP and change the GBP tag assignments and switch policy according to your needs.

   a. Make sure from now on you always have at least one GBP tag assignment and switch policy defined.

APPENDIX: Switch Template Configuration Examples

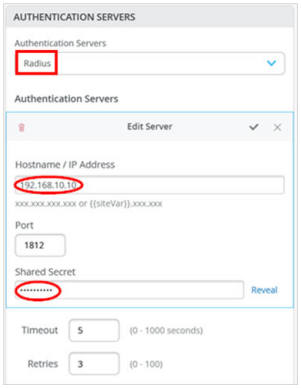
IN THIS SECTION

All configuration examples of this section are made in a switch template that is assigned to all switches. Switch templates can be configured via the **Organization > Switch Templates** tab of the Juniper Mist portal.

Third-Party RADIUS Server Configuration

At the beginning of the switch template, you can configure third-party RADIUS servers. The minimum items that must be configured are:

- Select Authentication Servers=`Radius`
- Add at least one new authentication server:
  - Configure the hostname or IP address through which this RADIUS server responds to requests.
  - Set a shared secret between the switch and the server to allow communication.



You must perform a similar process on the RADIUS server for each client. Configure the RADIUS server, the IP address of the client and the shared secret. Ensure you define the vendor-specific dictionary for the switch that acts as the RADIUS client.

Mist Authentication Configuration

There is not much to configure if you intend to use Juniper Mist Access Assurance:

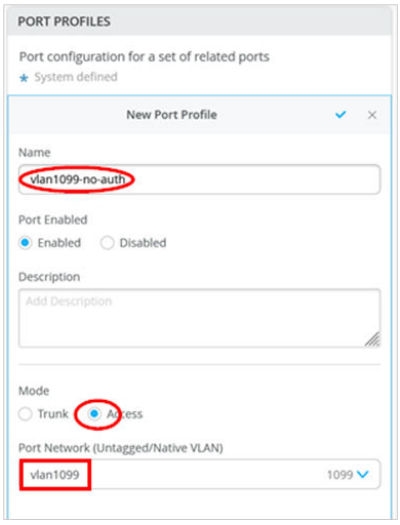
- Select as Authentication Servers=`Mist Auth`

Figure 11: Authentication Servers Configuration

Port Profiles Used for Testing

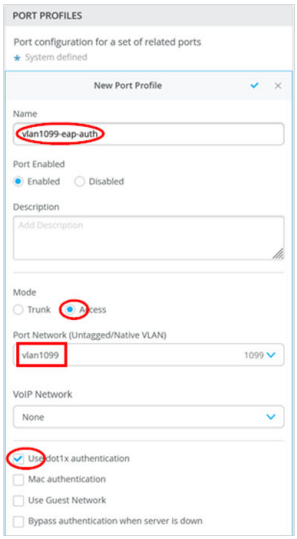
The following port profiles were used during testing:

- All static GBP tag assignments used one without any special authentication:
  - Port Profile Name=`vlan1099-no-auth`
  - Mode=`Access`
  - Port Network=`vlan1099`



- All dynamic GBP tag assignments with 802.1X supplicants used:

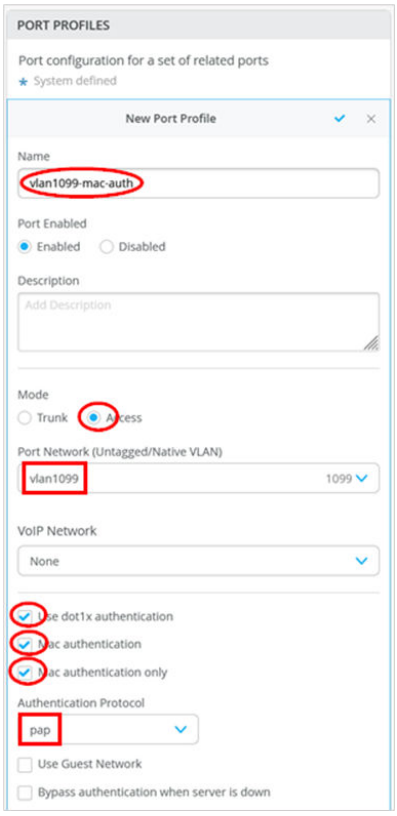
- Port Profile Name=`vlan1099-eap-auth`
- Mode=`Access`
- Port Network=`vlan1099`
- Use dot1x authentication=`Enabled`



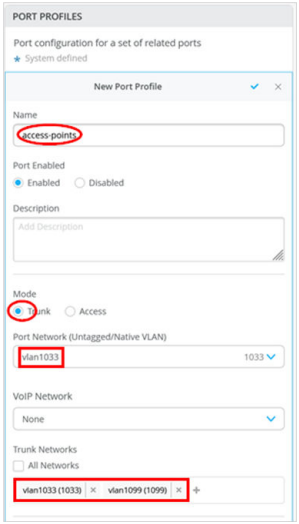
- All dynamic GBP tag assignments via MAC address used:
  - Port Profile Name=`vlan1099-mac-auth`
  - Mode=`access`
  - Port Network=vlan1099
  - Use dot1x authentication=`Enabled`
  - Mac authentication=`Enabled`
  - Mac authentication only=`Enabled`

    This prevents the switch from attempting an EAP-based authentication which would fail and cause 60 seconds of delay.
  - Authentication Protocol=`pap`

    This was easier to configure on the RADIUS server side.



- Finally, for the access point, we used the following port profile:
  - Port Profile Name=`access-points`
  - Mode=`Trunk`
  - Port Network=`vlan1033`
  - Trunk Networks=`vlan1033` and `vlan1099`



GBP Tag Assignments

We've used different GBP tag assignment configurations depending on the test cases.

Figure 12 on page 27 shows a list of GBP tag assignments that were used for testing the RADIUS servers with MAB and 802.1X clients.

Figure 12: Dynamic GBP Tags

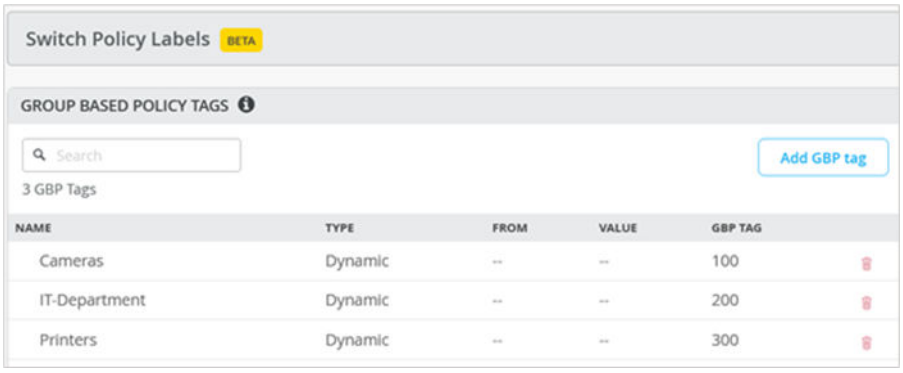
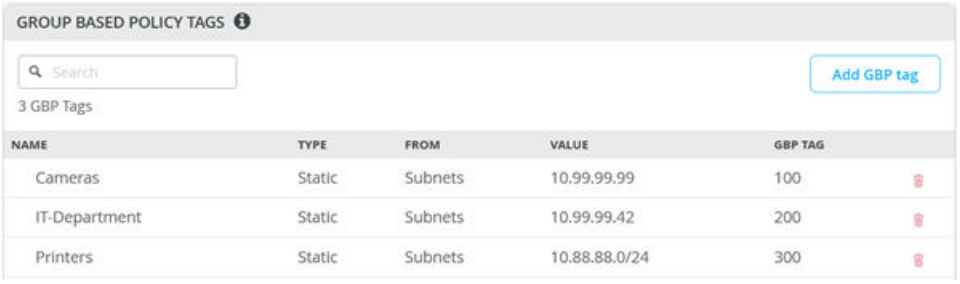


Figure 13 on page 27 shows a list of GBP tag assignments that were used for testing static, IP address-based assignments.

Figure 13: Static GBP Tags



- For the entire GBP tag assignment testing, more permutations of static assignments were used but we do not list them here.

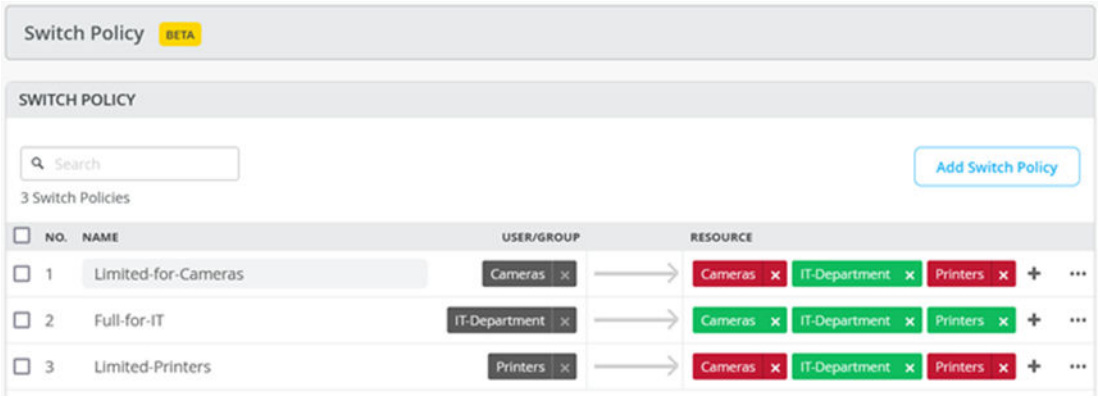
NOTE: If you use VLAN ID-based (network-based) assignments and the access switch is an EX4100 Switch which cannot utilize those features, the Juniper Mist cloud will automatically

filter out those invalid Junos OS commands, so they are not pushed to the switch. The remaining configuration stays intact as intended.

GBP Policy Assignments

Most of the time, the following matrix of SGT policy enforcements to block or allow traffic between GBP tags were used.

Figure 14: GBP Policy Assignments



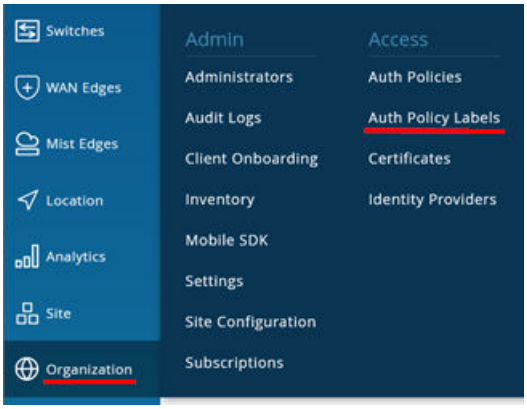
APPENDIX: Dynamic Client Authentication Using the Mist Authentication Cloud

IN THIS SECTION

In this section, we provide examples of how to authenticate wired clients using Juniper Mist Access Assurance and how you can repeat the testing performed in this JVD. First, ensure that your switch template uses “Mist Auth” in the authentication servers field as shown in Figure 11 on page 24.

Then, you must create the RADIUS **Authorization Policy Labels** on the **Organization > Auth Policy Labels** page.

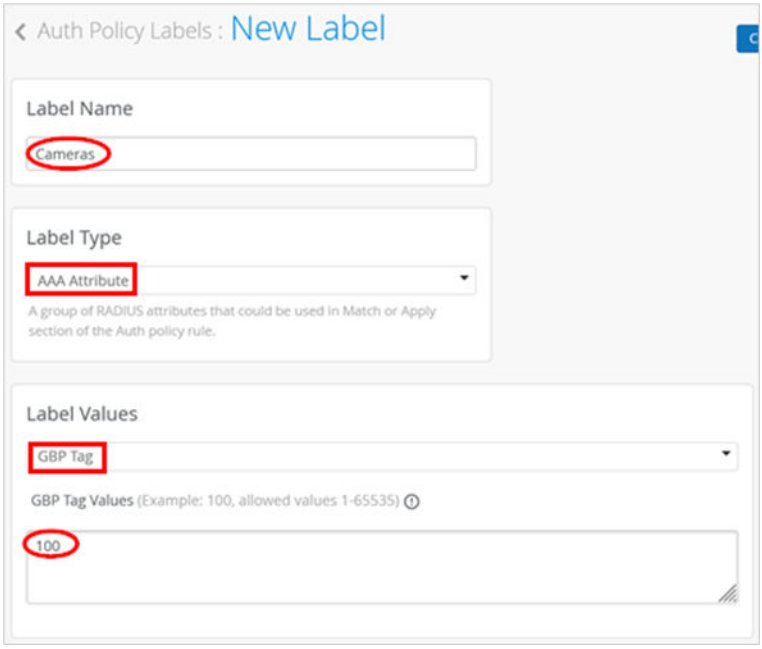
Figure 15: Authorization Policy Labels Location



Create labels for at least three GBP tags you want to assign:

- First, create the new auth policy label:
  - Label Name=`Cameras`
  - Label Type=`AAA Attribute`
    This is used to indicate it’s used as a RADIUS message.
  - Port Network=`GBP Tag`
  - GBP Tag Values=`100`

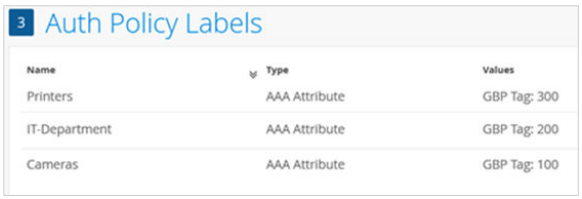
Figure 16: First New Auth Policy Label



- Second, create this new auth policy label:
  - Label Name=`IT-Department`
  - Label Type=`AAA Attribute`
  - Port Network=`GBP Tag`
  - GBP Tag Values=`200`
- Third, create this new auth policy label:
  - Label Name=`Printers`
  - Label Type=`AAA Attribute`
  - Port Network=`GBP Tag`
  - GBP Tag Values=`300`

The resulting configuration of all three labels should look like the list shown in Figure 17 on page 31.

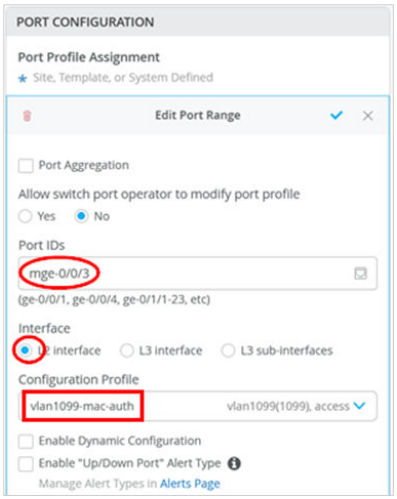
Figure 17: Auth Policy Labels



MAC Address-Based Client Authentication

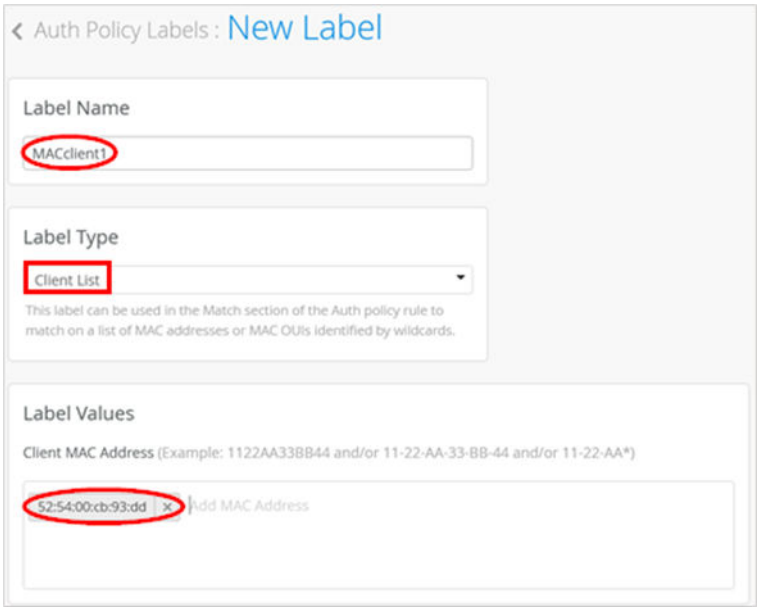
When you intend to use MAC address-based client authentication, ensure that the switch ports where your clients are attached use the right port profile. In our case, we used the port profile=”vlan1099-mac-auth” and configured the switch ports as shown in Figure 18 on page 31. Use port IDs appropriate for your environment.

Figure 18: Port Profile for MAC Address-Based Client Authentication



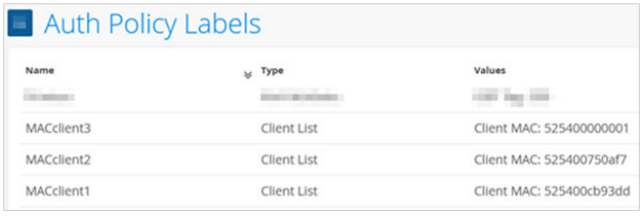
Next, create auth labels to identify the MAC addresses of your wired clients as shown in the following example:

- Create a new auth label:
  - Label Name=`MACclient1`
  - Label Type=`Client List` as this is used to validate MAC addresses.
  - Label Values=`<client1-MAC-Address>`



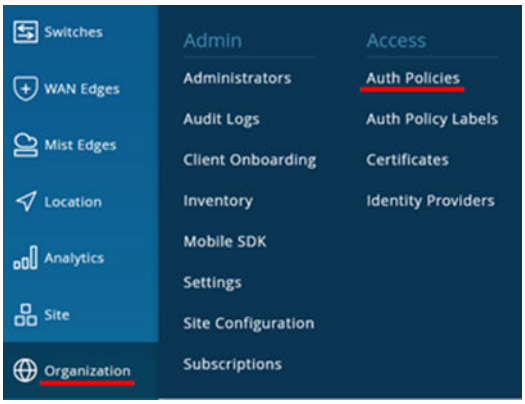
Create other auth labels based on the above example for at least 3 MAC address-based clients. An example of the result is shown in Figure 19 on page 32.

Figure 19: Example Auth Policy Label List



Next, you must create various authentication policies on the **Organization > Auth Policies** page.

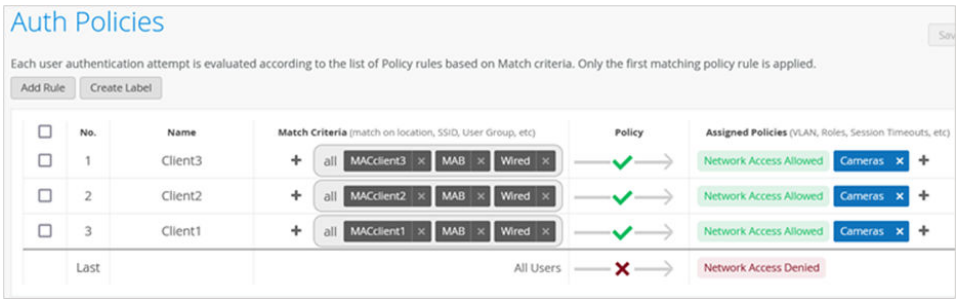
Figure 20: Authentication Policies Location



In the example below, we want every client to get GBP tag1 (our "Printers") assigned. Hence, the configuration looks like the following:

- Auth Policy for the first client:
  - Name=`Client1`
  - Match Criteria=`MACclient1` and `MAB` and `Wired`
  - Policy=`Pass`
  - Assigned Policies=`Network Access Allowed` and `Cameras`
- Auth Policy for the second client:
  - Name=`Client2`
  - Match Criteria=`MACclient2` and `MAB` and `Wired`
  - Policy=`Pass`
  - Assigned Policies=`Network Access Allowed` and `Cameras`
- Auth Policy for the third client:
  - Name=`Client3`
  - Match Criteria=`MACclient3` and `MAB` and `Wired`
  - Policy=`Pass`
  - Assigned Policies=`Network Access Allowed` and `Cameras`

Figure 21: Example Auth Policies List



We have chosen to define one authentication policy per client because you can change the assigned policy for each client individually to assign and test with a different GBP tag.

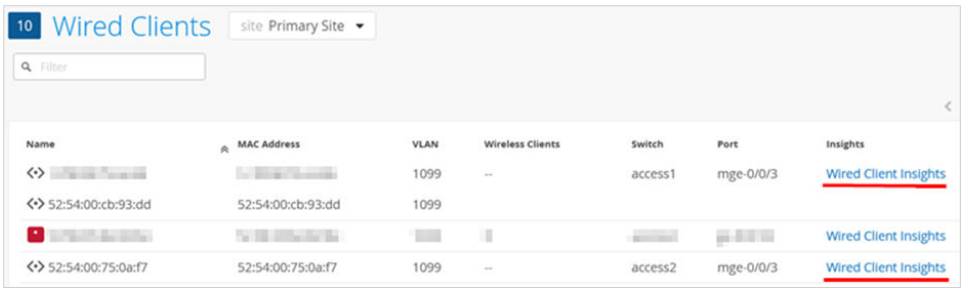
NOTE: When testing dynamic, MAC address-based authentication, there is a default time of 10 minutes before a re-authentication happens. When you change labels to test other combinations, 10 minutes might be too long to wait. In a lab situation, you can use the additional Junos OS CLI feature to shorten the reauthentication period. For example, to set a 60 second reauthentication period, use the following additional Junos OS CLI: `set protocols dot1x authenticator interface vlan1099-mac-auth reauthentication 60`.

After your clients are authenticated by Juniper Mist Access Assurance, you can check the GBP tag assignment. To do so, navigate to **Clients > Wired Clients** in the Juniper Mist portal.

Figure 22: Wired Clients Location

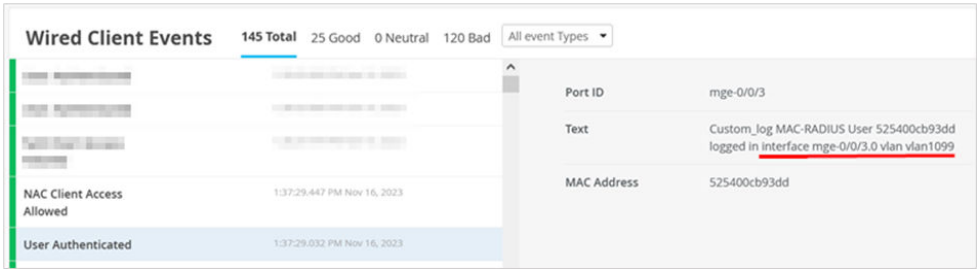
Identify the wired clients you have configured and click on **Wired Client Insights**.

Figure 23: Wired Client List



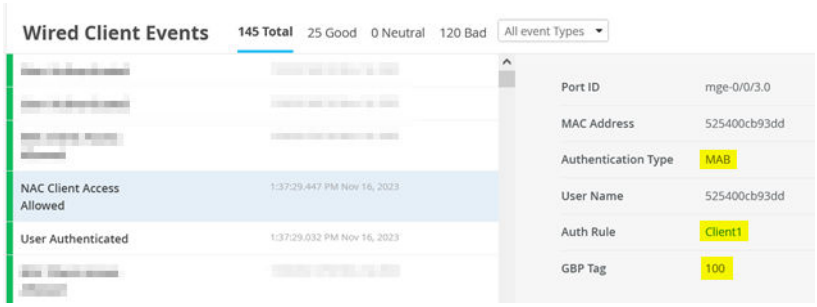
Below is an example of the first client events report. You can see which interface the new client connected through:

Figure 24: Wired Client Events List – User Authentication



The second event you would typically see is the NAC authentication itself. Below, you can see the authentication type, the Auth Rule that was found valid to be used and the final GBP tag that was applied as part of the dynamic authentication:

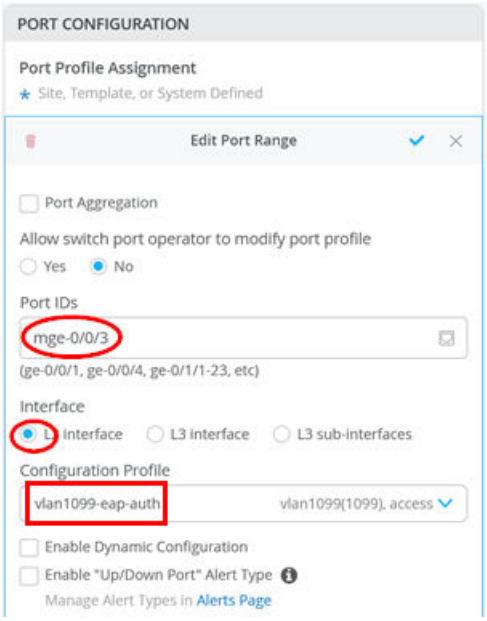
Figure 25: Wired Client Events List – NAC Client Access Allowed



IEEE 802.1X-Based Client Authentication

When you intend to use IEEE 802.1X-based client authentication ensure that the switch ports where your clients are attached use the correct port profile. In our case, we used the port profile, "vlan1099-eap-auth" and configured the switch ports as shown in the example below. Use port IDs appropriate for your environment.

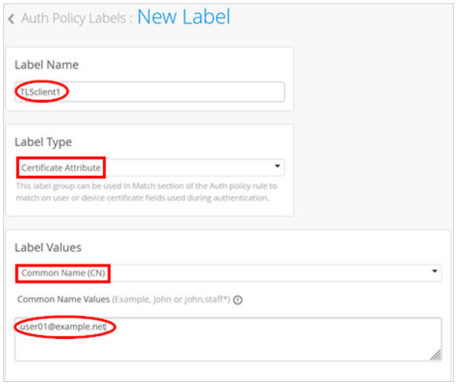
Figure 26: Port Configuration for 802.1x-Based Client Authentication



When testing, we wanted to be able to identify a minimum of three clients individually to be able to assign them different GBP tags dynamically. The approach chosen was to use EAP-TLS and determine the individual client by attributes of their client certificates stored on each supplicant. Which values you choose depends on the enterprise PKI you intend to use. In our case, we knew that each client has a different name in the Common Name attribute of the supplicant certificate. Hence, we used this field to create three client labels as shown in the example below:

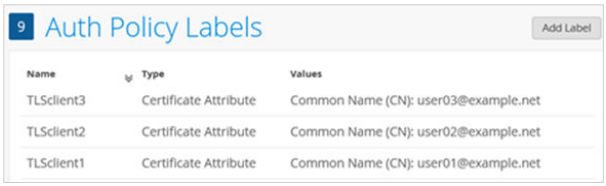
- Create a new authentication policy label by navigating to **Organization > Auth Label** and configuring the fields as shown in the following list:
  - Label Name=`TLSclient1`
  - Label Type=`Certificate Attribute`
  - Label Values=`Common Name (CN)`
  - Common Names Values=`user01@example.net`

Figure 27: Example Auth Policy Label for EAP-TLS Authentication

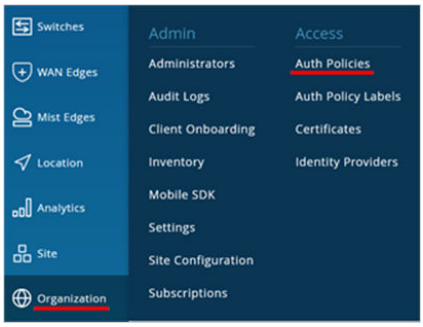


- Create other labels based on the example above for at least three TLS clients as shown in Figure 28 on page 37.

Figure 28: Example EAP-TLS Authentication Policy Label List



Next, create various authentication policies on the **Organization > Auth Policies** page:

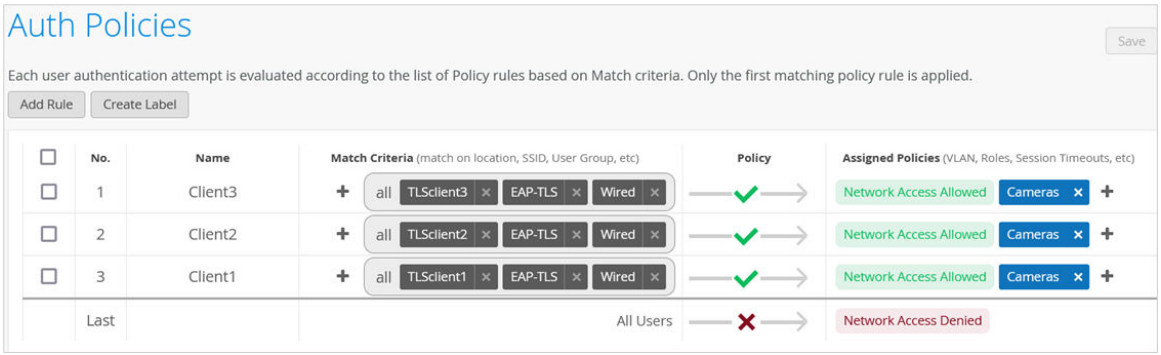


In the example below, we want every client to have the GBP tag1 (our `Printers`) assigned. Hence, the configuration looks like the following:

- Auth policy for the first client:
  - Name=`Client1`
  - Match Criteria=`TLSclient1` and `EAP-TLS` and `Wired`
  - Policy=`Pass`

    - Assigned Policies=`Network Access Allowed` and `Cameras`
- Auth policy for the second client:
    - Name=`Client2`
    - Match Criteria=`TLSclient2` and `EAP-TLS` and `Wired`
    - Policy=`Pass`
    - Assigned Policies=`Network Access Allowed` and `Cameras`
- Auth policy for the third client:
    - Name=`Client3`
    - Match Criteria=`TLSclient3` and `EAP-TLS` and `Wired`
    - Policy=`Pass`
    - Assigned Policies=`Network Access Allowed` and `Cameras`

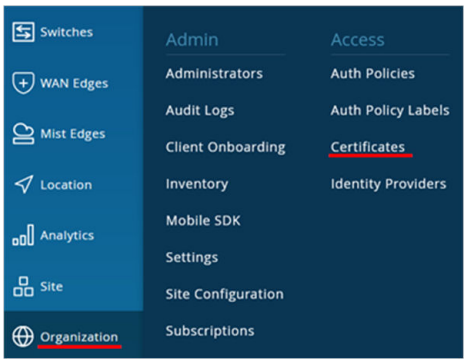
Figure 29: Example EAP-TLS Authentication Policies List



At this point, if not already done, you must configure your enterprise PKI for the Juniper Mist authentication cloud:

- Navigate to **Organization > Certificates**

Figure 30: Certificates Location in Mist GUI

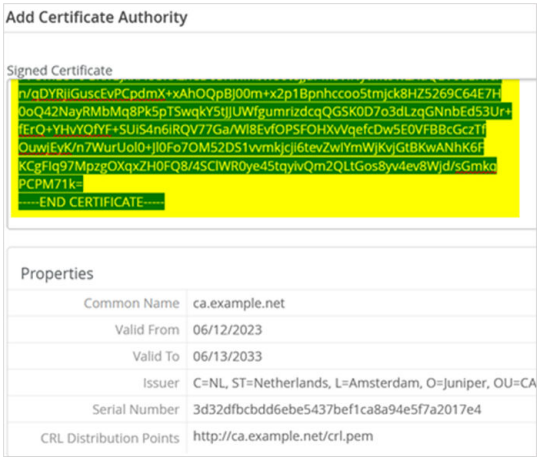


- Click on the **Add Certificate Authority** button as shown in Figure 31 on page 39.

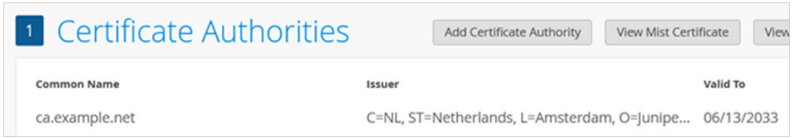
Figure 31: Add Certificate Authority

- Paste the base64-encoded part of your enterprise PKI root CA in the **Signed Certificate** window.

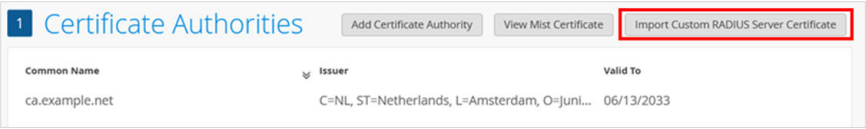
Figure 32: Signed Certificate Window



The result should look like this:

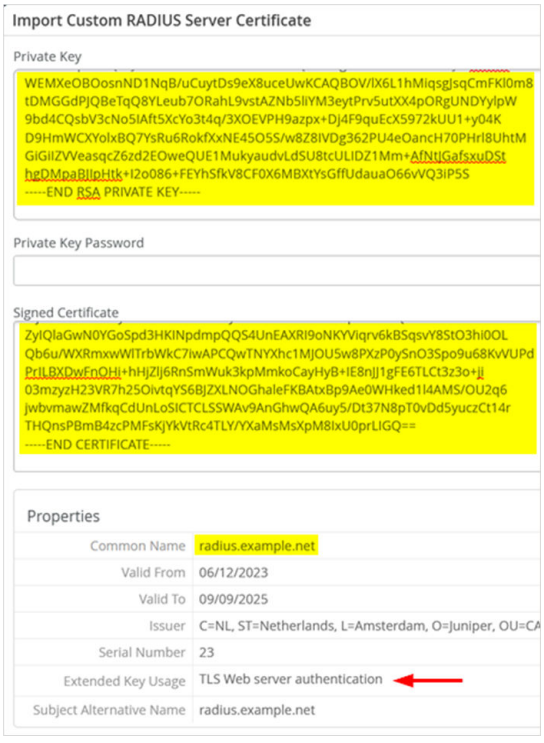


- Now, click on **Import Custom RADIUS Server Certificate**:

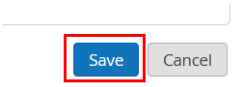


- Apply the following configuration:
  - Paste the content of the base64-encoded part of your enterprise PKI RADIUS server certificate key into the **Private Key** field.
  - Depending on your enterprise PKI, your RADIUS server certificate may need a password to open the encrypted key. If that is the case, provide this information here.
  - Paste the content of the base64-encoded part of your enterprise PKI RADIUS server public certificate into the **Signed Certificate** field.
- Confirm the information in the populated property fields:
  - The common name should be a DNS FQDN.
  - Extended Key Usage=**TLS Web server authentication**

Figure 33: Example of Filled-in Import Custom RADIUS Server Certificate Fields



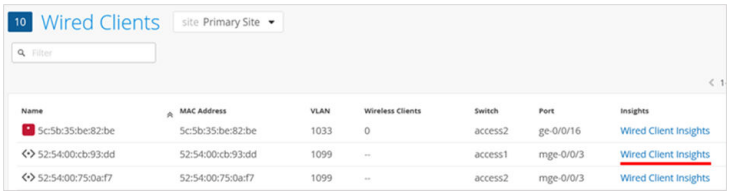
- Click **Save**.



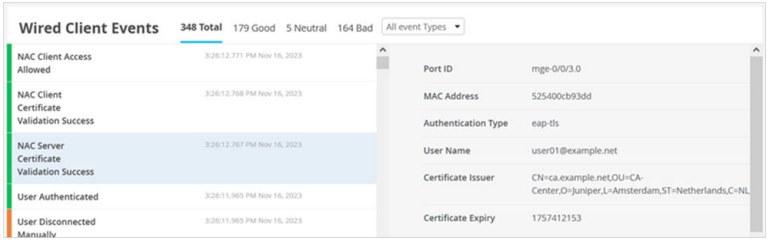
Now, you can start to authenticate your EAP-TLS clients.

After your clients are authenticated by Juniper Mist Access Assurance, you can check the GBP tag assignment. To do this, navigate to **Clients > Wired Clients**.

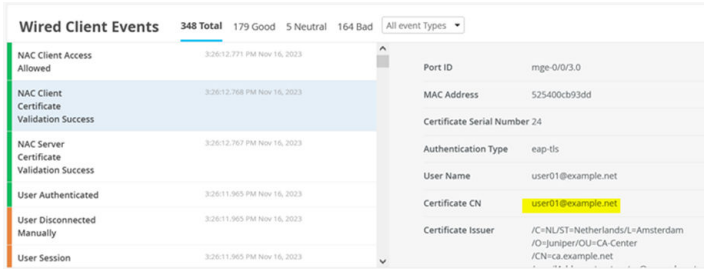
Identify the wired client you have configured and click on **Wired Client Insights**:



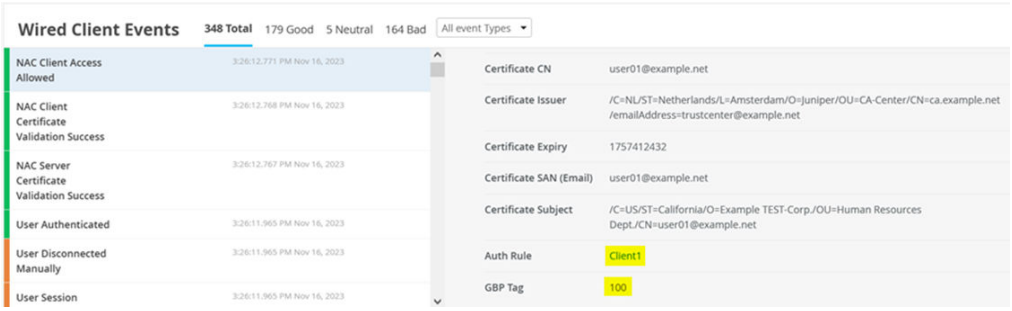
First, check the certificate of the RADIUS server:



Next, you see the information about the client certificate from the supplicant that the RADIUS server checked for validation. Here, it is important to review the certificate attributes because we use them to identify a single client.



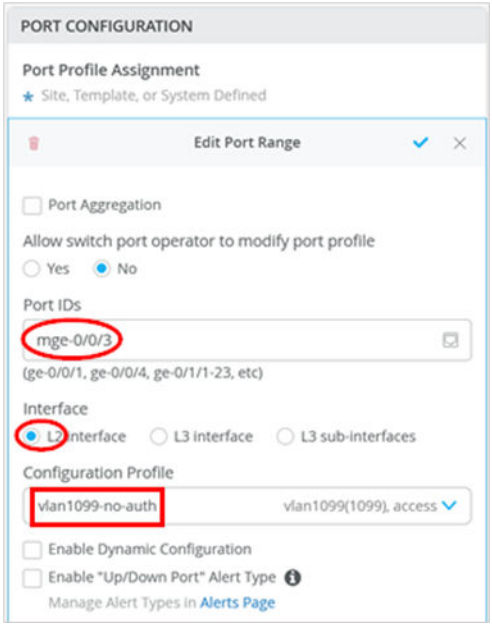
Then, you see the decision of the NAC system to allow network access for this client and which rule allowed it. The GBP tag assigned can also be reviewed:



APPENDIX: Static Client Assignments

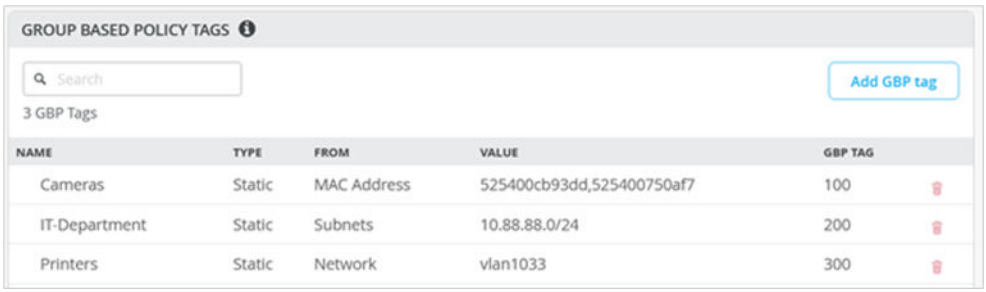
When you intend to use static GBP tag assignments, ensure that the switch ports where your clients are attached use the correct port profile. In our case, we used the port profile=`vlan1099-no-auth` (because we do not want any dynamic RADIUS assignment) and configured the switch ports as shown in the example below. Use port IDs appropriate for your environment.

Figure 34: Switch Port Configuration for Static GBP tag Assignment



Instead of a dynamic GBP tag assignment you must now modify the switch template to use static assignments. Here is an example of the configuration used during testing.

Figure 35: Example of Static GBP Tags List

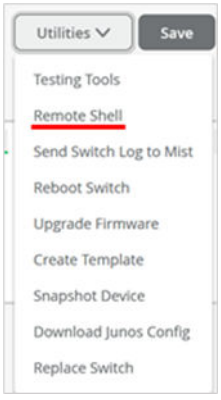


NOTE: Ensure your wireless clients really produce some traffic on the network. For example, Linux clients tend to be rather quiet, meaning you won't be able to see the GBP tag appear.

APPENDIX: Debugging Examples Using the Junos OS CLI

If you are familiar with the Junos OS CLI, you can utilize the commands shown below when checking something locally on a switch. The Juniper Mist portal can open a remote shell to each switch it manages as shown in Figure 36 on page 43.

Figure 36: Switch Management Utilities in the Juniper Mist Portal



Below is an example of a successful dynamic authentication using a MAB Auth-capable RADIUS server. You can see the dynamic filter attribute set the GBP tag to 300.

```
root@access1> show dot1x interface mge-0/0/3
802.1X Information:
Interface     Role           State           MAC address          User
mge-0/0/3.0   Authenticator  Authenticated   52:54:00:CB:93:DD    525400cb93dd

root@access1> show dot1x interface mge-0/0/3 detail
mge-0/0/3.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Enabled
  Mac Radius Authentication Protocol: PAP
  Reauthentication: Enabled
  Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: not configured
  Number of connected supplicants: 1
    Supplicant: 525400cb93dd, 52:54:00:CB:93:DD
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Mac Radius
      Authenticated VLAN: vlan1099
      Dynamic Filter: apply action gbp-tag 300
      Session Reauth interval: 3600 seconds
      Reauthentication due in 2595 seconds
      Session Accounting Interim  Interval: 36000 seconds
      Accounting Update  due in 34995 seconds
      Eapol-Block: Not In Effect
      Domain: Data
```

Next, review the MAC table of the local switch. For example:

- The dynamically learned MAC address `52:54:00:75:0a:f7` is reported as being reachable by remote VTEP and having the GBP tag 300 assigned.
- The dynamically learned MAC address `52:54:00:cb:93:dd` is reported as being reachable locally on interface mge-0/0/3.0 with the GBP tag 300 assigned.

```
root@access1> show ethernet-switching table
MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent static
           SE - statistics enabled, NM - non configured MAC, R - remote PE MAC, O - ovsdb MAC)
Ethernet switching table : 4 entries, 4 learned
Routing instance : default-switch
   Vlan                MAC                 MAC       GBP    Logical
SVLBNH/      Active
   name                address             flags     tag    interface              VENH
Index   source
   vlan1033            5c:5b:35:be:82:be   DR
vtep.32771                          172.16.254.5
   vlan1033            d4:20:b0:01:46:09   D                ge-0/0/16.0
   vlan1099            52:54:00:75:0a:f7   DR         300
vtep.32771                          172.16.254.5
   vlan1099            52:54:00:cb:93:dd   D          300   mge-0/0/3.0
```

NOTE: The Junos OS CLI

```
show ethernet-switching
mac-ip-table
```

will allow you to review GBP tag assignments in case of static IPv4/6 Prefix assignments. Both Tables are automatically synced as per configuration.

Below is an example of the Junos OS configuration for dynamically authenticated clients we used while testing:

```
set groups top firewall family any filter gbp_Limited-for-Cameras term 01 from gbp-src-tag 100
set groups top firewall family any filter gbp_Limited-for-Cameras term 01 from gbp-dst-tag 100
set groups top firewall family any filter gbp_Limited-for-Cameras term 01 then discard
set groups top firewall family any filter gbp_Limited-for-Cameras term 02 from gbp-src-tag 100
set groups top firewall family any filter gbp_Limited-for-Cameras term 02 from gbp-dst-tag 200
set groups top firewall family any filter gbp_Limited-for-Cameras term 02 then accept
```

```
set groups top firewall family any filter gbp_Limited-for-Cameras term 03 from gbp-src-tag 100
set groups top firewall family any filter gbp_Limited-for-Cameras term 03 from gbp-dst-tag 300
set groups top firewall family any filter gbp_Limited-for-Cameras term 03 then discard
set groups top firewall family any filter gbp_Full-for-IT term 01 from gbp-src-tag 200
set groups top firewall family any filter gbp_Full-for-IT term 01 from gbp-dst-tag 100
set groups top firewall family any filter gbp_Full-for-IT term 01 then accept
set groups top firewall family any filter gbp_Full-for-IT term 02 from gbp-src-tag 200
set groups top firewall family any filter gbp_Full-for-IT term 02 from gbp-dst-tag 200
set groups top firewall family any filter gbp_Full-for-IT term 02 then accept
set groups top firewall family any filter gbp_Full-for-IT term 03 from gbp-src-tag 200
set groups top firewall family any filter gbp_Full-for-IT term 03 from gbp-dst-tag 300
set groups top firewall family any filter gbp_Full-for-IT term 03 then accept
set groups top firewall family any filter gbp_Limited-Printers term 01 from gbp-src-tag 300
set groups top firewall family any filter gbp_Limited-Printers term 01 from gbp-dst-tag 100
set groups top firewall family any filter gbp_Limited-Printers term 01 then discard
set groups top firewall family any filter gbp_Limited-Printers term 02 from gbp-src-tag 300
set groups top firewall family any filter gbp_Limited-Printers term 02 from gbp-dst-tag 200
set groups top firewall family any filter gbp_Limited-Printers term 02 then accept
set groups top firewall family any filter gbp_Limited-Printers term 03 from gbp-src-tag 300
set groups top firewall family any filter gbp_Limited-Printers term 03 from gbp-dst-tag 300
set groups top firewall family any filter gbp_Limited-Printers term 03 then discard
set groups top forwarding-options evpn-vxlan gbp ingress-enforcement
set groups top forwarding-options evpn-vxlan gbp mac-ip-inter-tagging
set groups top chassis forwarding-options vxlan-gbp-profile
```

Revision History

Table 2: Revision History

Date	Version	Description
March 2025	JVD-IPCLOS-GBP-01-01	Initial publish