Cisco Unified Branch

Small Branch

October 2025

Introduction

In most industries, branch offices require continuous operations, strong future-proof security, and excellent customer experience, even as IT teams face resource constraints. Operational complexity continues to be a main challenge along with rising security vulnerabilities. In addition to rising security threats, there is a need to address the challenges of increased network traffic and critical uptime requirements due to increased AI and IoT initiatives.

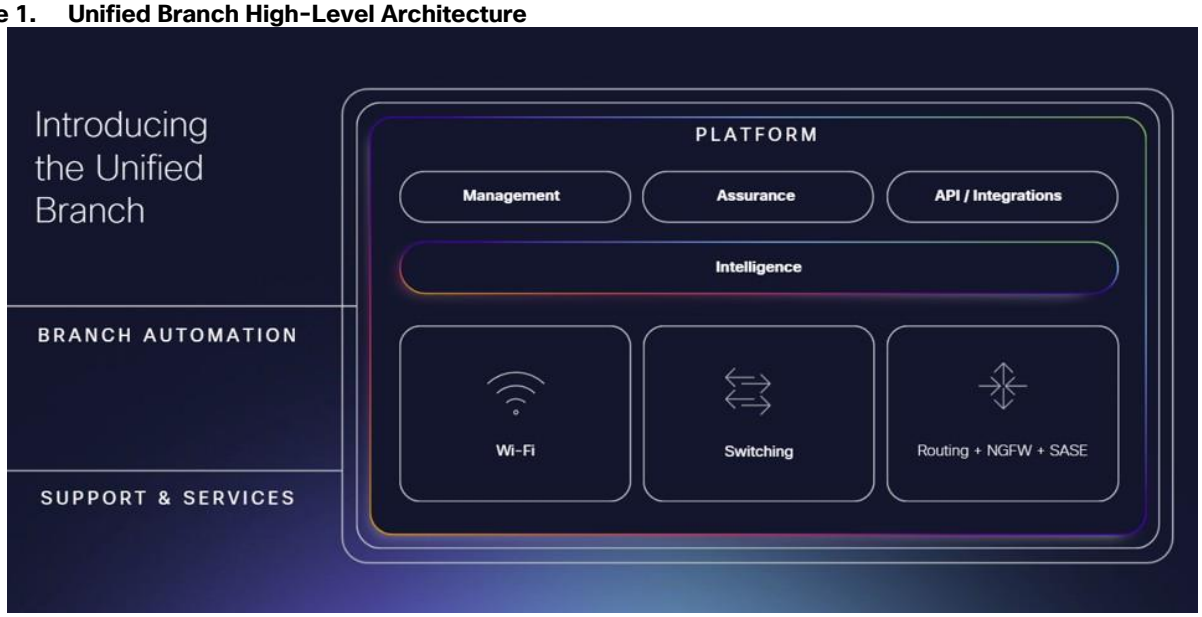
The Cisco full-stack Unified Branch solution was designed to make branch deployments faster, simpler, highly scalable, and easier to maintain. Unified Branch provides a set of products that are tested and verified together, uniting routing, next-generation firewall capabilities, Wi-Fi, IoT, and switching, all managed by a single, unified dashboard.

Security is incorporated as a core component fused into the network and embedded on multiple devices and multiple network layers. Security functionality includes next-gen firewall, identity services, and zero trust segmentation, as well as future post-quantum cryptography safeguards. Through Cisco Extended Detection and Response (XDR), security operations are simplified and enhanced through detecting, prioritizing, and remediating threats more efficiently

Cisco's unified management platform offers network visibility and detailed path and performance metrics through ThousandEyes. Also, with the addition of AgenticOps—Cisco's AI-driven operations powered by deep expertise—the platform helps IT teams automate and manage their networks more intelligently and efficiently. Using Cisco AI Canvas and Cisco AI Assistant, these capabilities enable AI-driven monitoring, troubleshooting, and remediation.

Branch as Code is an approach that applies Infrastructure as Code (IaC) principles to branch network deployment and management. It transforms branch network management and allows enterprises to deploy, manage, and scale branch infrastructure with agility, consistency, and confidence by leveraging Cisco's validated designs and automation frameworks. Cisco Workflows can also be used for network deployment and management. It is a powerful, flexible automation solution to help users streamline operations by automating a wide variety of tasks.

Figure 1. Unified Branch High-Level Architecture



About This Guide

The Unified Branch architecture, with supported platforms and a variety of use cases, is being developed, tested, and released in phases. In Phase I, the design is Meraki-based, supporting multiple flavors of MX, Catalyst switches, and access points at the branch using the Meraki cloud dashboard for management, and Auto VPN for the SD-WAN overlay. The Catalyst switches must run in cloud mode (not device mode), meaning they must be managed and configured only from the Meraki dashboard.

This guide provides an overview of the Unified Branch Architecture in release I, which includes a single network design for small branch sites, discussing the hardware, services, and features supported. It also includes the configuration choices for the Unified Branch design. An example small branch deployment is then presented, along with step-by-step instructions to deploy it using the Meraki dashboard.

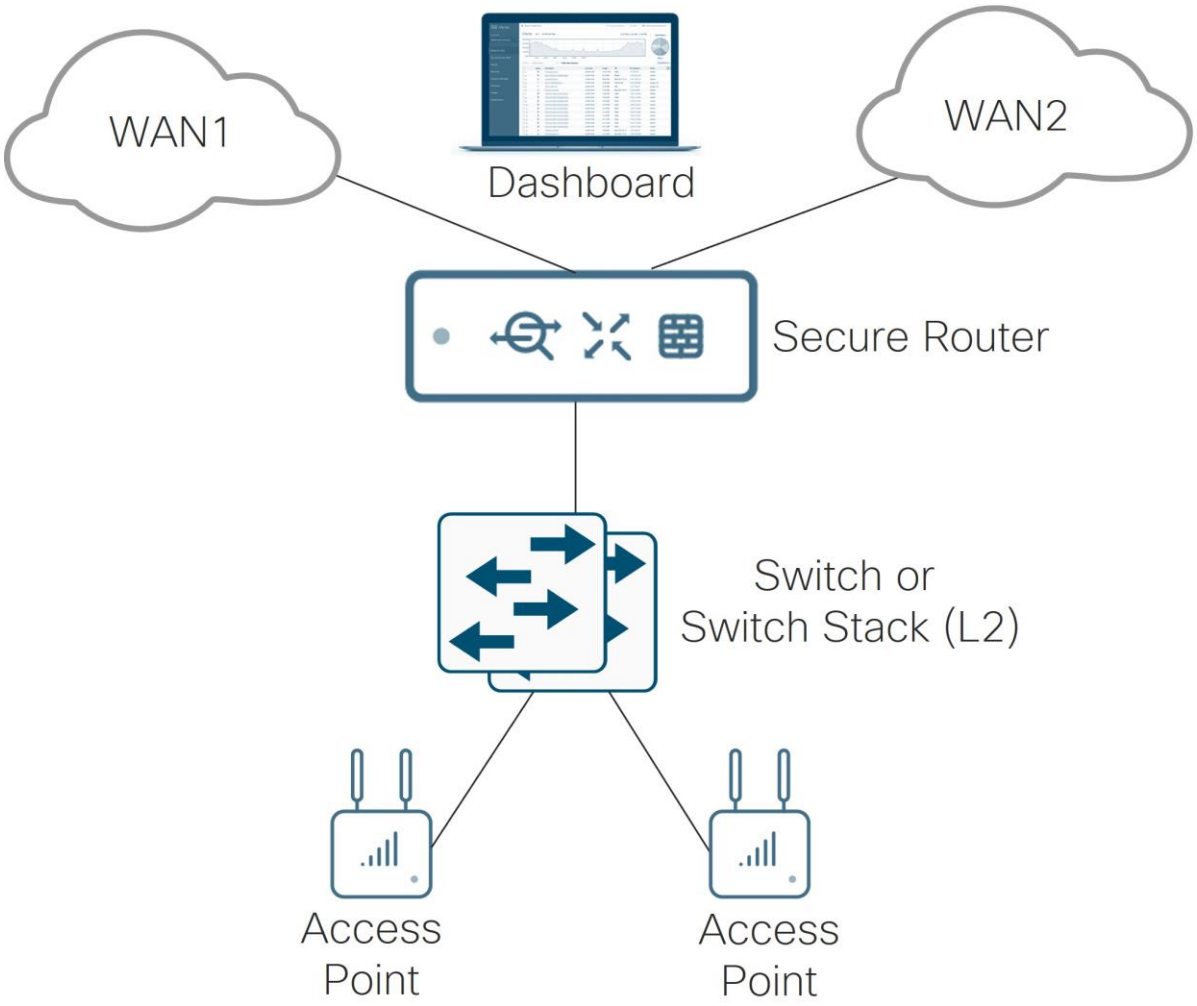
This guide does not cover Branch as Code or Cisco Workflows, as they will be covered separately.

Unified Branch Components

Refer to the following diagram as a reference for Unified Branch Release I, which highlights the small branch. At the branch, there is one secure router, one layer 2 switch or switch stack, and one or more access points managed by the Meraki dashboard in the cloud and accommodating both wired and wireless users, voice, and video. The secure router has 2 active WAN transports, both which have connectivity to the dashboard. It also terminates L3 connectivity for several groups of users at the branch. The group of users are segmented at the switch layer by VLANs, and the VLANs are trunked from the switch to the router. IPv4 is supported in this first release.

Note that the MX devices are often referred to as security appliances in documentation and the dashboard. In this document, they are referred to as routers or secure routers.

Figure 2. Unified Branch Architecture – Small Branch



The following hardware components are part of the release I architecture. For the Catalyst switches (C9200/L, C9300/X/L), they must be able to run in cloud mode for full Meraki dashboard-delivered management. Cloud mode delivers a complete cloud management experience, supporting UI or API-driven configuration and optional, read-only CLI.

The Catalyst 9200/9300 switches can optionally be ordered with a SKU ending in -M. These models arrive in cloud mode and can be immediately onboarded to the dashboard. Any non-M versions need to be

migrated to cloud mode. Cloud native IOS XE 17.15 and 17.18 have now been released, and cloud native images are the release of choice for cloud mode Catalyst devices moving forward. See Cloud Management with IOS XE Overview for more detailed information on SKU support, minimum versions for cloud management, and migration.

Note: The software minimum in the table below reflects the minimum software tested for Unified Branch Release I. The recommendation is to use the latest stable release version for each platform.

Component	Model Family	Software Minimum	License(s)**
Secure Router	*MX67/MX68/MX85/MX95/MX105	MX 18	Advantage Subscription
Access Switch	C9300/X/L (-M versions)	CS 17/IOS XE 17.15 or 17.18 depending on the model	Advantage Subscription
Access Switch	C9200/L (-M versions)	IOS XE 17.15 or 17.18, depending on the model	Advantage Subscription
Access Switch	MS150/MS130	MS 17.1.4	Advantage Subscription
Wireless LAN Access Points	AP CW9172 AP CW9176	MR 31	Advantage Subscription

*Base MX67/MX68 (non-W/CW versions)

**For more information on subscription licensing, refer to Subscription – Licensing Overview.

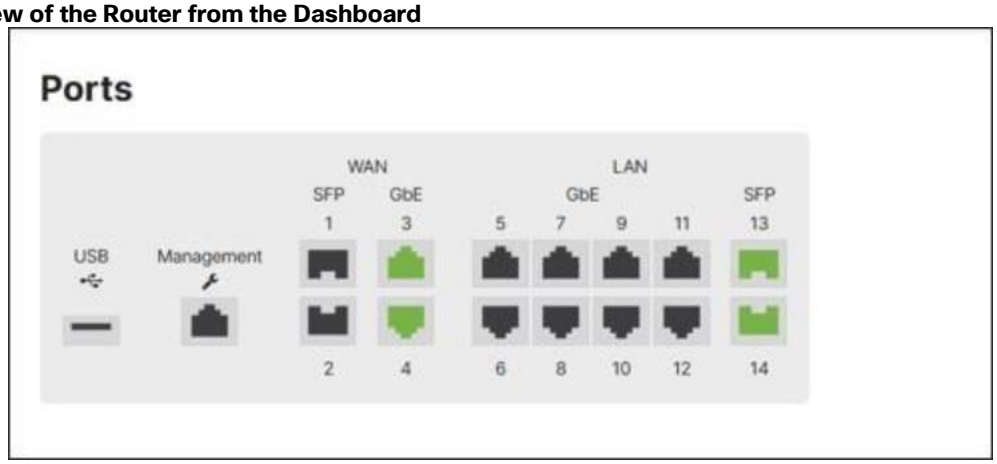
Check each model family's data sheet in the table above for stack cabling SKUs for switch stacking use cases.

The network devices require onboarding to the dashboard to be properly managed. Before attempting to onboard a device to the dashboard, ensure all the dashboard pre-requisites are met. This includes claiming devices, adding licenses, and configuring networks. Refer to the Getting Started Checklist for additional information.

Unified Branch Secure Router

Unified Branch Release 1 supports an MX67, MX68, MX85, MX95, or MX105 secure router. Check the individual datasheets in the table above for information for specifics on interface types, performance capabilities, physical characteristics, power requirements, Power over Ethernet (PoE) capabilities, etc.

Figure 3. View of the Router from the Dashboard



Deployment Mode

The secure WAN router can be deployed in either Routed (default) or Passthrough/VPN Concentrator mode. For this design, routed mode is enabled for the branch router.

In routed mode, the WAN router acts as a layer 3 gateway for subnets configured on the LAN side, and routes encrypted traffic over the auto VPN overlay to other sites or Internet traffic out the WAN uplinks to the Internet. Client traffic to the Internet is translated using NAT overload so its source IP address is the uplink IP address of the WAN router uplink. This mode is best if layer 3 networking capabilities are required and the WAN router is connecting directly to your Internet demarcation point with a public IP address issued by the Service Provider. Routed mode is the most common branch deployment model.

WAN Connectivity

The MX67/68 has 2 ports that can be used for WAN connectivity. The MX68 has 2 dedicated WAN ports and the M67 has one dedicated WAN port, but port 2 (LAN port) can be converted to a WAN port for the second uplink.

Secure Router	WAN Interfaces	Port Numbers
MX67	1x dedicated 1 Gigabit Ethernet RJ45 1x convertible 1 Gigabit Ethernet RJ45 (LAN/WAN)	Port 1 Port 2
MX68	2x dedicated 1 Gigabit Ethernet RJ45	Ports 1-2

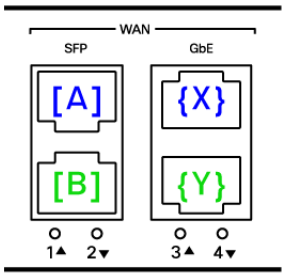
The MX85/95/105 has 4 total possible ports that can be used for WAN connectivity, which are represented in the following table.

Secure Router	WAN Interfaces	Port Pairing
MX85	2x dedicated 1 Gigabit Ethernet SFP 2x dedicated 1 Gigabit Ethernet RJ45	Port 1 (SFP) – Port 3 (RJ45) Port 2 (SFP) – Port 4 (RJ45)
MX95/MX105	2x dedicated 10 Gigabit Ethernet SFP+ 2x dedicated 2.5 Gigabit Ethernet RJ45	Port 1 (SFP) – Port 3 (RJ45) Port 2 (SFP) – Port 4 (RJ45)

The MX in release I has two active uplink (WAN) interfaces. If an SFP is detected at device boot for port 1 or 2, then that port is enabled, and its RJ45 port pair partner is disabled (port 3 or 4). If an SFP is not detected at device boot for port 1 or 2, then that port is disabled, and its RJ45 port pair partner is enabled

(port 3 or 4). Port preference is retained until the next boot, even if an SFP is removed during device operation. Port selection can also be configured through the device's local status page and not through the main dashboard.

Figure 4. SFP/RJ45 Port Pairs on MX85/95/105



Port 4 on each model supports PoE+, which could be used to support any WAN gateway device, such as a cellular gateway, or satellite or cable modem. For more information, see the WAN Behavior on MX75/85/95/105 document.

Device Onboarding

By default, the MX WAN ports are set to receive their IP address, IP gateway, and DNS information through DHCP from the WAN Service Provider (SP). Once this information is obtained, the router can connect to the dashboard on the Internet for software upgrade, monitoring, and configuration. The WAN interface parameters (static IP address and mask, gateway IP address, and primary/secondary DNS) can also be configured through the device's local status page if needed for connectivity to the provider. These parameters can also be changed through the dashboard once the device is connected.

WAN Uplink Dashboard Reachability Preference

By default, the first WAN interface on the MX router is chosen as the primary WAN interface to establish connectivity to the cloud dashboard when both WAN links are active. If the first link is down, then the second WAN uplink will attempt to connect to the cloud dashboard. The Primary WAN uplink is configurable under the dashboard settings. This link is also the default interface for routed VPN and Internet traffic in the absence of traffic steering policies or Internet traffic load balancing configuration.

LAN Connectivity

The MX85 and MX68 have 10 possible ports that can be used for LAN connectivity, while the MX95/105 has 6. The MX67 has 4 possible ports that can be used for LAN connectivity, although one port (port 2) can be converted into a WAN port. The LAN interfaces are represented in the following table.

Secure Router	LAN Interfaces	Port Numbers
MX67	3x dedicated 1 Gigabit Ethernet RJ45 1x convertible 1 Gigabit Ethernet RJ45 (LAN/WAN)	Ports 3-5 Port 2
MX68	8 dedicated 1 Gigabit Ethernet RJ45 2 dedicated 1 Gigabit Ethernet RJ45 PoE+	Ports 3 -10 Ports 11-12
MX85	8x dedicated 1 Gigabit Ethernet RJ45 2x dedicated 1 Gigabit Ethernet SFP	Ports 5-12 Ports 13-14
MX95/MX105	4x dedicated 1 Gigabit Ethernet RJ45 2x dedicated 10 Gigabit Ethernet SFP+	Ports 5-8 Ports 9-10

The MX router by default is configured for single VLAN (untagged VLAN 1) operation, which is called **Single LAN** mode. All LAN ports are placed into VLAN 1 and a VLAN 1 layer-3 interface is configured with an IPv4 subnet of 192.168.128.0/24, along with a DHCP server configuration and DHCP pool of addresses in the range of 192.168.128.2 - .254. The purpose of the DHCP pool is to hand out IPv4 addresses to downstream LAN devices (switches, APs, etc.), allowing them to be quickly and easily onboarded to the dashboard.

When **VLAN** mode is configured, several VLANs are defined along with their respective layer 3 interface IP addresses that act as IP gateways for downstream clients. When VLAN mode is set for the first time, the **Single LAN** IP address appears under VLAN 1 (named Default) This VLAN also inherits the DHCP server configuration and DHCP pool for devices in VLAN 1 that request DHCP services.

By default, all MX ports are enabled and defined as 802.1Q trunks, allowing all VLANs with VLAN 1 as the native/untagged VLAN. In this design, the link to the switch is left as the default trunk, and all unused ports are disabled to reduce security risks.

In the small branch design, 5 additional VLAN interfaces are defined in addition to the default VLAN 1, including DATA (VLAN 10), VOICE (VLAN 20), IOT (VLAN 30), GUEST (VLAN 50), and INFRA (VLAN 999).

Downstream Device Dashboard Onboarding

When a downstream, connected cloud-managed switch is booted for the first time, all its switch ports default to trunk ports with the native/untagged VLAN defined as 1. The switch initiates an untagged DHCP request on all connected interfaces and receives an IPv4 address in the 192.168.128.2 - .254 address range and gateway address (192.168.128.1) from the MX router. Likewise, when a downstream cloud-managed wireless AP is connected to the switch and initially booted, the AP initiates an untagged DHCP request for an IP address from the same DHCP pool and gateway on its uplink port. The MX router firewall is, by default, configured to allow all outbound traffic to the Internet initiated internally on VLAN 1, and it NATs the traffic to the IP address of the WAN interface. This allows any downstream devices to connect to the dashboard.

Management VLAN

When downstream devices are onboarded by default, their internal management connections are untagged on VLAN 1 and end up sourced with an IP address from the 192.168.128.0/24 pool. This same pool is used as the default for all MX routers in all branches. This allows the devices to connect to the dashboard through the MX's Internet uplink, but if the device needs to access shared services in the data center such as radius, DNS, and other services, then a unique subnet needs to be used instead at each branch for these infrastructure devices.

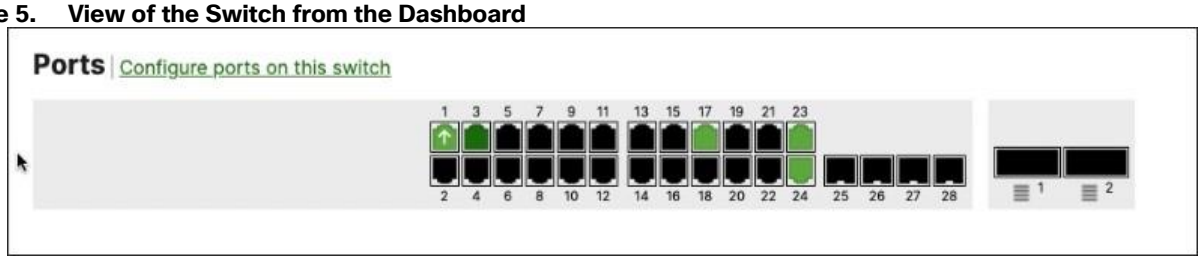
Switches and access points by default try to contact the dashboard on the untagged VLAN, but alternatively, a tagged VLAN can be used under the device configuration settings. In this design, a separate VLAN 999 is created called INFRA and the management control traffic is tagged for that VLAN. Once a device is onboarded to VLAN 1 and connected to the dashboard, it can pull its configuration from the dashboard, to begin tagging its control traffic with VLAN 999. VLAN 999 uses a unique subnet per branch.

To reach the shared services in the data center, the MX router uses the highest VLAN defined and sources the traffic from its IP address in that subnet, which is why VLAN 999 is chosen (so all devices source their management control traffic from the same VLAN). Use the highest VLAN for device management traffic if all devices should use a management IP address from the same subnet.

Unified Branch Switch

Unified Branch release I supports MS150, MS130, C9200/L, C9300/X/L and -M models of switches to provide LAN connectivity to devices within the small branch. Check the individual datasheets for information for specifics on interface types, performance capabilities, physical characteristics, power requirements, Power over Ethernet (PoE) capabilities, etc.

Figure 5. View of the Switch from the Dashboard



Power over Ethernet (PoE)

Support for PoE on switch ports may be needed when connecting wireless LAN (WLAN) APs, IP phones, surveillance cameras, and other devices to the switch.

Several of the MS, C9200, and C9300 models support 802.3at / PoE+ (Type 2) which can supply up to 30W per port up to the total power budget for PoE devices of the switch. Several C9300-M models also support 802.3bt / UPOE (Type 3) which can supply up to 60W per port up to the total power budget for PoE devices of the switch. A few MS models can also support UPOE on a subset of their ports. The total power budget for PoE devices depends on the number of power supplies installed within the switch, as well as the power rating of the individual power supplies (715 Watts AC vs. 1100 Watts AC, etc.). Check the individual data sheets for more details. The Cisco Power Calculator can also be leveraged to determine PoE power consumption for select Cisco models.

Uplink Connectivity to Switch

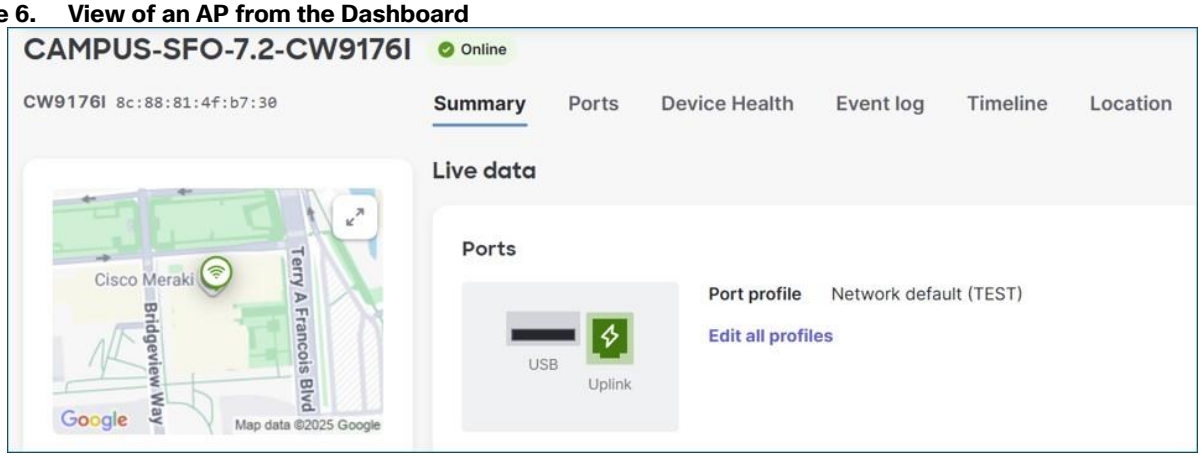
By default, the switch port uplink connecting to the MX device is configured as an 802.1Q trunk port allowing all VLANs with VLAN 1 being the native/untagged VLAN. While unused VLANs can be pruned off the trunk, if VLANs are added or changed, extra configuration steps are required to add/change VLANs on the trunks. Also, an unused VLAN can be configured as the native/untagged VLAN for additional security hardening. In this design, all VLANs are allowed on the trunk to keep configurations simple, and VLAN 1 remains the native/untagged VLAN. VLAN 1 is used as initial onboarding for any new devices added to the network and has access only to the Internet (for dashboard connectivity). Once a device configuration is downloaded, devices use the INFRA tagged VLAN 999 for management traffic.

The link speed (10 Mbps, 100 Mbps, 1 Gbps, and/or 10 Gbps) and duplex (full or half) of the Ethernet ports on the MX router and the switch must match for the uplink to come up active. A best practice is to leave the link speed for auto-negotiation of speed and duplex.

Unified Branch WLAN Access Points

Unified Branch release I supports C9172 and C9176 models of Access Points (APs) to provide wireless LAN (WLAN) connectivity within the branch. Check the individual data sheets for information for specifics on capabilities, power requirements, etc.

Figure 6. View of an AP from the Dashboard



Uplink Connectivity to the Switch

The CW9176 and CW9172 APs support a single uplink port for connectivity to the switch. By default, the AP uplink connecting to the switch is configured as an 802.1Q trunk port allowing all VLANs with VLAN 1 being the native/untagged VLAN. As mentioned previously, VLAN 1 is the default/untagged VLAN to ensure downstream switches and APs can initially connect to the dashboard to onboard, but the device management is moved into the tagged INFRA VLAN 999 once configurations are downloaded. Since the AP will service both corporate and guest users in different VLANs, the connection between the AP and switch should be configured as a trunk port. In this design, the default trunk configuration settings are used for simplicity.

As with the uplink between the MX router and the switch port, link speed and duplex (full or half) of the Ethernet ports on the switch and the AP must match for the uplink to come up active. Again, a best practice is to typically leave the link speed for auto-negotiation of speed and duplex.

Access Point Model	LAN Uplink Interfaces
CW9172I/CW9172H	1x 100M/1G/2.5G BASE-T Ethernet (RJ45)
CW9176I/DI	1x 100M / 1G / 2.5G / 5G / 10G BASE-T Ethernet (RJ45)

PoE Requirements for Access Points

When configuring the uplink between the switch and APs, the network administrator needs to consider how power is to be supplied to the APs. Power can be supplied via a switch that supports PoE and supplies the necessary power (in terms of Watts) required for the AP model, or through an external device such as a power supply or inline PoE injector. To ensure the power is sufficient to power the AP, check the individual AP data sheets for minimum and maximum power requirements.

Throughput requirements

The aggregate throughput requirements of each AP within a small branch site should be determined based on the number of clients and each client's application requirements and traffic expectations and ensure that uplink speeds to the switch are adequate and can accommodate for future growth.

Unified Branch Services

Multiple services are included in Unified Branch Release I, such as WAN services, wired LAN services, wireless LAN services, security services, and network management services.

WAN Services

Secure WAN services are implemented by the MX router. This includes Software-defined WAN (SD-WAN) and its features, such as secure WAN connectivity, LAN to WAN routing, and traffic shaping.

Software-defined WAN (SD-WAN) is a set of features that enables networks to automatically adapt to changing WAN conditions without manual intervention, ensuring optimal performance for critical applications and minimizing disruptions for sensitive traffic like VoIP. It also offers secure, granular traffic control and is often a more scalable and cost-effective solution compared to traditional WAN circuits such as MPLS. SD-WAN makes use of the Auto VPN feature, which is a proprietary technology that facilitates route advertisements and allows VPN tunnels to be easily built between WAN routers in the network branches.

WAN Connectivity

WAN connectivity refers to the wide area network's topology and how the router connects to it. The router in a branch typically connects directly to the service provider, obtains a dynamic IP address by default, and receives a gateway address and DNS server address through DHCP. Traffic from the branch router is sent towards the service provider to connect to the dashboard, to route Internet traffic, or to route encrypted VPN tunnel traffic to another branch site. Note that IP addresses, gateways, and DNS server addresses can also be statically defined as an alternative to DHCP.

This design uses DHCP on both transports to obtain IP addresses, gateways, and DNS server addresses.

WAN Topology

A WAN topology refers to the different ways that a Wide Area Network can connect to multiple locations, such as full mesh, hub-and-spoke, and partial mesh. Unified Branch release I implements the hub-and-spoke topology, where all branch sites (spokes) set up direct VPN tunnels to a central hub or multiple hubs.

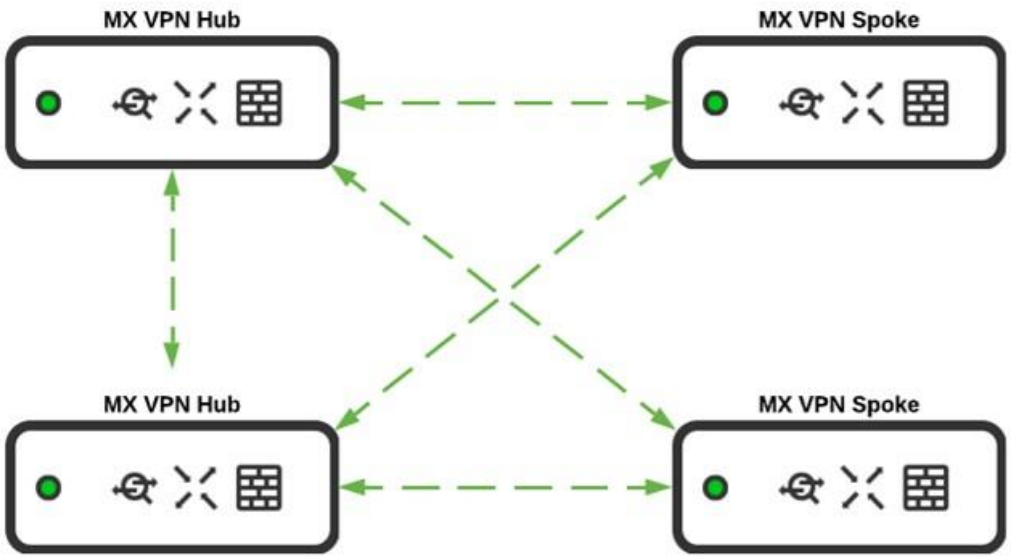
A hub is defined as a central site, such as headquarter locations, data centers, and large campuses that is hosted near resources and services that other locations need to access. Hubs also set up direct VPN tunnels to other hubs. All spoke-to-spoke communication must traverse the hub.

This model simplifies management and traffic flow and is cost-effective because only hubs need to have the capacity to scale the number of VPN tunnels required. However, it introduces additional latency as all traffic must pass through the hub, which could also become a congestion point if not properly designed. For proper redundancy, ensure that more than one hub is defined.

When configuring spokes in a hub-and-spoke VPN topology, the spokes must have the hubs explicitly listed or configured as peers to establish tunnels. Before hubs can be chosen in the drop-down menu in the spoke configuration, they must have first been defined as a hub in their own configuration. In what order the hub is listed determines the hub priority for that spoke. When a route is available through multiple hubs, the spoke routes to the hub highest on the list.

In this design, two hubs are defined with DC1 as primary and DC2 as backup.

Figure 7. Hub-and-Spoke Topology with Two Hubs for Redundancy



Auto VPN

Auto VPN is a proprietary technology that automatically builds encrypted VPN tunnels between WAN routers in the network branches. The main mechanism that allows Auto VPN to happen is the VPN registry, which is a cloud service that keeps track of contact information for the WAN routers participating in Auto VPN for an organization. Routing across the secured WAN leverages the contact information found in the VPN registry. It is important that certain IP addresses and ports are open on any upstream firewalls so WAN routers can reach the VPN registry. See Auto VPN Configuration and Troubleshooting for more information.

Dual WAN

In Unified Branch release I, dual WAN transports are implemented, both of which have connectivity to the dashboard. Dual WAN uplink provisioning to separate service providers is a general best practice for resiliency purposes so when a connection to one transport or provider fails, there is still connectivity for traffic through the opposite transport or provider. Connection monitoring is performed on each WAN uplink interface once carrier is detected and an IP address is assigned (static or dynamic), which can determine the health of the uplink and Internet connectivity and determine when failover needs to take place. See the Connection Monitoring Test Process page for more information.

By default, control connectivity to the dashboard leverages the first WAN (WAN 1) but will leverage the second WAN (WAN 2) if the first WAN uplink connectivity fails. The primary WAN uplink can be configured through the dashboard and is also the default interface for routed VPN and Internet traffic in the absence of traffic steering policies or Internet traffic load balancing configuration.

With dual uplink solutions, VPN tunnels can run over both available uplinks or when the primary link fails. This design utilizes VPN tunnels over both uplinks.

Dual WAN can be implemented as active/standby or active/active. With active/standby, all traffic (VPN and Internet) is directed out WAN 1 and falls back to WAN 2 when WAN 1 fails. With active/active, both uplinks are available for traffic forwarding. In active/active mode, Internet traffic and VPN traffic can use traffic

steering to direct some traffic out one link or the other, but there is also the ability to load-balance Internet traffic.

This design implements dual WAN as active/active. Some VPN and Internet traffic is directed out of the second WAN transport with traffic steering policies, and all other traffic is directed out of the first WAN transport by default.

With load balancing, Internet-bound traffic flows are distributed between the two uplinks. How the load is distributed between the WAN 1 and WAN 2 links depends on the bandwidth configured under the Uplink configuration. The link with the higher configured bandwidth distributes more flows. Note that load balancing is based on flows considering source and destination IP and port and will attempt to round-robin connections on both WAN uplinks.

Note that some applications spawn off multiple sessions for a single use session which could get load-balanced to the opposite WAN uplinks with different NAT addressing. This can cause application failures. Disable load-balancing in those cases and use traffic steering policies to distribute traffic to the WAN uplinks.

This design does not implement load-balancing for Internet-bound traffic.

LAN to WAN Routing

Auto VPN through the VPN registry populates the routing table of subnets which belong to other sites. For a VLAN subnet to be advertised, its **VPN mode** setting is set to **Enabled** in the dashboard configuration. For VLAN subnets that should not be advertised, their **VPN mode** setting is set to **Disabled** (the default). In this design, the default VLAN 1 and Guest VLAN 50 subnets are set to disabled, while all other VLANs are set to enabled.

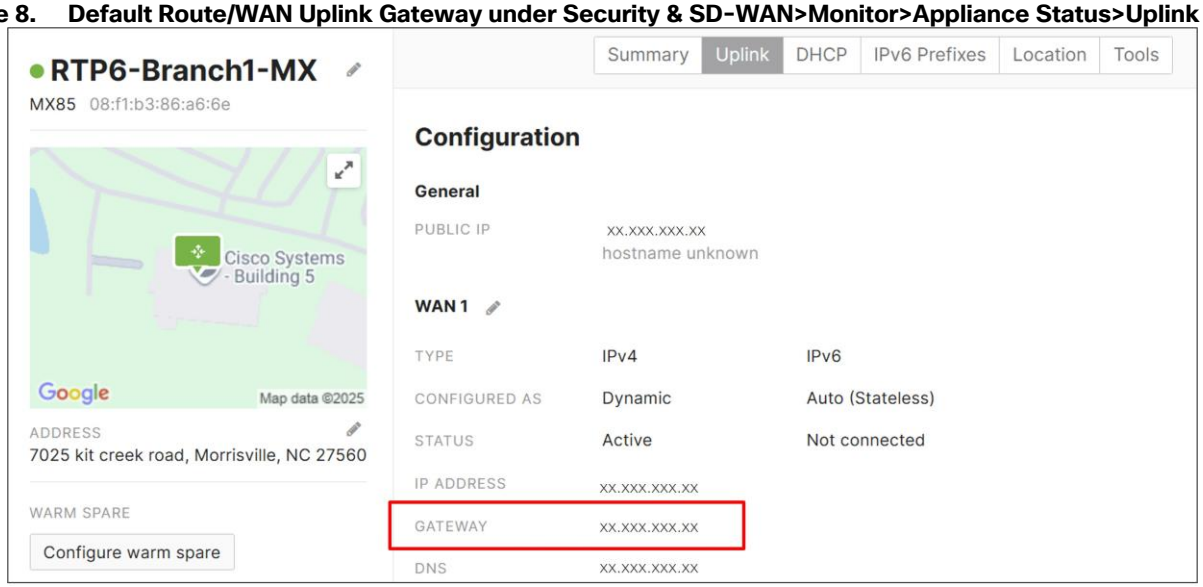
When client traffic needs to be routed, the routing table is consulted for the destination for the longest-match prefix. If the route exists in the table, then the traffic is routed according to the next hop. The route could be a connected or static route, client VPN and other VPN peer route, Auto VPN route (where traffic will be directed over the VPN tunnel to a particular site), or BGP-learned route. Given the same route, one route type is selected depending on the priority. See the MX Routing Behavior document for more information. Connected, static, and Auto VPN routes are supported in Unified Branch release I.

If a specific Auto VPN route has multiple next hops to its hubs after the longest-match prefix is selected, then the router will choose to route to the hub with the highest priority. This priority is established through the order in which the hubs are defined on the spoke's **Site-to-site VPN page** on the dashboard.

Default Route Advertisement

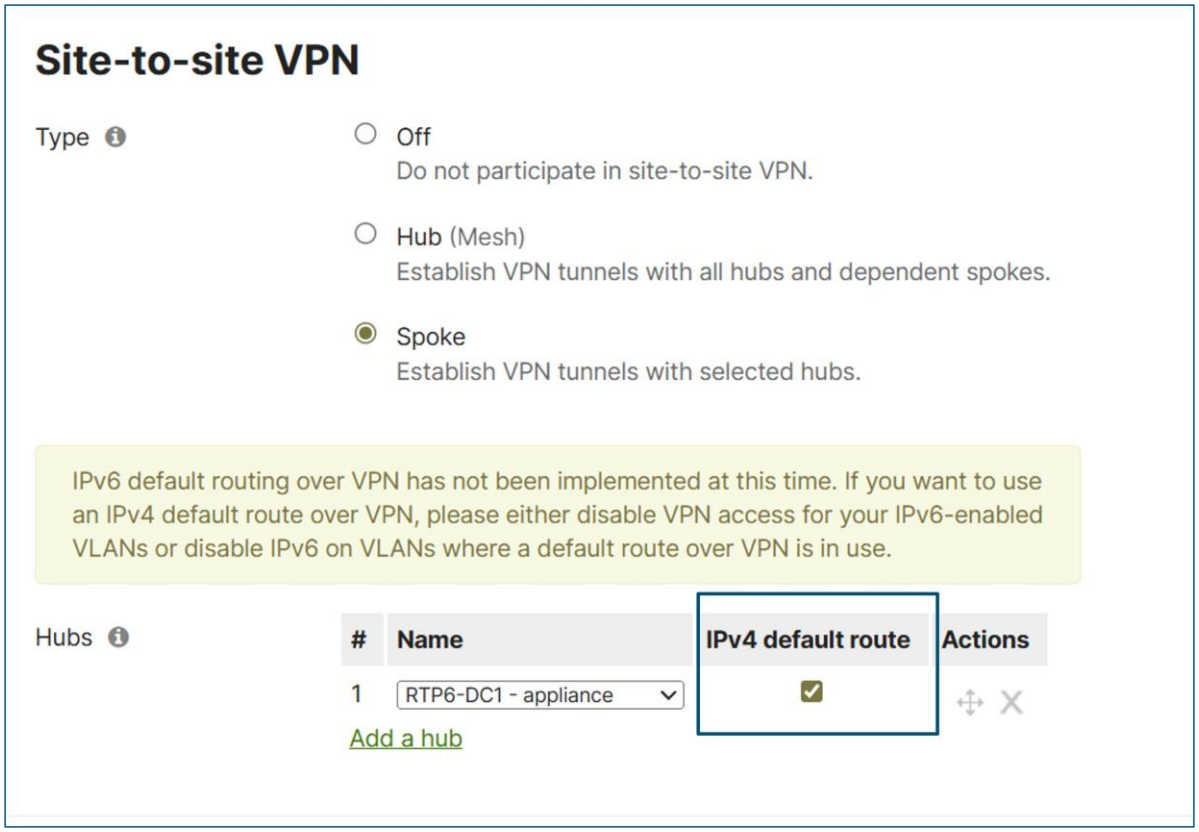
There are multiple ways for default routes to be defined for an MX router. By default, default routes are always installed using the WAN uplinks as the next hop out to the Internet. If no other default routes are defined, traffic will take the default route directly to the Internet if it doesn't match a route in the Auto VPN overlay.

Figure 8. Default Route/WAN Uplink Gateway under Security & SD-WAN>Monitor>Appliance Status>Uplink



A default route can also be configured from a hub when the hub is defined on the spoke's **Site-to-site VPN** configuration page. Next to the hub definition, an IPv4 default route box can be checked. This default route takes precedence over an uplink default route. This means that all traffic not matching other VPN routes, which includes Internet traffic, takes the overlay to the hub advertising the default route and is routed from there. If multiple hubs advertise the default route, then the router will choose to route to the hub with the highest priority.

Figure 9. IPv4 Default Route from Hub



Another way to advertise a default route from the hub is to add a static default route and enable it for VPN mode or advertise it from the hub through BGP.

The routing table on the branch router can be viewed under **Monitor>Route Table** on the dashboard.

In this design, default routes are advertised from each hub using the IPv4 default route configuration on the spoke's **Site-to-site VPN** configuration page.

Direct Internet Access (Local Internet Breakout)

By default, if there are no default routes advertised from the hub sites, traffic can be sent out direct Internet access (DIA) from the branch using the WAN uplink if there are no matches to routes already in the routing table. When a default route is advertised from the hub sites, this puts the branch in full tunnel mode which means all traffic is now tunneled, including Internet traffic. The exception to this is for any VLAN subnet with **VPN mode** disabled, which means the subnet is not advertised across the Auto VPN. This traffic is also not transmitted across the VPN and can only be transmitted out the direct Internet uplink, unless prohibited by firewall rules.

If direct Internet access is needed while in full tunnel mode, VPN exclusions must be configured. This allows the administrator to configure layer-3 and some layer-7 destination rules to determine exceptions to the full tunnel VPN configuration, allowing some traffic to go out to the Internet directly.

DIA improves the user experience since it eliminates any performance degradation related to backhauling Internet traffic to a centralized data center.

In this design, some SaaS traffic for corporate users and dashboard traffic for downstream switch and AP devices leverage VPN exclusions.

SD-WAN Traffic Policies

SD-WAN traffic policies match traffic and steer traffic to a particular uplink and failover to the opposite uplink should the preferred one fail or if SLAs are not met for performance. Rule definitions for classifying/matching traffic are based on L3 characteristics (source and/or destination IP address and/or port) or L7 characteristics (application and/or application category). If a policy is contingent on performance, it references a previously configured performance class. Performance classes are configured to define the max loss, latency, and jitter a traffic class can tolerate. SD-WAN policies are defined separately for Internet and VPN traffic.

For VPN traffic, performance probes (UDP data of approximately 100 bytes) are sent every second and are used to determine loss, latency, and jitter over each Auto VPN tunnel. For Internet data, uplink statistics are gathered. The default target is 8.8.8.8 (Google DNS), but it can be modified from the dashboard under **Security & SD-WAN>Configure>SD-WAN & traffic shaping>Uplink configuration>Uplink statistics**.

Note that all traffic not matching a defined policy is routed to the default WAN uplink until it is declared down, regardless of loss, latency, or jitter. It is recommended to define a default traffic policy with a default performance class to catch all other traffic not already specified in policy to avoid traffic being transported across a poor-performing tunnel.

In this design, both Internet traffic and VPN traffic steering policies were created. Custom performance classes were defined for SaaS traffic, critical application traffic, and default VPN traffic.

WAN Traffic Shaping

On the MX router, uplink bandwidth settings, both upload and download bandwidth, can be set. These values are used for rate-limiting all traffic in and out through each WAN port. This is used when the

contracted bandwidth for the WAN service (the sub-line rate) is less than the physical bandwidth of the connection. Bandwidth limits can even be set on each client device's total incoming/outgoing traffic.

There are also shaping polices that can be applied on a per user per-application basis. Applications or custom expressions (CIDR/IP ranges, ports, local networks, etc.) can be used to match traffic, then bandwidth limits (optionally), priority, and DSCP tags can be assigned. Priorities can be set to High, Normal, or Low and allow the MX router to prioritize a given network flow relative to the rest of the network traffic. Expedited Forwarding traffic (DSCP 46) is given highest priority. Default shaping rules can be used with additional rules added, or rules can be completely customized.

For more information, see the SD-WAN and Traffic Shaping document.

In this design, uplink bandwidth setting examples are provided. Also, default shaping rules are used with additional rule examples for guest and critical application traffic.

Wired LAN Services

Some wired LAN services are implemented by the MX router, some by the switch, and some by both. These services include LAN connectivity, Link Layer Discovery Protocol (LLDP), VLAN segmentation, Spanning Tree Protocol, STP Guard, storm control, access policies, shared services VLAN, LAN Routing, DHCP, and LAN Switch QoS (ingress classification, marking, and queuing).

LAN Connectivity

For LAN connectivity, there are 802.1Q trunks between the MX router, switches, and access points to carry VLAN-tagged traffic as well as native/untagged VLAN 1 traffic. Ports on the network devices are set to auto-negotiate port speed and duplex as a general best practice unless there is a specific reason otherwise.

Link Layer Discovery Protocol (LLDP)

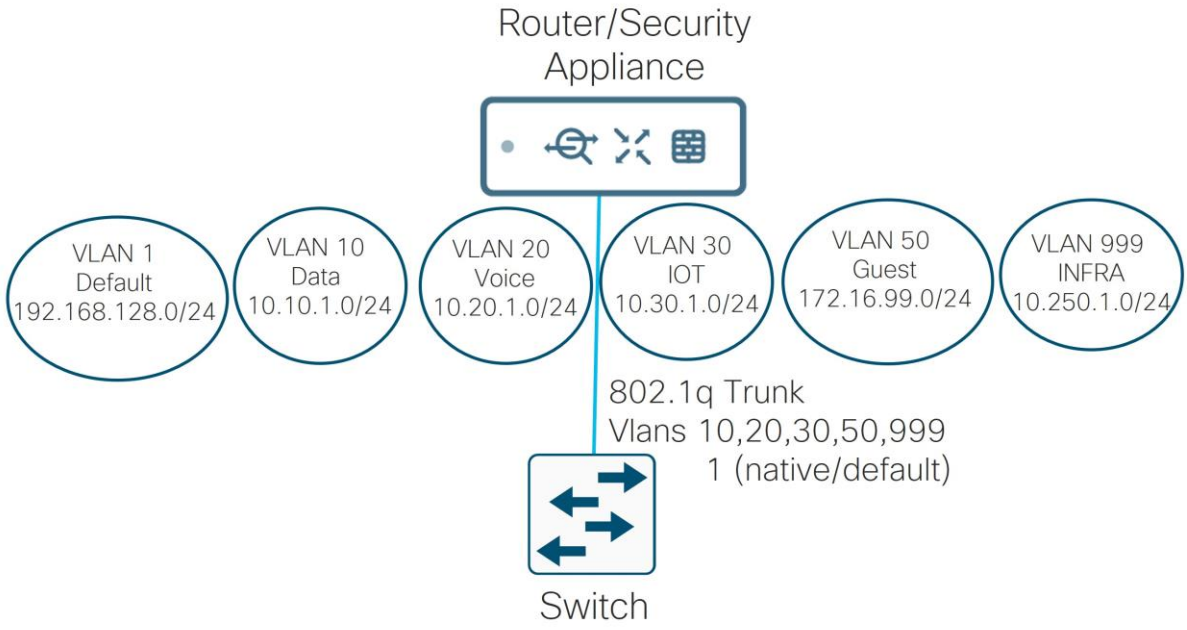
LLDP is a layer-2 protocol that automatically discovers connected devices. It is used to identify devices and their capabilities on the network, inform VoIP devices of the voice tagged VLAN, and negotiate PoE needs. LLDP is turned on by default.

VLAN Segmentation

VLAN segmentation provides a way to partition the network into different broadcast domains, each with a separate subnet. Data packets can be tagged with a VLAN identifier (VLAN ID) and switches can use tags to only forward between ports that share the same VLAN ID. Access ports assign incoming untagged traffic to a VLAN based on the port configuration, and trunk ports can carry all tagged VLAN traffic, as well as untagged traffic that is assigned to the native VLAN defined on the trunk. To communicate with devices in other VLANs, traffic needs to be forwarded to a layer-3 device that can route between VLANs.

The router provides the layer 3 termination point (SVIs) for multiple network VLANs, and by default, allows routing between those VLANs. In this design, the router is configured for six different VLANs: Default (VLAN 1), Data (VLAN 10), Voice (VLAN 20), IOT (VLAN 30), Guest (VLAN 50) and INFRA (VLAN 999). VLANs 10, 20, 30, 50, and 999 are carried on the trunk port between the router and switch, and VLAN 1 is the native or default VLAN for any untagged traffic coming in.

Figure 10. VLAN Segmentation



To prevent inter-VLAN communication, firewall rules can be added on the MX. To prevent subnets from being advertised and traffic from being routed across the VPN network, subnets are **Disabled** for **VPN mode** in the dashboard. For example, the Guest and Default subnets are Disabled as their traffic should not traverse the VPN tunnel network. It is assumed that the Guest and Default VLAN traffic will have direct Internet access only and may be further restricted based on security policies implemented on the MX. The rest of the subnets are **Enabled** for **VPN mode** and advertised to other WAN routers through the VPN registry.

Spanning Tree Protocol

Spanning tree is a network protocol designed for Ethernet networks to prevent bridge loops and broadcast storms that result from them. It operates at layer 2 (the Data Link Layer) of the OSI model. Rapid Spanning Tree Protocol (RSTP) is an enhanced version of the original protocol, providing faster convergence times after network topology changes or link failures.

On the switches, RSTP is enabled by default and will be active on all switches in the current network. Access ports on link up will bypass the learning state and immediately go into a forwarding state. It is critical that spanning-tree remains enabled to protect from unintended loops in the network. It's also best practice to choose and configure the root switch and backup root switches, which are typically in the core or distribution layers. In the small branch, the single switch or switch stack can be configured with a bridge priority of 4096 to make it the root switch or switch stack. Using 4096 as the bridge priority instead of 0 provides flexibility to make temporary modifications to the root bridge if necessary. The default bridge priority is 32768. Once RSTP is enabled globally, it is enabled at the port level by default. It is recommended that RSTP be enabled on all ports. It is important to note that the MX router does not run spanning tree and will not exchange BPDUs with other switches nor participate in the root bridge election process. If the MX router receives BPDUs on the LAN, these BPDUs are re-forwarded to other ports within the same VLAN, or broadcast domain.

In this design, RSTP is enabled, and the switch/switch stack is configured to be the root switch/switch stack with a priority of 4096.

STP Guard

STP guard is a configuration option under the switch port or switch port profile. Settings include **Disabled**, **Root guard**, **BPDU guard**, or **Loop guard**. STP Guard is disabled by default.

For the single switch/switch stack design, only BPDU guard is applicable. This configuration protects the spanning tree topology by enforcing the STP domain borders. The port moves into a disabled state if it receives a BPDU. This should be applied to all ports or ports connected to clients. Do not apply to the uplink port connecting the switch to the router.

In this design, BPDU guard is applied to all ports except the port connecting to the MX.

Unidirectional Link Detection (UDLD)

UDLD detects and acts on logical one-way links to prevent forwarding loops and blackholing of traffic. It is supported on switches and configured under a port or port profile. The **Alert only** setting (default) generates an alert if UDLD detects one-way traffic. The **Enforce** setting blocks network traffic if UDLD detects one-way traffic. Enforce is recommended to be used on point-to-point links between switches.

This design uses the **Alert only** setting for UDLD on all ports.

Storm Control

Storm control is designed to prevent network performance degradation caused by a network storm of excessive broadcast or multicast traffic. It can be enabled on switches to suppress broadcast, multicast, and unknown unicast packets based on a traffic percentage on an interface. Each category of traffic bandwidth is monitored on each switch port every second. Traffic that exceeds the defined limit is dropped.

To set the percentage of broadcast, multicast, and unknown unicast traffic, the administrator needs to understand what the normal level of broadcast, multicast, and unknown unicast traffic is in the network. This will vary from network to network and may depend on the day of the week and even the time of day.

In this design, an example storm control policy is created.

Access Policies for Port Access

Access policies can be configured on the switch, which require authentication from a RADIUS server before network access is granted. These are commonly configured on access-layer switch ports to prevent unauthorized devices or users from connecting to the network. RADIUS servers can pass back dynamic VLAN information the client belongs to and well as other information, and the client can then obtain IP address information through DHCP.

The Radius server can be the built-in radius server from the dashboard or a standalone server in the network.

There are three access policy types:

- 802.1x: Clients that connect are prompted for their credentials. If credentials are valid, their device can be granted access to the network.
- MAC Authentication Bypass (MAB): When MAB is enabled, the client's MAC address is authenticated against a RADIUS server. If the server determines the MAC address is a valid credential, the device will be allowed access.
- Hybrid Authentication: With hybrid authentication, clients are prompted for their credentials for 802.1x authentication, but if the client doesn't start 802.1x authentication then the client's MAC address will be

authenticated with the RADIUS server. Hybrid authentication is useful when not every device supports 802.1x authentication, however, MAB is less secure and more easily spoofed.

Host mode for 802.1x refers to how many clients can be authenticated and connected through a single port, and there are 4 different settings. **Single-host** allows only one client per port. **Multi-host** allows multiple clients, and one successful authentication grants access to all clients on that port. **Multi-auth** allows multiple clients but each authenticates separately. **Multi-domain** requires separate authentication for voice and data devices on the same port.

In this design, a RADIUS server in the data center is leveraged. The access policies are applied to client ports using hybrid authentication and set for single-host mode. No failed Auth VLANs are defined if authentication fails.

Shared Services VLAN

A shared services VLAN is designated to host network services that can be leveraged by other VLANs. Its purpose is to centralize, secure, and efficiently manage common network services that are utilized by other VLANs. In a local branch, a shared services VLAN might contain shared resources such as local printers or files servers that do not need to reside at a data center or central site. To allow certain traffic or restrict certain traffic to this VLAN locally, layer-3 and layer-7 firewall rules can be added to the MX router.

In the data center, shared services could be DHCP, DNS, RADIUS, syslog, NetFlow, etc. VLANs with devices that need to reach shared services in the data center need to have their VPN mode enabled so their subnet can be reachable from the data center. To allow certain traffic or restrict certain traffic across the Auto VPN overlay, site-to-site firewall rules can be added to the MX router.

This design doesn't leverage a shared services VLAN but uses firewall rules to allow access to a subset of resources in a local branch VLAN and data center.

LAN Routing

In Unified Branch Release I, the MX router is configured for layer-3 routing with Switched Virtual Interfaces (SVIs), meaning the routing to the LAN is through the directly connected VLAN interfaces (connected routes). Static routing is also supported in this release. Static routes are used so traffic can be routed to other subnets reachable through another layer 3 device on the network. Each static route requires a next hop IP address defined that is included within the scope of a configured VLAN/subnet so traffic can be routed successfully. When a static route is added to the MX router, it can optionally be enabled for VPN mode so it can be advertised to other sites.

This design uses connected routes on the LAN.

Dynamic Host Configuration Protocol (DHCP)

DHCP is a network protocol used on IP networks and automates address assignment and other network configuration parameters to devices to allow them to communicate on the network. It reduces manual workload for network administrators, minimizes errors, and allows new devices to be added quickly or moved to other network segments without manual intervention.

In Unified Branch Release I, the MX router can act as a DHCP server, or it can forward DHCP messages to a centralized server, commonly located in a data center. As a DHCP server, lease time is configurable up to a week, boot options and DHCP options and DNS servers can be specified, and reserved ranges and fixed IP assignments can be configured. Mandatory DHCP is also configurable, and if enabled, client traffic without DHCP leases (ex. static IP addresses) will be dropped.

DHCP settings are set for each VLAN that has a layer-3 interface on the router.

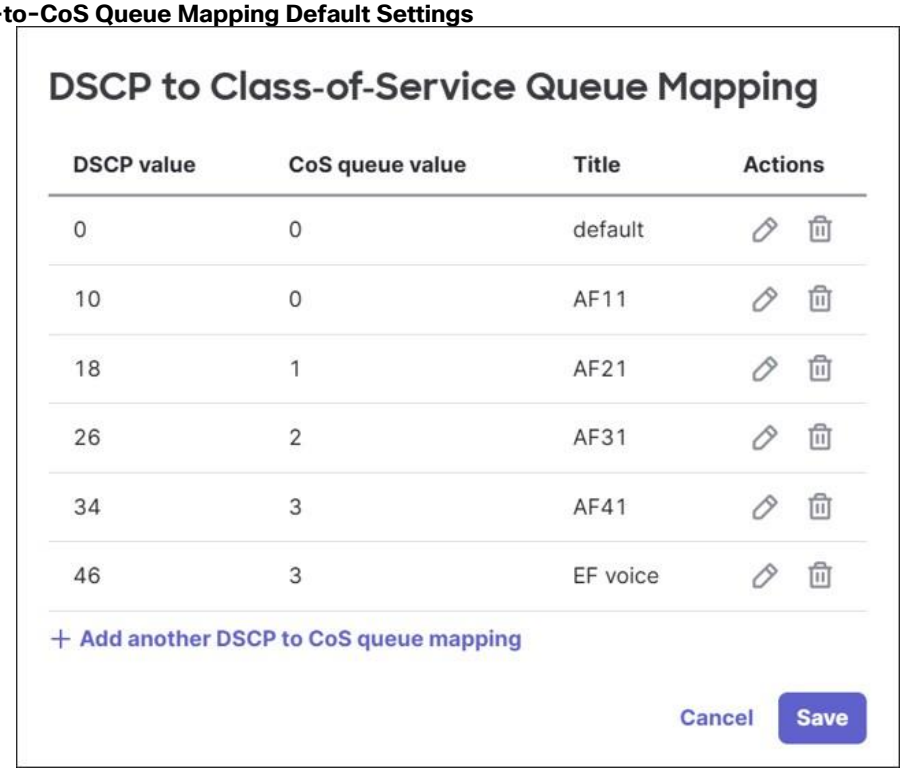
In this design, the default VLAN, guest VLAN, and Infra VLAN use local DHCP services from the MX router, while the other VLANs get relayed by the MX to a DHCP server positioned in the data center. The default VLAN and guest VLAN receive OpenDNS IP addresses on the Internet to use for DNS, while the other VLANs receive DNS server information in the data center. For the Infra VLAN, fixed IP assignments are created for the switch and AP, so their IP addresses stay the same and no static IP address configuration is required for ease of operation.

LAN Switch Quality of Service (QoS)

QoS allows for prioritization of traffic in the network. It guarantees some fraction of the link to each configured priority level when there is congestion on the link. Higher priority queues receive more bandwidth than those in lower priority queues, but bandwidth can be used by other queues when there is no congestion.

Differentiated Services Code Point (DSCP) bits in the packet header inform switches what Class-of-service (CoS) queue should be used through a DSCP-to-CoS queue mapping policy table that can be modified.

Figure 11. DSCP-to-CoS Queue Mapping Default Settings



DSCP bits can be added, modified, or trusted for a particular packet. The switches use QoS network rules matching on VLAN, protocol, source port or destination port to define how to handle DSCP tagging of packets.

By default, DSCP tags are trusted and passed through unmodified, and default DSCP-to-CoS settings are used to determine what outgoing queue packets will use. An incoming packet with DSCP set that does not match a QoS rule will keep the DSCP setting, and if a packet's DSCP does not match the DSCP-to-CoS mapping, it is placed into the default queue.

Note that Switch QoS settings are network-wide settings, so all switches sharing a network inherit the same settings. See MS Switch Quality of Service Defined for more information.

In this design, the DSCP-to-CoS mappings were kept at default. Guest traffic is set to untrusted and get assigned DSCP 0, while other traffic is set to trust DSCP values.

Wireless LAN Services

Wireless LAN (WLAN) services consist of configuration related to wireless LAN clients. The services consist of wireless connectivity, support for multiple SSIDs, guest services, RF profiles with radio resource management (Auto RF and AI-RRM), and wireless QoS.

Wireless Connectivity

Wireless LAN connectivity is provided through Wi-Fi 7 / 802.11be compliant CW9172 and/or CW9176 cloud-managed access points (APs) which function as gateways that bridge wireless LAN clients onto the wired LAN as well as provide connectivity between WLAN clients where desired. In bridge mode, wireless LAN clients receive IP addresses either from centralized DHCP servers or from DHCP pools defined on the MX router.

In this design, guest clients receive IP addresses from a local pool defined on the MX router, while the corporate clients receive IP addresses from a centralized DHCP server in the data center.

Multiple SSIDs

Multiple SSIDs can be configured to provide different services and levels of security within the branch deployment. For example, an SSID targeted for employee traffic can be configured 802.1X authentication using an external Radius server, operating in WPA3 transition mode.

In this mode, wireless clients that support both WPA3 – the latest Wi-Fi security protocol – can connect to the SSID using the 2.4, 5, or 6 GHz bands. Additionally, wireless clients that support only WPA2 can connect to the same SSID using only the 2.4 or 5 GHz bands.

Rather than provisioning multiple SSIDs for data, voice, and IoT devices, the Radius server can leverage group policy configured through the dashboard to assign the VLAN which the client traffic is to be terminated based on its identity, learned via username/password, digital certificate, or MAC address / MAB. This reduces the number of SSIDs broadcast within the branch.

Alternatively, for IoT devices, another SSID configured for pre-shared key (PSK) authentication, operating in WPA2 mode may be provisioned to alleviate the burden of maintaining MAC address lists.

In this design, one guest and one corporate SSID are configured. Within the corporate SSID, 802.1x authentication and WPA3 transition mode are enabled. After the client authenticates, a group policy name is passed back from the Radius server which references a VLAN to assign for the client traffic.

Note that Wi-Fi 7 cannot be enabled in the corporate SSID until per-group SSID configuration is supported because the guest SSID, which resides on the same AP, does not meet the security standards necessary. Per-group SSID configuration is available starting in MR release 32.1.4, where Wi-Fi 7-compliant SSIDs can co-exist on the same AP as non-Wi-Fi 7-compliant SSIDs as long as they are in separate SSID groups.

Guest Services

To support wireless guest services, a separate SSID may be provisioned within the branch. There are multiple methods for provisioning guest wireless access, from self-registration portals to requiring an internal sponsor within the organization. The most basic wireless guest access consists of an open SSID mapped to a VLAN, with a simple click-through splash page.

Guests may be allowed access to the Internet only, optionally with the ability to restrict the content to which they are allowed to access through the content filtering and next-gen firewall capabilities of the MX router. There is also a setting to enable layer-2 LAN isolation where clients can only communicate with their IP gateway and not to other clients within the SSID.

In this design, a separate guest SSD is provisioned using an open SSID mapped to a VLAN with a simple click-through splash page. Guests are allowed only access to the Internet with layer-2 isolation enabled.

SSID Availability

With this feature, the administrator can specify certain times of day that an SSID is available on a particular access point. Once enabled, an existing schedule template can be chosen, or a custom schedule can be created.

In this design, a custom schedule is created.

RF Profiles with Radio Resource Management (Auto RM and AI RRM)

The dashboard provides pre-configured RF profiles for ease of deployment. For release I of Unified Branch, only a single RF profile is needed for small branch designs. The Basic Indoor Profile can be used directly or copied first then modified as needed to meet the requirements of branch. The RF profile controls various settings including RF bands (2.4, 5, & 6 GHz) enabled within the branch - either on a per AP, or per SSID basis, minimum bit rate configurations - either on a per band or per SSID basis, minimum and maximum transmission power or the radios within each band, as well as channel width as well as channel assignments within each band, among other functions. Band steering is also an option which steers capable clients to use the higher frequencies to leave lower frequencies available for legacy clients. A best practice is to allow radio resource management (RRM) and AI-RRM to leverage the RF profile to optimize the RF environment for wireless client devices.

In this design, the corporate SSID is enabled for 2.4 GHz, 5 GHz, 6 GHz, as well as band steering. The guest SSID is enabled for 2.4 GHz and 5 GHz. Default settings were mostly chosen.

Wireless QoS

Cloud managed APs support per-user and per-SSID bandwidth shaping in the upstream and/or downstream direction. For SSIDs with employee traffic (such as the Corp SSID) there may be no need or desire to limit traffic. However, there may be a desire to limit traffic on the Guest SSID, so that it consumes only a certain amount of bandwidth on the wireless medium as well as on the Internet WAN connection. This can be accomplished through per-client and per-SSID bandwidth shaping configuration within the dashboard. Note that this can only be enforced on a per-AP basis.

In addition to bandwidth shaping, cloud-managed APs also support traffic shaping. Traffic shaping provides the ability to identify traffic based on custom rule definitions specifying HTTP hostnames, port number, IP address range, or combinations of IP address range and port; or based on pre-defined Layer 7 application categories. Once categorized, rule actions control shaping and/or prioritization of the traffic by allowing unlimited bandwidth usage (ignoring bandwidth shaping limits set for the SSID), obeying the SSID limits set for the SSID, or applying more restrictive limits than specified for the SSID. The cloud dashboard provides a default set of rules for ease of deployment, which can be enabled or disabled.

In terms of QoS classification & marking traffic, cloud-managed APs implement a default downstream mapping of DSCP value to 802.11 access categories found at the following URL: https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Wireless_QoS_and_Fast_Lane

In the upstream direction, QoS sent by the client is honored. The DSCP field within the traffic sent from the client is maintained on the Ethernet network.

In this design, both guest and corporate SSIDs leverage default shaping rules. Only guest traffic utilizes the per-client and per-SSID bandwidth limit settings.

Security Services

Security is already built into different layers of the branch and across multiple devices. This section specifically covers the next-generation firewall features of the MX router.

A traditional firewall provides basic security, NAT, and stateful rule-based inspection and filtering but lack application awareness and advanced features. Next-generation firewalls include advanced features such as deep-packet inspection, intrusion detection and prevention system (IDS/IPS), advanced malware protection (AMP), URL and other content filtering capabilities.

Firewall

Firewall rules apply to traffic passing through the firewall and not traffic that originates or terminates on the firewall itself. There are two different areas in the dashboard to configure firewall rules on the MX router:

- Site-to-site VPN firewall rules: These rules apply only to outbound site-to-site VPN traffic, and these rules apply at the organization level for all MX routers that enable site-to-site VPNs. By default, all traffic is permitted from site-to-site. Rules can be configured for UDP, TCP, or ICMP protocols, source and destination subnets and source and destination port numbers if needed. Objects and object groups can be configured in lieu of source and destination subnets for ease of use.

  In this design, site-to-site VPN firewall rules are used to permit access to shared services in the data center and prevent access to other VLANs across the auto VPN fabric.

- Layer 3 and Layer 7 firewall rules: Layer 3 rules are stateful and apply to direct Internet traffic as well as inter-VLAN traffic on a specific MX router. In NAT/routed mode, traffic is allowed outbound by default, and no traffic is allowed inbound except for ICMP directed to the MX router. To allow additional inbound traffic, NAT rules should be modified, and inbound rules to explicitly allow the traffic on inbound need to be configured. Outbound Layer 3 rules can be created for outbound Internet traffic and Inter-VLAN traffic. Rules can be configured for UDP, TCP, or ICMP protocols, source and destination subnets or VLANs and source and destination port numbers if needed. Objects and object groups can be configured in lieu of source and destination subnets for ease of use.

  Layer 7 firewall rules are stateless and allow traffic to be blocked by application or application category, HTTP hostname, port and/or remote IP range. Geo IP-based rules can also be created, where traffic can be blocked based on country. If traffic is permitted by the layer 3 firewall, it is evaluated by the layer 7 firewall rules before being permitted. Layer 7 rules apply to VPN site-to-site traffic as well as direct Internet and inter-VLAN traffic, unlike Layer 3 rules, which do not apply to VPN site-to-site traffic.

  In this design, layer 3 rules are created to allow local shared services access, allow direct Internet access for some VLANs, and deny access between VLANs. No layer 7 rules were created.

Intrusion Detection and Prevention System (IDS/IPS)

The IDS/IPS is designed to detect and prevent cyber attacks by monitoring the network for malicious activity. It analyzes network packets and matches them against rulesets for known and emerging threats, such as viruses, worms, and other threats. The rulesets are curated by Talos, and the cloud will automatically keep the ruleset up-to-date.

IDS/IPS inspects all traffic between the LAN and Internet and all traffic between VLANs, but not traffic within the same VLAN. The mode can be set to **Disabled**, **Detection**, or **Prevention**. With prevention,

traffic is automatically blocked by best effort if it is detected as malicious based on the detection ruleset. It is recommended to enable IDS/IPS services. The ruleset can be set as **Connectivity**, **Balanced**, or **Security**, with **Balanced** being the default as it offers a compromise between security and performance. Select traffic categories and IP addresses/subnets can be configured to be bypassed when IDS/IPS or AMP is enabled (Trusted Traffic Exclusions). See Threat Protection for additional information.

In this design, intrusion prevention is enabled using the balanced ruleset and no traffic exclusions.

Advanced Malware Prevention (AMP)

AMP is an anti-malware technology which inspects HTTP file downloads and blocks or allows file downloads based on threat intelligence retrieved from the AMP cloud. It can be enabled or disabled and files and URLs can be specified in an allow list. It is recommended to have AMP enabled. Select traffic categories and IP addresses/subnets can be configured to be bypassed when IDS/IPS or AMP is enabled (Trusted Traffic Exclusions). See Advanced Malware Protection (AMP) for more information.

In this design, AMP is enabled with no traffic exclusions.

Content Filtering

Content filtering works by classifying URLs based on threat categories and web content curated by Talos. The router inspects the URL in the HTTP payload or the Server Name Indication field of the outbound TLS traffic. The records are used to query Talos for possible matches. Content filtering can only block domains when TLS/HTTPs is used. In the configuration, content and threat categories can be blocked, URL lists can be allowed or blocked, web searches can be blocked, and YouTube content can be restricted. See Content Filtering for more information.

In this design, several content and threat categories are blocked, along with an example URL.

Network Management Services

Network management services that are included in Unified Branch Release I are SNMP, Syslog, and NetFlow.

Simple Network Management Protocol (SNMP)

SNMP can be used for network configuration (SNMP queries) and/or for network monitoring (SNMP polling/queries or SNMP traps).

SNMP polling is supported, which can be used to query and gather information (read only access) either from the dashboard or directly from devices (routers, switches, and access points) within networks. SNMP traps are also supported from the dashboard. In this design, SNMP polling (dashboard and devices) and traps (dashboard) are enabled. The SNMP server is assumed to reside in the data center.

Dashboard Polling

SNMP access to the dashboard is enabled at the Organization level.

In the settings, SNMP v3 access should be enabled and SNMP v2 should be disabled. SNMP v2 sends the community string in clear text and therefore is not recommended to be used over an unsecure network such as the Internet. SNMP v3 is generally recommended since it includes provisions for privacy. Once SNMP v3 is enabled, the Authentication mode, Authentication password, Privacy mode, and Privacy password fields will appear. For the additional settings:

Authentication mode should be set to SHA (MD5 is weaker), and privacy mode to AS128 (DES is weaker). The authentication and privacy passwords should be strong passwords consisting of letters, numbers, and

special characters a minimum of 8 characters in length. For the IP restrictions section, it is highly recommended to limit SNMP access to the dashboard to the minimal set of IP addresses needed. For example, if the organization NATs all traffic bound for the Internet to the outside interface of a firewall, you may wish to restrict dashboard SNMP access to only that IP address. This will at least limit dashboard SNMP access to hosts within your organization so you can minimize the possibility of any data leakage out of your organization occurring through unauthorized access.

Note that for SNMP v3, the username is not a configurable parameter. You can find the hostname:port and user settings along with an SNMPwalk example under the **Privacy password** field in SNMP settings. A timeout value of 10 seconds is recommended to give the SNMP agent enough time to respond. For more details, review the SNMP Overview and Configuration document.

Dashboard Traps

SNMP traps allow for near real-time alerting of network events. SNMP traps are always forwarded from the cloud dashboard. SNMPv3 is used as best practice, so a username and passphrase are requested. SNMP traps use SHA1 for authentication and AES128 for privacy. The same passphrase is used for authentication and privacy. A public IP address must be used as the receiving server IP address since traps are generated from the dashboard. This may require port forwarding to be configured through the firewall as traffic needs to be initiated from the outside of the firewall.

To complete trap configuration, alerts should be chosen, and **SNMP** should be included as the default recipient under **Organization>Setting>Alerts**. This allows both email alerts and SNMP traps to be sent.

Device Polling

Individual devices can also be polled using SNMP, which is done at the network level. Just as in previous sections, SNMP v1/v2 or v3 can be enabled, but v3 is recommended. For v3, pick a username and passphrase and specify the privacy mode (AES128 is recommended). SHA1 is used for authentication, and the passphrase is used for both authentication and privacy.

Typically, the SNMP server sits in the data center. By default, the MX router denies SNMP packets that come from outside (non-local, non-VPN) networks. To enable communication, go to **Security & SD-WAN>Configure>Firewall>WAN appliance services** and configure the allowed remote IP addresses next to the SNMP server.

Syslog

The devices can send event logs to a syslog server. The router can be configured to send Wireless events, Air Marshal events, switch events, appliance events, security events, URLs, and flows. If URLs are configured, any HTTP get request generates a syslog entry. If flows are selected, then inbound and outbound flows that are matched against a firewall rule will generate a syslog message. Individual firewall rules can be enabled to generate syslog messages if configured under **Security & SD-WAN>Configure>Firewall**.

Figure 12. Enabling syslog messages for Firewall Flows

Syslog server configuration is under **Network-wide** settings. It allows you to configure a server address, port, and what event types to send messages for. This design leverages syslog.

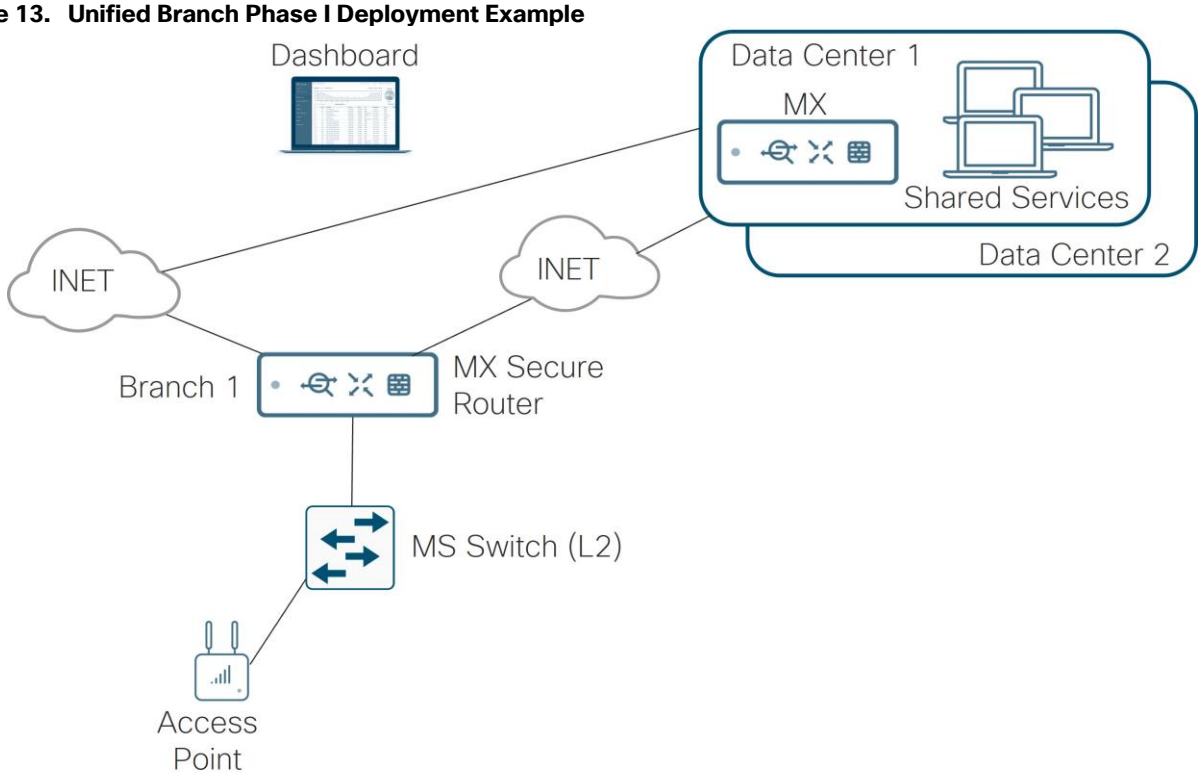
NetFlow

NetFlow is a monitoring tool that exports IP network traffic flow statistics where it can be analyzed by a NetFlow collector. NetFlow is supported on MX routers and 9300/X/L-Ms, and 9200/L-Ms. On the MX, NetFlow data is only exported for traffic that hits the CPU (traffic that is routed or NAT'ed). NetFlow version 9 is supported. This design leverages NetFlow.

Deployment Example

The following topology depicts a branch (Branch 1) composed of an MX secure router, an MS Layer-2 LAN switch, and an access point. There are two WAN interfaces, each connected to an Internet transport. Branch 1 is configured in a hub and spoke topology, with data center 1 as the primary hub and data center 2 as the secondary. The spoke receives a default route from the hubs for forwarding of Internet traffic with some exceptions. At the data center, multiple shared services exist, including DNS, DHCP, radius, and various management platforms for SNMP, syslog, and NetFlow. For SNMP, traps from the dashboard and polling to the dashboard and devices are implemented.

Figure 13. Unified Branch Phase I Deployment Example



See Appendix C to view the hardware models and code versions used in this example topology. New dashboard GUI versions were used wherever possible at the time of this writing (September 2025). Also, Appendix A reflects the dashboard and device settings that were used so the step-by-step and screenshots can be skipped if desired. Appendix B illustrates the ISE RADIUS configuration used in testing wired and wireless 802.1X for this example topology.

The following details further describe the network:

- The MX router for the hubs and branch are deployed in Routed mode.
- The following describes the six interface VLANs that are defined. The subnet structure is designed so global firewall rules can be minimized. DHCP can be local to the branch or relayed to the data center to a centralized DHCP server. The DNS server can be located on the Internet or at the data center. Some VLANs are not advertised across the auto VPN overlay (indicated by **Disabled** under the **VPN Mode** column).

VLANs	Subnet Structure	DHCP Location	DNS Location	VPN Mode
VLAN 1 (default)	192.168.128.0/24	Local	Internet (Use OpenDNS)	Disabled
VLAN 10 (DATA)	10.<VLAN#>.<SITE#>.0/24	Data Center	Data Center	Enabled
VLAN 20 (VOICE)	10.<VLAN#>.<SITE#>.0/24	Data Center	Data Center	Enabled
VLAN 30 (IOT)	10.<VLAN#>.<SITE#>.0/24	Data Center	Data Center	Enabled
VLAN 50 (Guest)	172.16.99.0/24	Local	Internet (Use OpenDNS)	Disabled
VLAN 999 (INFRA)	10.250.<SITE#>.0/24	Local	Data Center	Enabled

- VLAN 1 is used for initial onboarding to the dashboard, then all device management is switched to tagged VLAN 999 with unique addressing so this traffic can use the various services in the data center, such as radius, and syslog/NetFlow/SNMP services.
- In general, traffic from one VLAN cannot access another VLAN due to firewall rules. Exceptions are made for shared services (printer services within the branch and shared services within the data center). Guest and Default VLAN traffic and some traffic from the DATA and INFRA VLANs are permitted to go out Direct Internet Access (DIA).
- The WAN uplinks on the MX router are set to rate limit on the provider sub-line rate, and VPN tunnels are formed on both WAN transports. No load-balancing is done for Internet traffic. Internet break-out traffic is confined to Guest and default VLAN traffic, a few corporate SaaS applications, and dashboard traffic for the INFRA VLAN for downstream devices. All other traffic that is Internet-bound goes through the primary hub over the VPN Auto Tunnel before exiting to the Internet.
- Performance-based routing is enabled for corporate SaaS traffic using the Internet break-out, and VoIP and video conferencing, a custom critical application, and default traffic using the Auto VPN overlay.
- All trunk port connections in this example carry all VLANs, including the native VLAN 1. The MX router has one trunk connection to the switch, and all other ports are disabled. The switch has a trunk connection to the MX router and to the access point, which carries all VLANs, including the native VLAN 1. The access ports of the switch are configured for BPDU guard, storm control, and 802.1x/MAB.
- 802.1x enabled on the access ports of the switch leverage an ISE 3.4 server using RADIUS authentication and accounting. Single-Host mode is used. The policy type is hybrid authentication, meaning, if there is no authentication for 802.1x, Mac Authentication Bypass can be used instead. Voice authentication is also enabled. There is no access to the network if either 802.1x or MAB authentication fails. If authentication succeeds, a VLAN is passed back from the RADIUS server, putting the user into the DATA, VOICE, or IOT VLANs.
- For QoS on the switch, the Guest VLAN traffic DSCP is not trusted and set to DSCP 0. For other VLAN traffic, DSCP is trusted. On the MX router, default traffic rules are used, and rules are added to include guest traffic and custom critical application traffic.
- Wireless guest traffic is configured for Open authentication (no encryption), mandatory DHCP, and a click-through splash page which must be acknowledged before being allowed on the network. DHCP is performed by the MX router and traffic is tagged for the Guest VLAN (VLAN 50). Layer 2 LAN isolation is enabled so guest users cannot communicate with each other, and a per-client bandwidth and per-SSID bandwidth limit is enabled. SSID availability is scheduled according to a custom schedule. The Guest Wi-Fi uses 2.4 and 5 GHz bands and AI-RRM is enabled.
- Corporate Wi-Fi traffic is configured to use 802.1x Enterprise authentication with RADIUS (authentication and accounting). WPA3 transition mode is used, and fast roaming and protected management frames are enabled (Protected management frames allow unsupported clients). DHCP is performed by the MX

router and by default, traffic is tagged for the DATA VLAN, although the Override VLAN tag is enabled. RADIUS will respond back with a group policy name (Employees, Voice, or IOT) which has a VLAN set based on the identity of the user. SSID availability is scheduled according to a custom schedule. The Corp Wi-Fi uses 2.4, 5, and 6 GHz bands, Band steering, and AI-RRM is enabled.

- Wi-Fi 7 is not enabled yet for the Corporate Wi-Fi as it requires a separate access point from the guest Wi-Fi due to security requirements. Per-group SSID configuration is available starting in MR release 32.1.4, where Wi-Fi 7-compliant SSIDs can co-exist on the same AP as non-Wi-Fi 7-compliant SSIDs as long as they are in separate SSID groups. See WPA3_Encryption and Configuration Guide for additional information.

For this deployment, the following steps are discussed:

- Complete the prerequisites
- Create a new network
- Configure the devices
- Onboard the devices/Verify device operation
- Complete device configurations

Once the devices are onboarded and verified, configuration templates can be created then modified from a configured network which can then be used to quickly deploy additional branches. See Managing Multiple Networks with Configuration Templates for more details.

Complete the Prerequisites

There are several prerequisites that need to be addressed before template creation and onboarding can begin.

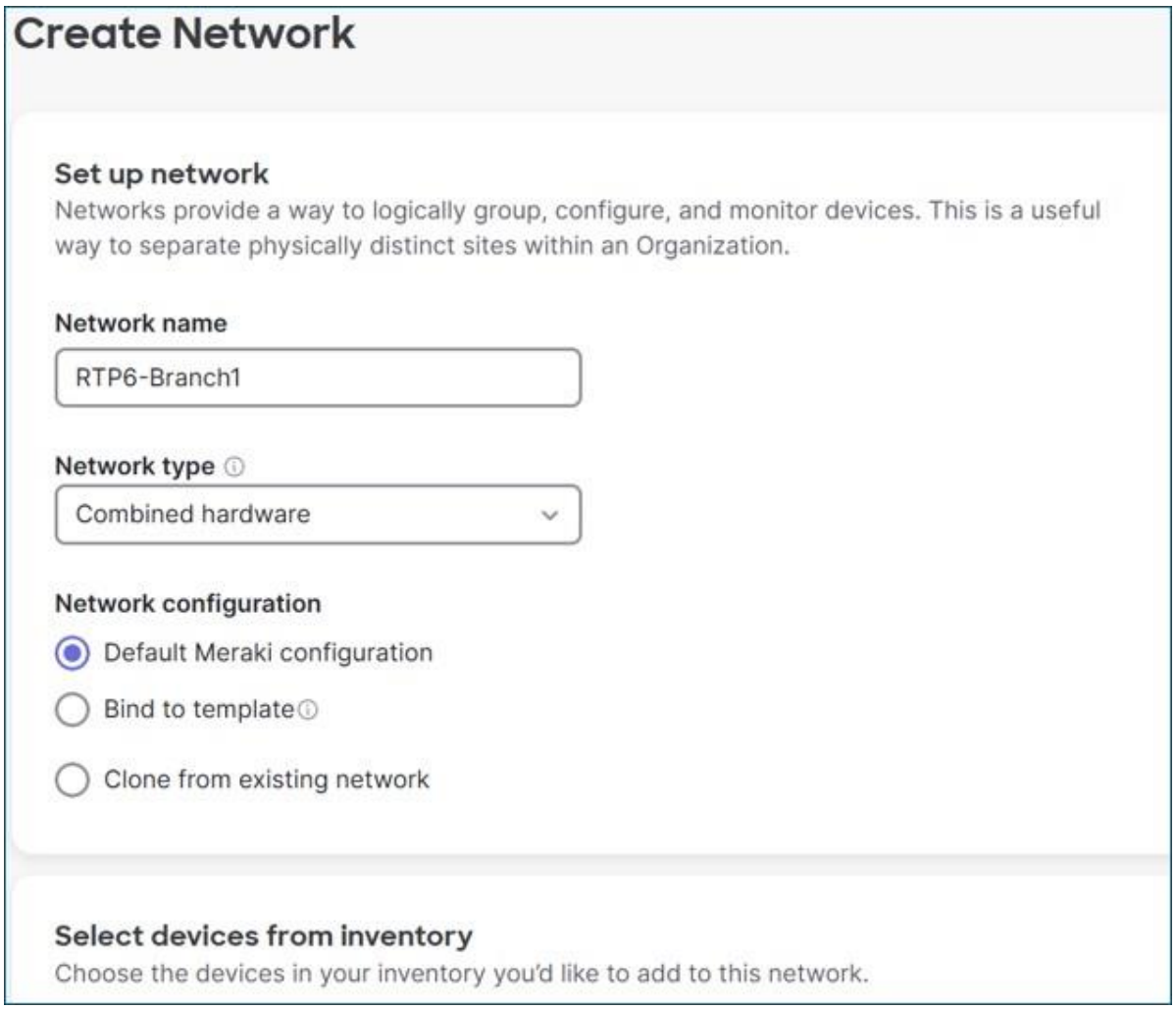
- All configurations can be performed on the Meraki cloud dashboard. Devices should have connectivity to the Internet to connect to the Meraki cloud. Device onboarding is simplified if the provider provides an IP address, gateway, and DNS information through DHCP to the WAN uplink on the MX router, as device registration to the dashboard is automatic. In addition, it is important to ensure that if there are any firewalls upstream from the router, the proper rules are configured so the device can reach the proper cloud services. See Upstream Firewall Rules for Cloud Connectivity for details on what IP addresses and ports need to be allowed.
- Ensure a Meraki dashboard account and Organization is created. The organization is created at the same time as the account. From the account, organizations, networks, and devices are managed. An organization is made up of multiple networks, and each network is made up of one or more devices. A network typically correlates to a physical location. See Creating a Dashboard Account and Organization for more information.
- Ensure the devices to be managed are added in the Organization inventory on the dashboard (**Organization>Configure>Inventory**). They can be entered using an order number or serial number.
- Ensure the required licenses are added to the dashboard. License status can be found on the **Organization>Configure>License Info** page on the dashboard. Licenses are added automatically if they are part of an order number that was entered in the Inventory page, otherwise, they can be added manually using a Claim Key if the order number is not known or the license is ordered separately from the devices.

For more detailed information, review the Getting Started Checklist.

Create a New Network

On the dashboard, go to **Organization>Configure>Create Network**. In the text box, type the **Network name** (RTP6-Branch1) and specify the **Network type** (if needed) from the drop-down box (Combined

hardware). This network will use the **Default Meraki configuration** before additional configurations are added. Select the devices from inventory which should be included in the network (these should have been added during the prerequisite steps). Select **Create network**.



The dashboard switches to the newly created network.

Configure the Devices

The devices can be pre-configured before onboarding. The following sequence creates a majority of the configuration before onboarding and leaves some port-level configuration until after onboarding. From the RTP6-Branch1 network, the MX router, switch, and AP are configured.

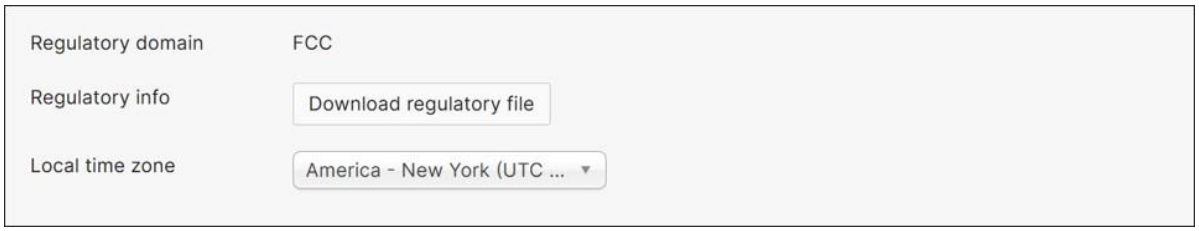
Name the Devices

By default, the MX, switch, and AP devices are named by their mac-addresses. To give them more user-friendly names:

- MX: Go to **Security & SD-WAN>Monitor>Appliance Status**, click edit next to the mac address in the top left corner, and fill in the **Appliance name** (RTP6-Branch1-MX). Click **Save**.
- Switch: Go to **Switching>Monitor>Switches**, choose the switch mac address to view, click edit next to the mac address in the top left corner, and fill in the **Switch name** (RTP6-Branch1-SW1). Click **Save**.
- AP: Go to **Wireless>Monitor>Access Points**, choose the AP mac address to view, click edit next to the mac address in the top left corner, and fill in the **Access point name** (RTP6-Branch1-AP1). Click **Save**.

Network-wide: Configure Time Zone

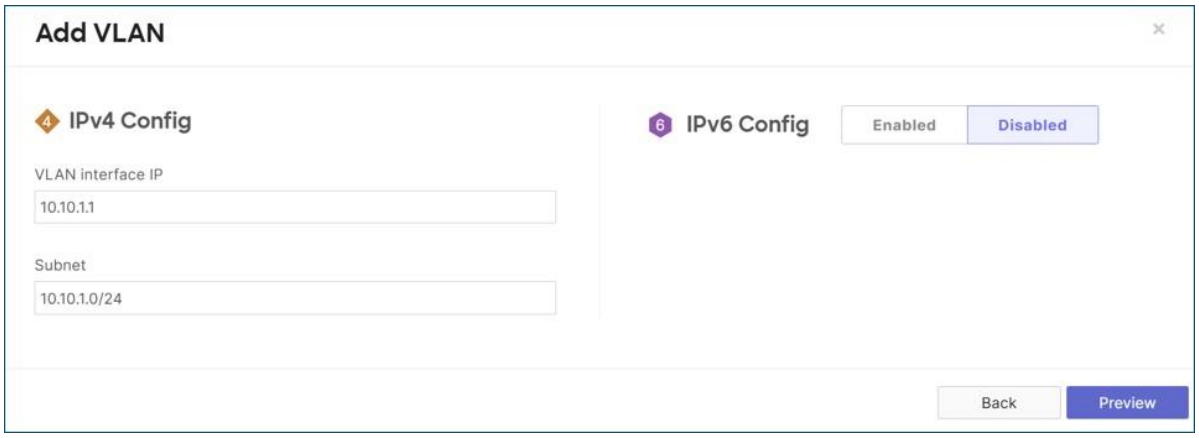
Time zone is used for time-sensitive features such as SSID Availability or Port Scheduling. In this example, it is used to set the schedule for SSID availability. Go to **Network-wide>Configure>General**. Next to **Local time zone**, select the appropriate time zone from the drop-down box if it's not already configured. In this example, America – New York (UTC -4.0, DST) is selected. Click **Save** or **Save Changes**.



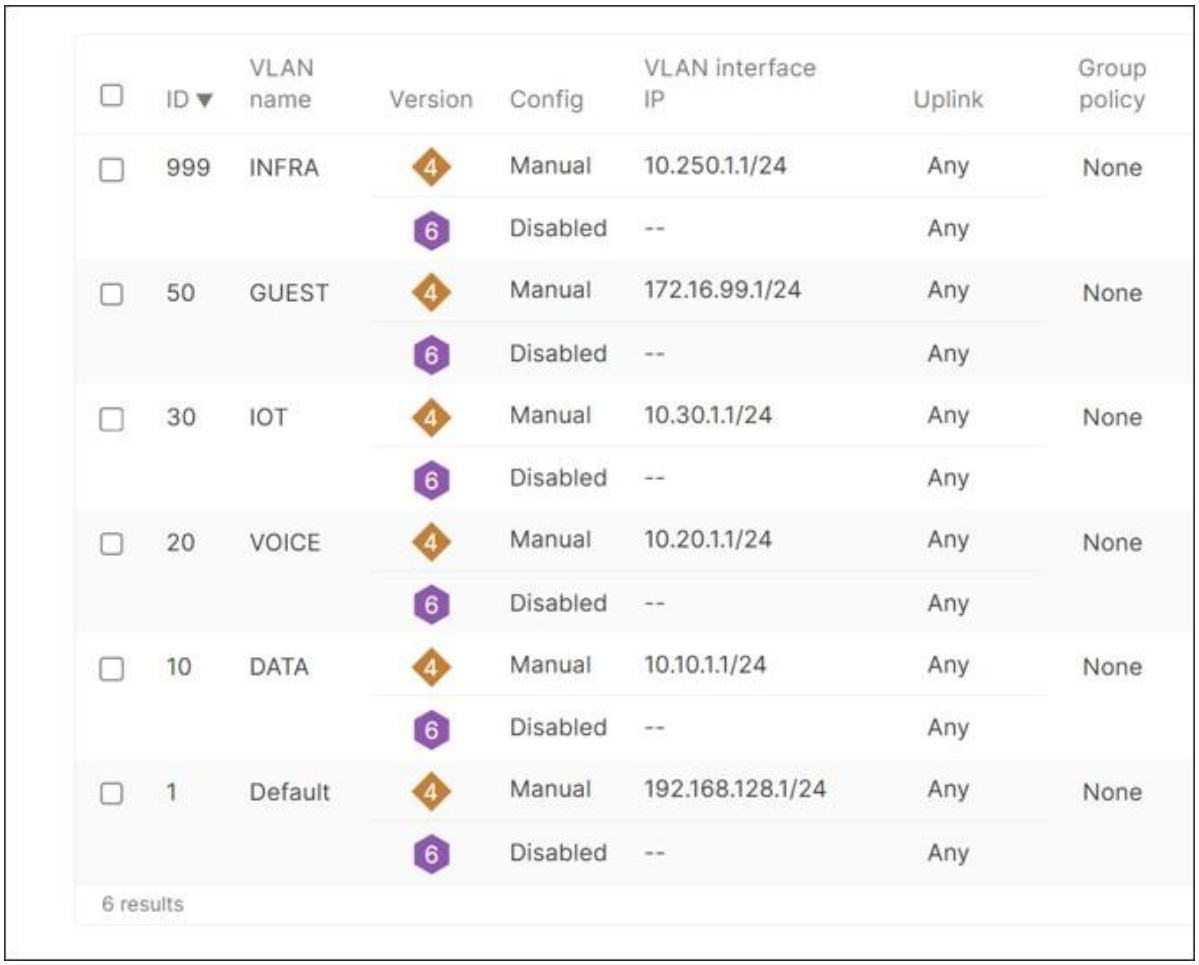
MX Secure Router: Configure VLAN Interfaces

Under **Security & SD-WAN>Configure>Addressing & VLANs>Routing>LAN setting**, select **VLANs**. VLAN 1 is automatically created with a VLAN interface IP of 192.168.128.1/24. In the **Subnets** section, click **Add VLAN**. Enter **VLAN name** (DATA) and **VLAN ID** (10). Click **Next**.

Under **Add VLAN>IPv4 Config>VLAN interface IP**, enter the IP address of the MX gateway for VLAN 10 (DATA) (10.10.1.1). This is in the form 10.<VLAN#><SITE#>.1 so global firewall rules for site-to-site VPNs can be efficiently applied. Under **Subnet**, the VLAN subnet is specified (10.10.1.0/24). Next to **IPv6 Config**, **Disabled** has been selected for this VLAN. Click **Preview**, then **Update**.



Repeat the steps to add additional VLANs for 20 (VOICE), 30 (IOT), 50 (GUEST), and INFRA (999). VLAN 1 interface IP address is left at default (192.168.128.1) and VLAN 999 (INFRA) interface IP address is configured as 10.250.<site#>.1. VLANs 10, 20, 30 interface IPs follow the scheme 10.<VLAN#><Site#>.1. All subnets are /24 masks. All guest traffic on all branches will share the same subnet (172.16.99.0/24).



ID	VLAN name	Version	Config	VLAN interface IP	Uplink	Group policy
999	INFRA	4	Manual	10.250.1.1/24	Any	None
		6	Disabled	--	Any	
50	GUEST	4	Manual	172.16.99.1/24	Any	None
		6	Disabled	--	Any	
30	IOT	4	Manual	10.30.1.1/24	Any	None
		6	Disabled	--	Any	
20	VOICE	4	Manual	10.20.1.1/24	Any	None
		6	Disabled	--	Any	
10	DATA	4	Manual	10.10.1.1/24	Any	None
		6	Disabled	--	Any	
1	Default	4	Manual	192.168.128.1/24	Any	None
		6	Disabled	--	Any	

6 results

Click **Save**.

MX Secure Router: Configure DHCP

In this network, the Default, INFRA, and GUEST VLANs use local DHCP pools, while the other subnets use DHCP services in the data center. INFRA devices use reserved IP addresses from the DHCP pool. All DHCP

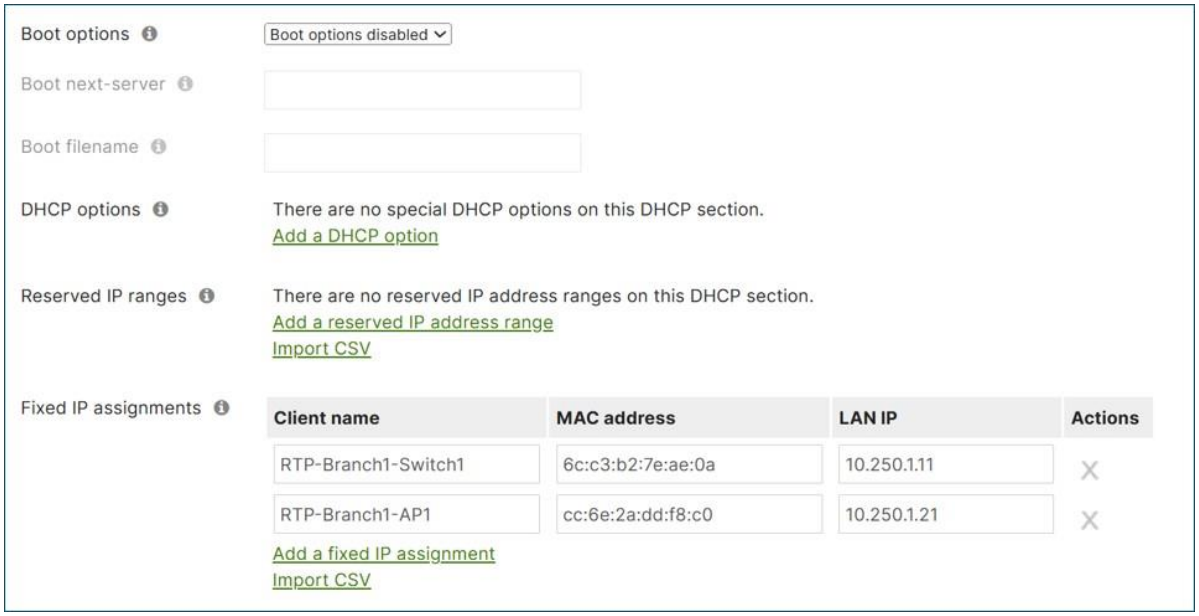
pools are local by default and proxy to an upstream DNS, which is out on the Internet transport. Only GUEST and Default VLANs should use an Internet DNS server (OpenDNS), while everything else uses DNS services in the data center.

Before configuring this section, gather the mac addresses from any switches and access points so the Management IP addresses can be reserved from the DHCP pools.

Device	Dashboard Location	Mac Address
RTP6-Branch1-SW1	Switching>Monitor>Switches>MAC address	6c:c3:b2:7e:ae:0a
RTP6-Branch1-AP1	Wireless>Monitor>Access Points>MAC address	cc:6e:2a:dd:f8:c0

Go to **Security & SD-WAN>Configure>DHCP** and under **VLAN 999 (INFRA)** next to **DNS nameservers**, select **Specify nameservers.** Next to **Custom nameservers**, type in the DNS servers at the data center (10.102.1.160 and 10.102.1.161 in this example).

Next to **Fixed IP assignments**, click **Add a fixed IP assignment**. Enter a name for the device, the mac address, and what LAN IP address is to be assigned. Repeat for all devices.

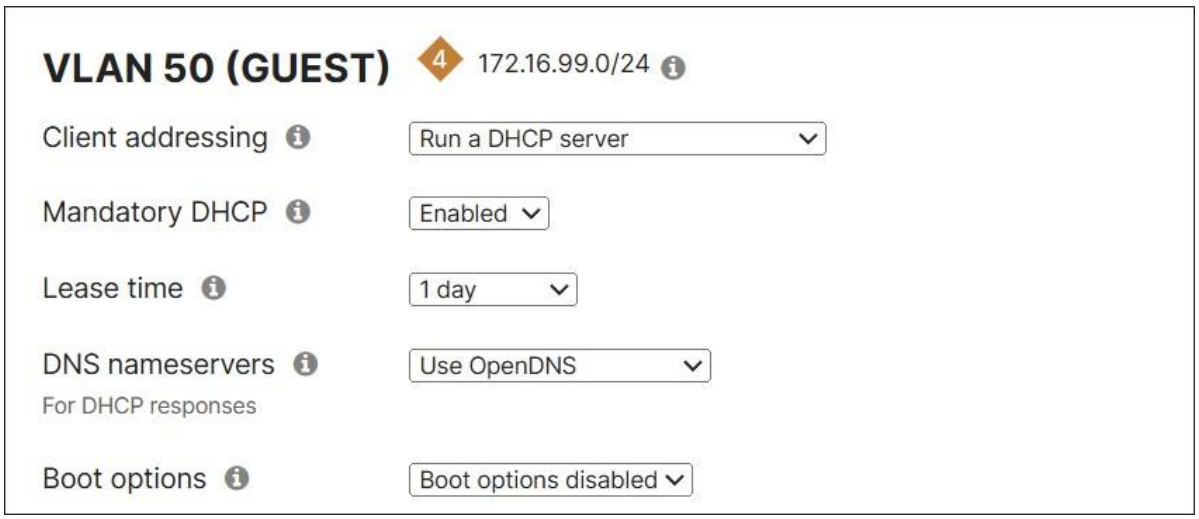


Click **Save Changes** at the bottom of the page.

For VLANs 10, 20, and 30, next to **Client addressing**, select **Relay DHCP to another server** and next to **DHCP server IPs**, type in the data center DHCP servers (10.102.1.160 and 10.102.1.161 in this example). Click **Save** or **Save Changes**.

Note: The DHCP relay IP address must be in a subnet connected to the network or on a subnet reachable through the site-to-site VPN (not through the default route). In the example data center, there is a static route defined to reach the DC services network, and that static route is in VPN mode so it can be advertised to other Auto VPN members.

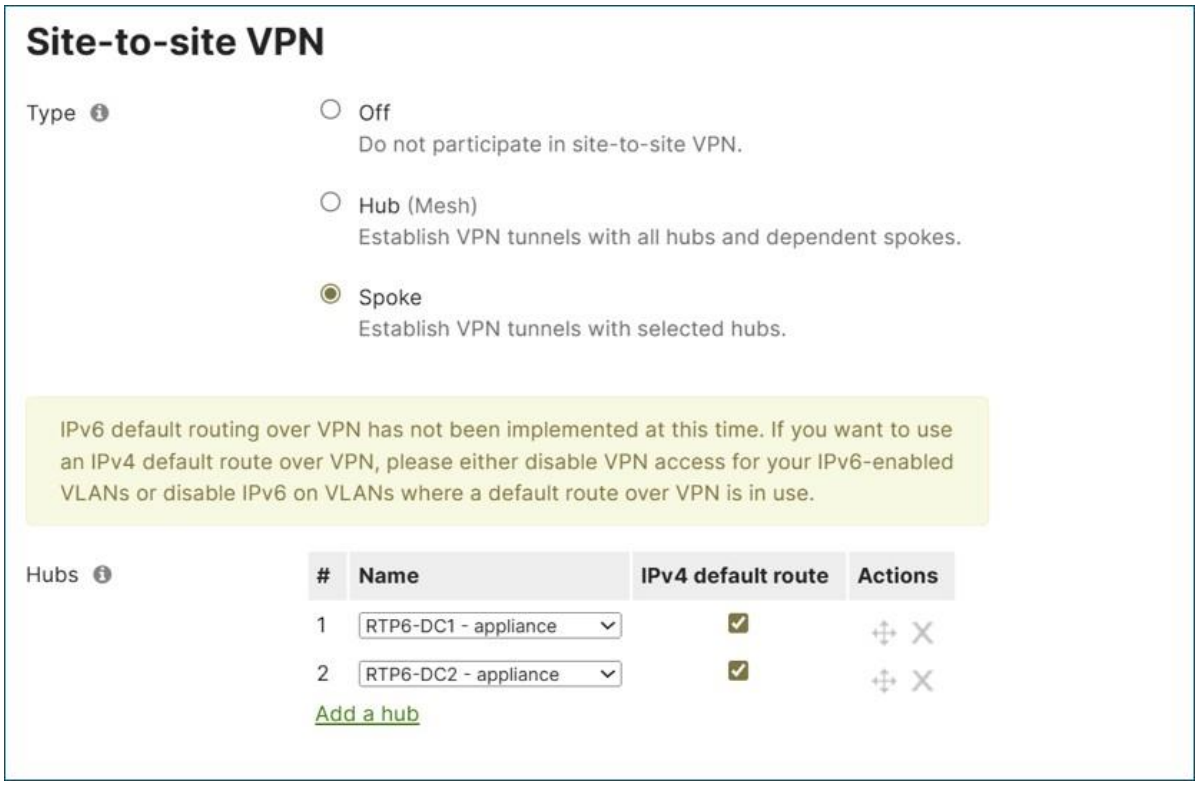
For the GUEST VLAN (50) and Default VLAN (1), next to Mandatory DHCP, select **Enabled** from the drop-down box. Next to DNS nameservers, select Use OpenDNS from the drop-down box. Click **Save** or **Save Changes**.



MX Secure Router: Configure Site-to-Site VPNs and Data Center Default Route

Under **Security & SD-WAN>Configure>Site-to-site VPN**, next to **Type**, select **Spoke**. Next to **Hubs**, click **Add a hub** and select the primary hub (RTP6-DC1 – appliance in this example). Click **Add a hub** and select the secondary hub (RTP6-DC2 – appliance in this example). Since DC1 was selected first, this prioritizes DC1 as the primary hub, so if routes are equal, DC1 is selected to route the traffic.

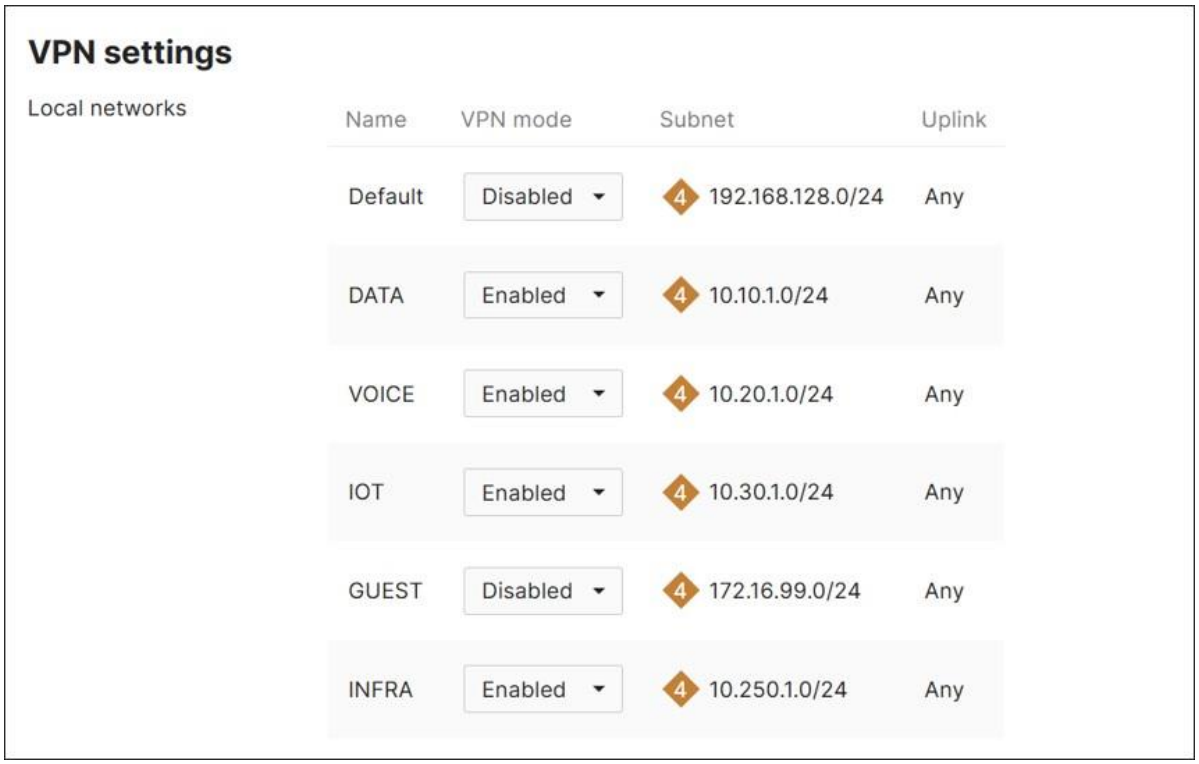
Under **IPv4 default route**, select checkboxes next to both hubs since both can route default traffic. Click **Save** or **Save Changes**.



MX Router: Configure VPN Settings for VLANs

By default, subnets are not advertised to other sites through the VPN registry. Under **Security & SD-WAN>Configure>Site-to-site VPN**, under **VPN settings>Local networks**, choose **Enabled** under **VPN**

mode for DATA, VOICE, IOT, and INFRA so these networks can be advertised. Click **Save** or **Save Changes**.

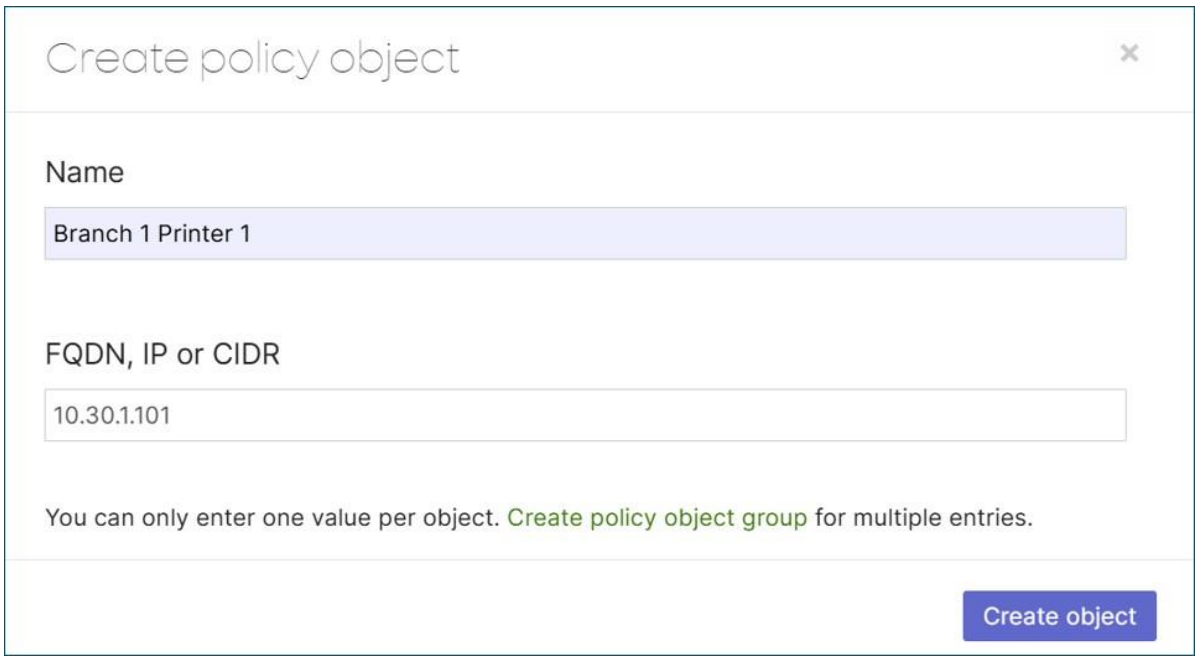


MX Secure Router: Configure Firewall Rules

Firewall rules apply to LAN traffic as well as Internet traffic. It does not apply to VPN site-to-site traffic. The following policy is implemented:

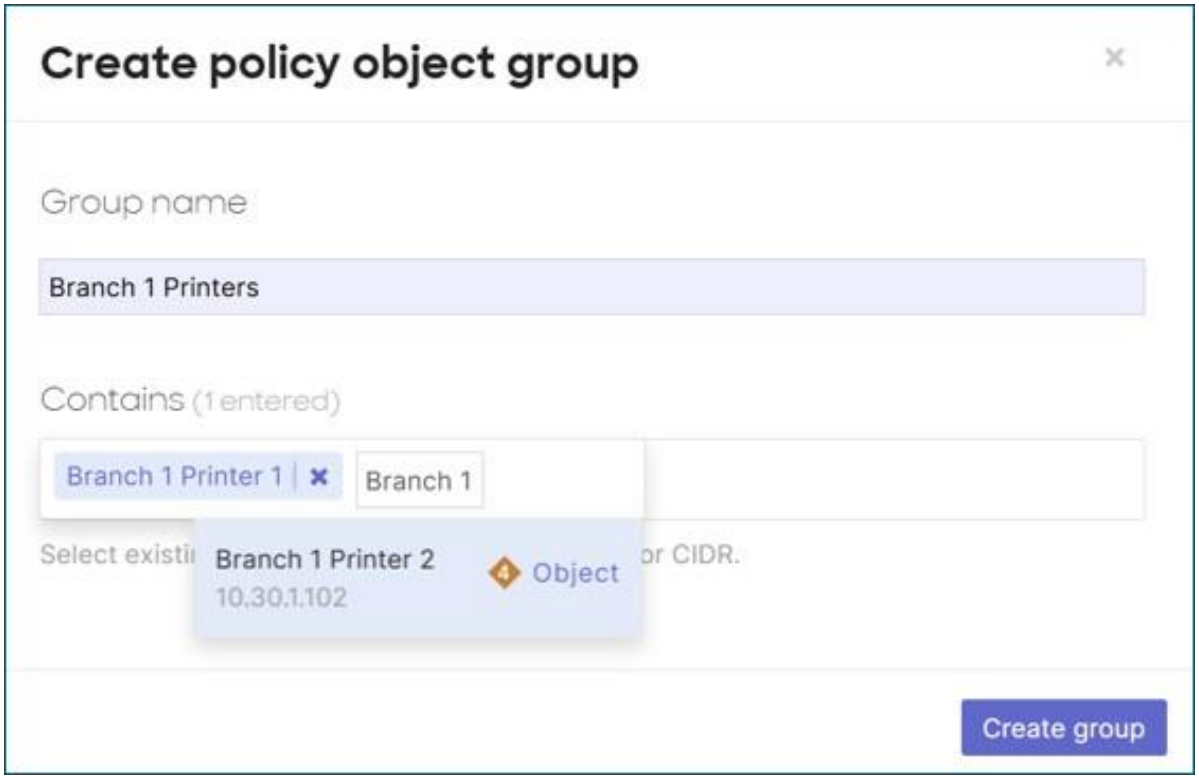
- Allow Data VLAN to access local Printers (10.30.1.101 and 10.30.1.102) on the IOT VLAN. The Layer 3 firewall rules are stateful, so traffic in the opposite direction is allowed back through.
- Allow Direct Internet Access (DIA) for Default, INFRA, DATA, and GUEST VLANs.
- Deny everything else. This does not affect VPN site-to-site traffic, which is governed by site-to-site VPN firewall rules. This means that all VLAN-to-VLAN layer 3 traffic will be blocked and IOT and VOICE VLANs will be denied DIA as well.

First, a policy object is created. Go to **Organization>Configure>Policy Objects**. Under the **All objects** tab, click **Add new**. Under **Name**, type in a name (Branch 1 Printer 1 in this example) and under **FQDN, IP or CIDR**, add an IP host (10.30.1.101 in this example). Click **Create object**.



Repeat the steps for Branch 1 Printer 2 (10.20.1.102).

A policy object group can be created from the newly created objects. From **Organization>Configure>Policy Objects** under the **Groups** tab, click **Add new**. Under **Group name**, type Branch 1 Printers, then under **Contains**, type Branch 1, and from the drop-down box, select the Branch 1 Printer 1 object. Then add the Branch 1 Printer 2 object. Click **Create group**.

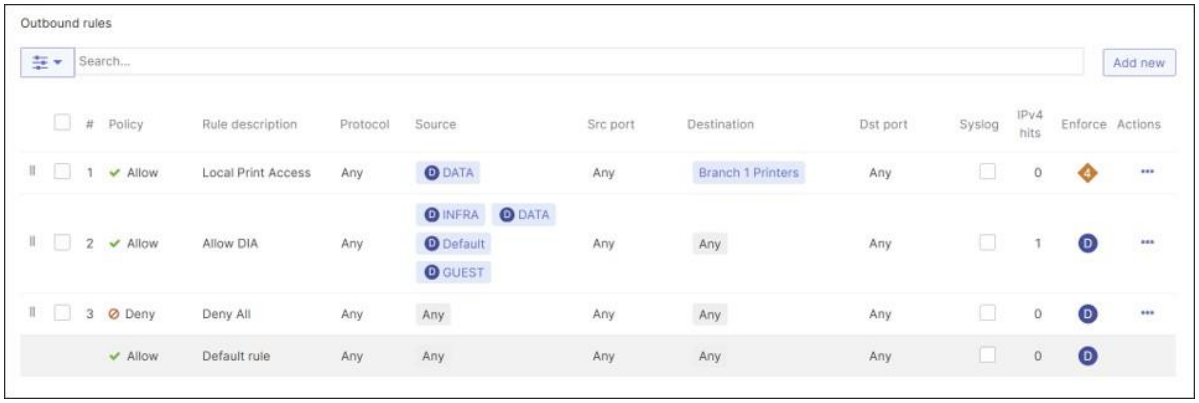


The Network object group is updated. Select **Close** on the pop-up window.

Select **Security & SD-WAN>Configure>Firewall** and under **Layer 3>Outbound rules**, click **Add new**. Fill out the parameters and click **Add new** to add the next rule as shown in the table below.

Policy	Rule Description	Protocol	Source	Src Port	Destination	Dst Port
Allow	Local Print Access	Any	DATA VLAN	Any	Branch 1 Printers (Object group)	Any
Allow	Allow DIA	Any	Default VLAN/INFRA VLAN/DATA VLAN/GUEST VLAN	Any	Any	Any
Deny	Deny All	Any	Any	Any	Any	Any
Allow	Default rule	Any	Any	Any	Any	Any

Once complete, click **Finish editing**, then **Save** or **Save Changes**.



MX Secure Router: Configure VPN Site-to-Site Outbound Firewall Rules

The VPN site-to-site outbound firewall rules apply to outbound VPN traffic destined to other VPN-connected sites and is applied at an organization level, meaning, these same rules apply to every MX router in the organization with site-to-site VPN enabled. This is important as it influences the way the rules should be crafted. In the example network, the network scheme is 10.<vlan#><site#>.0/24 so firewall rules could be applied more easily at the organizational level. The Data VLAN across the organization is represented by the subnet 10.10.0.0/16 instead of a list of disjointed 10.x networks.

While the L3 firewall rules on the device can reference VLANs inside the rules, the site-to-site VPN firewall rules do not. Only policy objects, policy object groups, IPv4/v6 addresses, or subnets can be referenced. The following policy is implemented:

- Allow the Data, IOT, Voice, and Infra subnets in any branch to reach Corporate shared services (DHCP, DNS, Radius, SNMP, and Management) and allow Corporate shared services to reach the Data, IOT, Voice, and Infra subnets in any branch.
- Deny access from Data, IOT, Voice, and Infra subnets to other subnets in other sites. Meaning, Data subnets cannot reach IOT, Voice, and Infra subnets, etc.
- Allow everything else. This is the default rule and allows Data subnets to reach other Data subnets as well as the Internet through the hub. Voice subnets can reach other voice subnets as well as the Internet through the hub, etc.

Note that Guest and Default traffic do not traverse the VPN overlay due to VPN mode being disabled for these VLANs. They can be included in the rule as “Deny Guest subnet or Default subnet to Any” and “Deny

Any to Guest subnet or Default subnet" if desired, in the event the Guest or Default VLAN's VPN mode is enabled, and a unique subnet is configured.

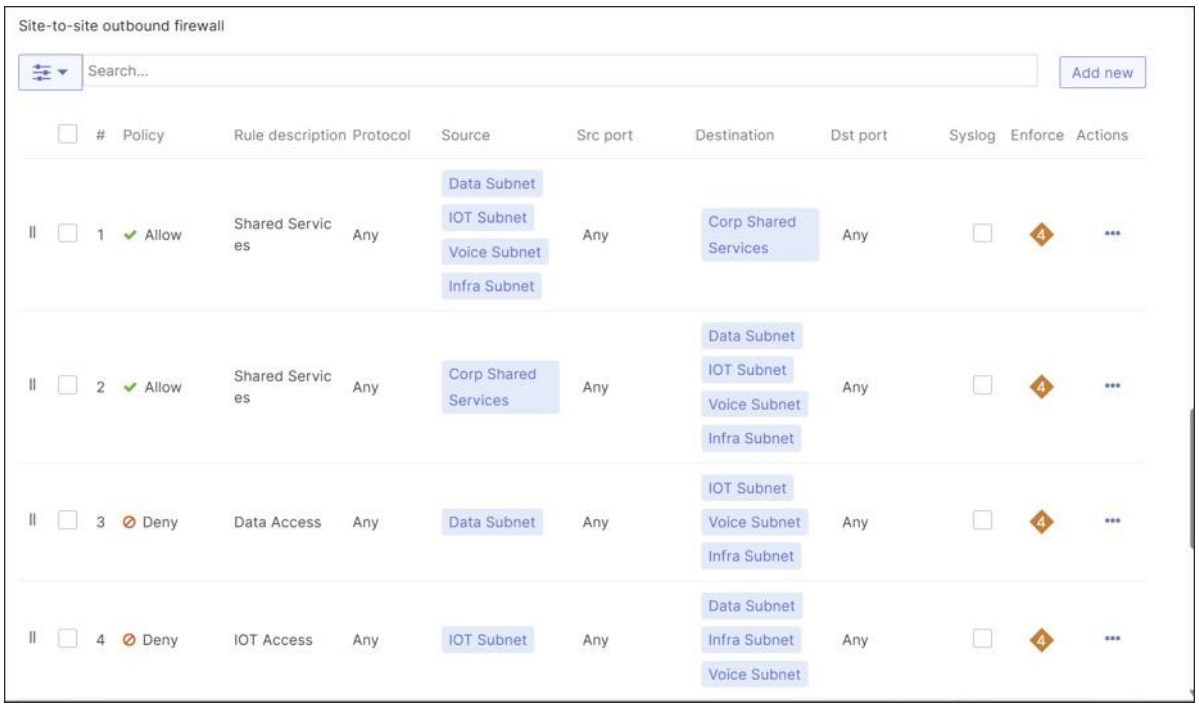
Go to **Organization>Configure>Policy Objects** and create the following objects and object group. Note that objects within policy groups can be created before the policy group object is created or after the policy group object is defined.

Object or Object Group	Name	Type	Value
Object	Corp DNS-DHCP	CIDR	10.102.1.160
Object	Corp Mgt	CIDR	10.102.1.160
Object	Corp Radius	CIDR	10.102.1.160
Object	Data Subnet	CIDR	10.10.0.0/16
Object	Voice Subnet	CIDR	10.20.0.0/16
Object	IOT Subnet	CIDR	10.30.0.0/16
Object	Infra Subnet	CIDR	10.250.0.0/16
Object Group	Corp Shared Services	--	Corp DNS-DHCP/Corp Mgt/Corp Radius

Go to **Security & SD-WAN>Configure>Site-to-Site VPN**. Under **Site-to-site outbound firewall**, configure the following:

Policy	Rule Description	Protocol	Source	Src Port	Destination	Dst Port
Allow	Shared Services	Any	Data Subnet/IOT Subnet/Voice Subnet/Infra Subnet (Objects)	Any	Corp Shared Services (Object group)	Any
Allow	Shared Services	Any	Corp Shared Services (Object group)	Any	Data Subnet/IOT Subnet/Voice Subnet/Infra Subnet (Objects)	Any
Deny	Data Access	Any	Data Subnet (Object)	Any	Voice Subnet/IOT Subnet/Infra Subnet (Objects)	Any
Deny	Voice Access	Any	Voice Subnet (Object)	Any	Data Subnet/IOT Subnet/Infra Subnet (Objects)	Any
Deny	IOT Access	Any	IOT Subnet (Object)	Any	Data Subnet/Voice Subnet/Infra Subnet (Objects)	Any
Deny	Infra Access	Any	Infra Subnet (Object)	Any	Data Subnet/Voice Subnet/Infra Subnet (Objects)	Any
Allow	Default Rule	Any	Any	Any	Any	Any

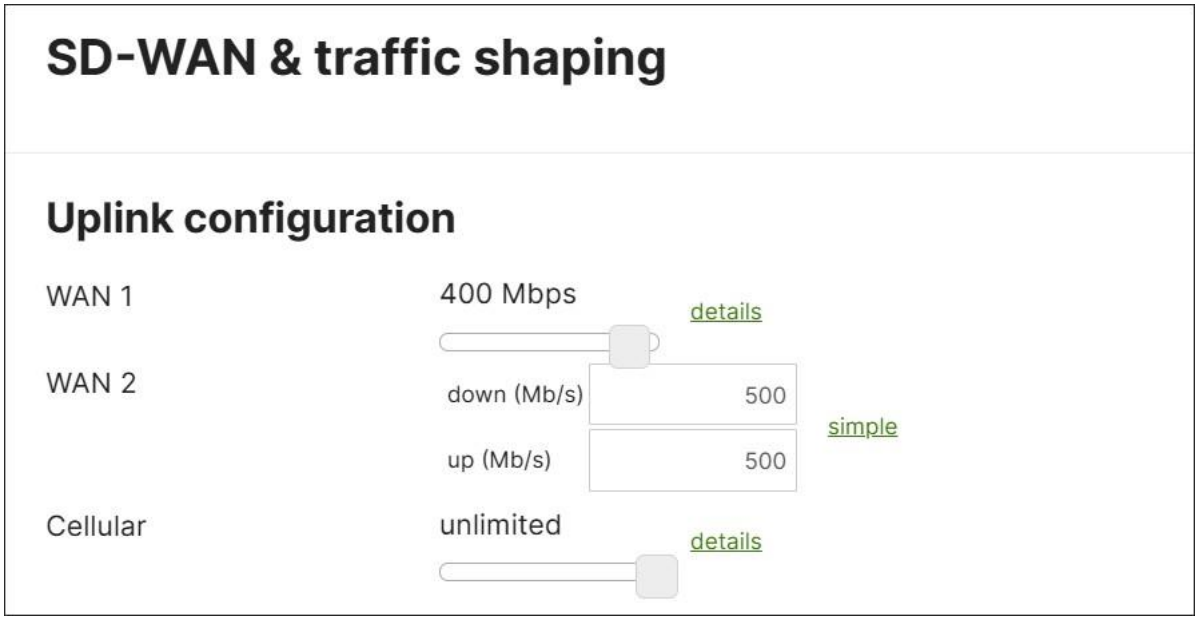
Click **Save Changes**.



MX Secure Router: Configure SD-WAN & Traffic Shaping

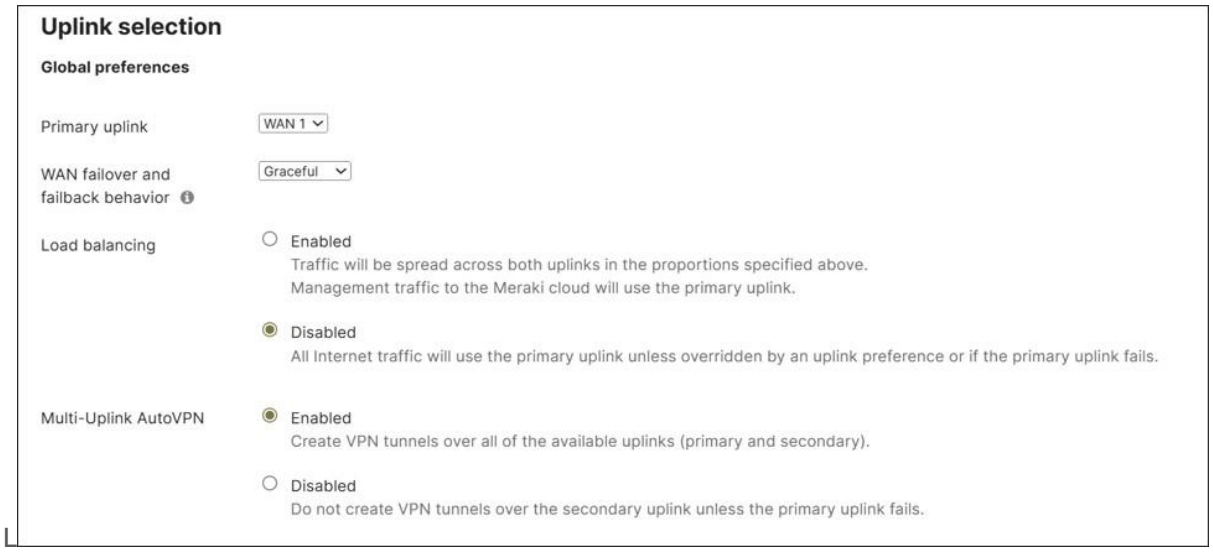
Uplink Configuration

In this example, rate limiting is set on each WAN link to match the provider's service sub-line rate. Go to **Security & SD-WAN>Configure>SD-WAN & Traffic Shaping**. Under **Uplink configuration**, set **WAN 1** to 400 Mbps and **WAN 2** to 500 down (Mb/s) and 500 up (Mb/s) in this example.



In this example, the **Primary uplink** is kept as **WAN 1** (default). There is also no **Load balancing** enabled for Internet traffic. Most Internet traffic takes the tunnel to the primary hub. Guest traffic, Data/Corporate SaaS traffic (O365 and Webex), device dashboard INFRA traffic, and Default traffic (if any) takes the direct Internet access from the branch.

In addition, VPN tunnels are created over both available uplinks (**Multi-Uplink AutoVPN** is Enabled).



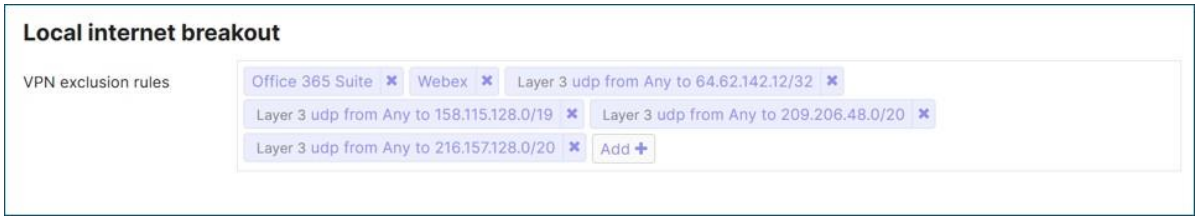
Local Internet Breakout

Because default routes are pointing to the hubs, the site is assumed to be in full-tunnel mode. This means that all Internet traffic is sent through the hub. The exception is Guest (and Default VLAN) traffic because their VPN mode is set to disabled and Internet access for these VLANs is allowed as a rule in the L3 firewall. To break out traffic for DIA, VPN exclusions first need to be configured. In this example, SaaS application (Office 365 and Webex) traffic from the Corporate/Data VLAN need to be broken out, as well as dashboard INFRA VLAN traffic for the switch and AP control planes.

Go to **Security & SD-WAN>Configure>SD-WAN & Traffic Shaping** and under **Local internet breakout** next to **VPN exclusion rules**, click the **Add +** button, select **Major applications** and choose **Office 365 Suite** and **Webex**. Under **Custom expressions**, specify the **Protocol**, **Destination**, and **Dst port**, then click **Add expression**. Use the following custom expressions to allow dashboard cloud communication and VPN registry traffic. Any is used for the destination port since only one port, or **Any** can be specified per custom expression. See [Upstream Firewall Rules for Cloud Connectivity] for latest, up-to-date port requirements for the dashboard.

Protocol	Destination	Dst Port
UDP	64.62.142.12/32	Any
UDP	158.115.128.0/19	Any
UDP	209.206.48.0/20	Any
UDP	216.157.128.0/20	Any

Click **Save** or **Save Changes**.



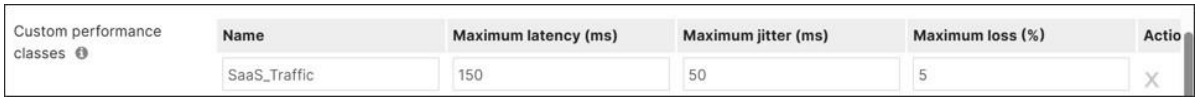
SD-WAN Policies: Internet

In this part of the configuration, traffic steering and performance-based routing policies are configured. The first section applies to Internet traffic only. Because no load-balancing is configured, traffic chooses the primary uplink (WAN 1 in this case) unless there is a policy to steer it differently. In this example, the following policies are desired:

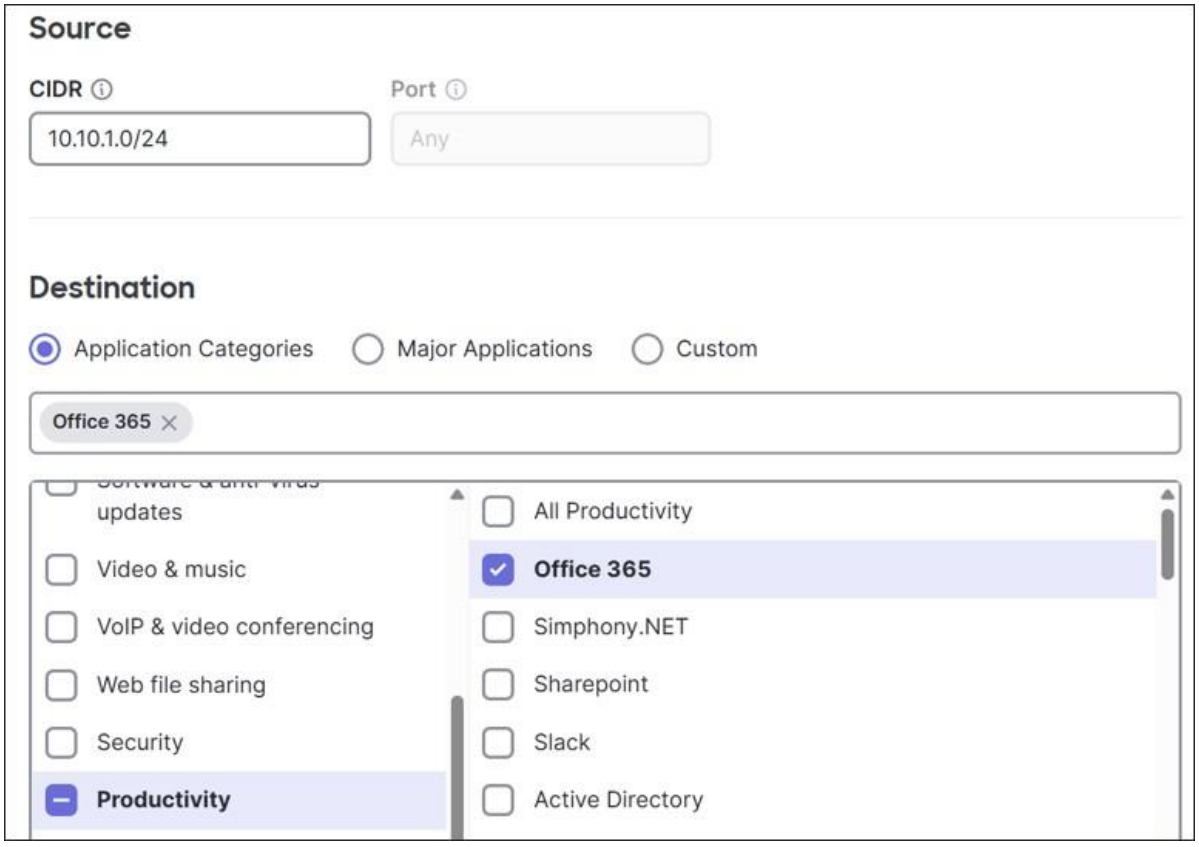
- Guest traffic is directed over WAN 1. If the link is declared down, the traffic is redirected to WAN 2.
- SaaS Traffic is directed over WAN 2 and should be redirected to WAN 1 if performance is poor.
- Device dashboard traffic is directed over WAN 2. If the link is declared down, the traffic is redirected to WAN 1.

Guest traffic doesn't need to be included in the policy since this is the default behavior when no load-balancing is chosen and the primary uplink is WAN 1.

A custom performance class for SaaS traffic should be configured before configuring the policy. Go to **Security & SD-WAN>Configure>SD-WAN & Traffic Shaping** and under **SD-WAN policies** and **Custom performance classes**, select **Create a new custom performance class**. Fill in the **Name** (SaaS_Traffic), **Maximum latency (ms)** (150), **Maximum jitter (ms)** (50), and **Maximum loss (%)** (5). Click **Save** or **Save Changes**.



Under **SD-WAN Policies>Internet Traffic**, click **+ Add policy**, specify the **Protocol**, **Source CIDR**, **Destination**, and **Uplink Selection**. Click **Save** to Add the policy to the dashboard. Repeat to add additional lines of policy.



The following two uplink selection policies are configured in this example:

Protocol	Source	Destination Type	Value	Preferred Uplink	Fail Over If:	Performance Class:
Any	10.10.1.0/24	Application Categories	Productivity>Office 365 VoIP & video conferencing>Webex	WAN 2	Poor performance	SaaS_Traffic
Any	10.250.1.0/24	Custom	CIDR=Any	WAN 2	Uplink Down	N/A

Note that dashboard destination traffic is Any. The VPN exclusions already defined what specific destination traffic is DIA (dashboard IP address destinations). Click **Save** or **Save Changes**.

SD-WAN Policies: VPN Traffic

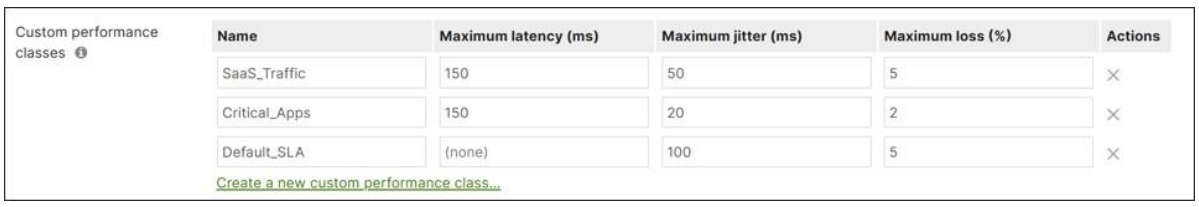
In this part of the configuration, traffic steering and performance-based routing policies are configured for VPN traffic. Load-balancing doesn't apply to VPN traffic, so VPN traffic always chooses the primary link (WAN 1 in this case) unless there is a policy to steer it differently. In this example, the following policies are desired:

- All VoIP and Video Conferencing traffic is directed over WAN 2 and should be redirected to WAN 1 if performance is poor.
- A critical company application (TCP from Any to 10.102.1.161/32:443) is directed over WAN 2 and should be redirected to WAN 1 if performance is poor.
- All other traffic is directed over WAN 1 and should be redirected to WAN 2 if performance is poor.

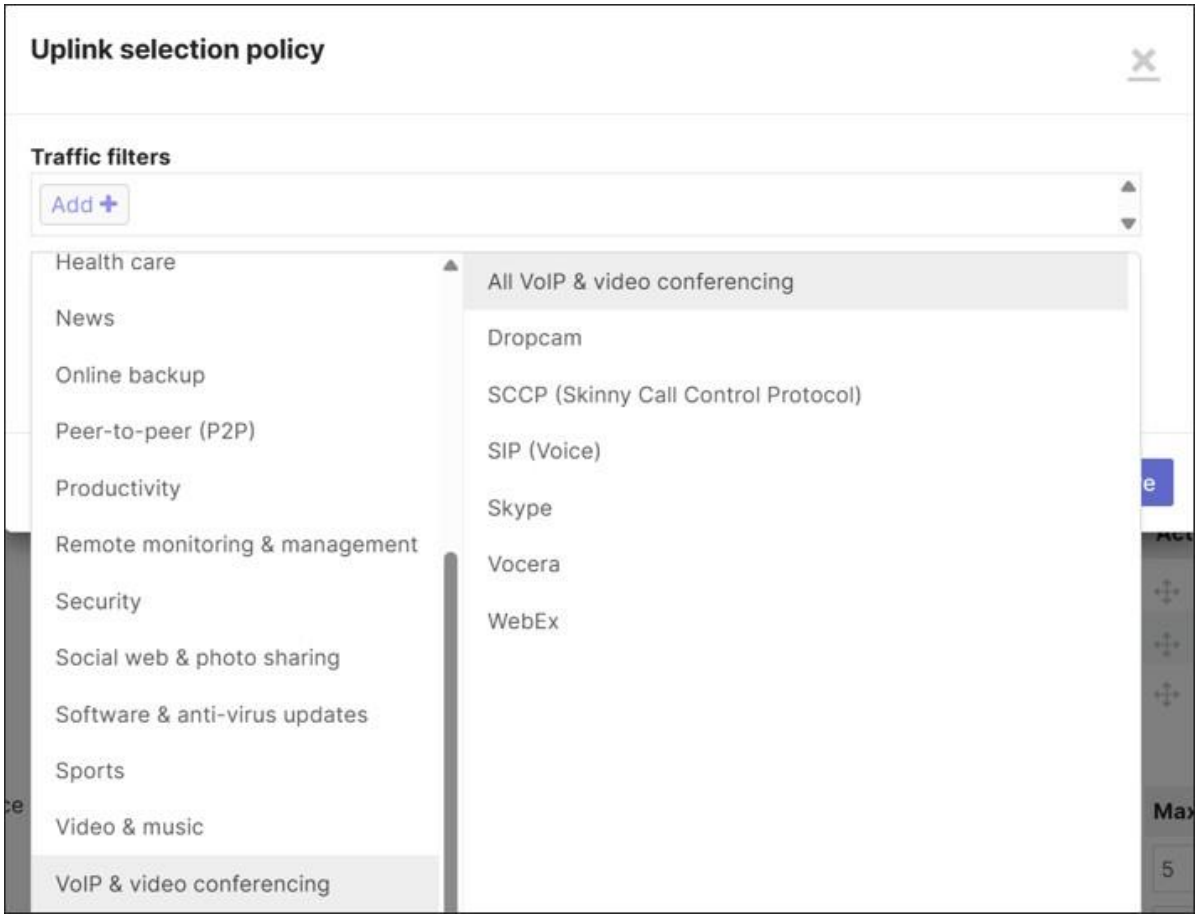
Custom performance classes for the critical application traffic and default traffic should be configured before configuring the policy. Go to **Security & SD-WAN>Configure>SD-WAN & Traffic Shaping**, then under **SD-WAN policies** and **Custom performance classes**, select **Create a new custom performance class**. Fill in the **Name** (Critical_Apps), **Maximum latency (ms)** (150), **Maximum jitter (ms)** (20), and **Maximum loss (%)** (2).

Select **Create a new custom performance class**. Fill in the **Name** (Default_SLA), **Maximum jitter (ms)** (100), and **Maximum loss (%)** (5).

Click **Save** or **Save Changes**.



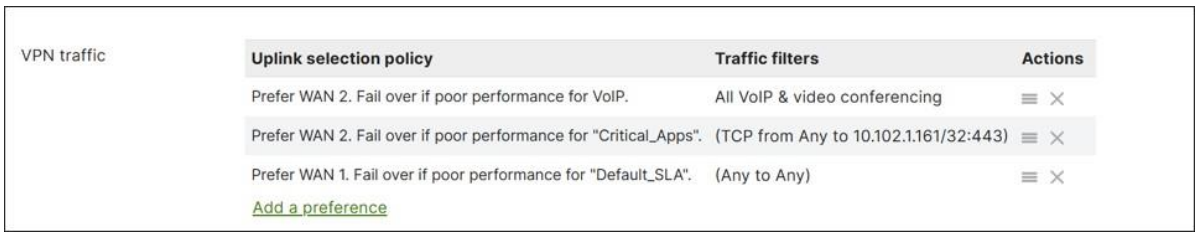
Under **SD-WAN Policies>VPN traffic**, click **Add a preference**. Under **Traffic filters**, click **Add +** and select an application or application family or create a custom expression to match VPN traffic. Select the preferred uplink and click **Save**. Repeat to add any additional lines of policy.



The following two uplink selection policies are configured in this example:

Traffic Filters	Preferred Uplink	Fail Over If:	Performance Class:
All VoIP & video conferencing	WAN 2	Poor performance	VoIP
Layer 3 TCP from Any to 10.102.1.161/32:443	WAN 2	Poor performance	Critical_Apps
Layer 3 Any to Any	WAN 1	Poor performance	Default_SLA

Click **Save** or Save Changes.



Traffic Shaping Rules

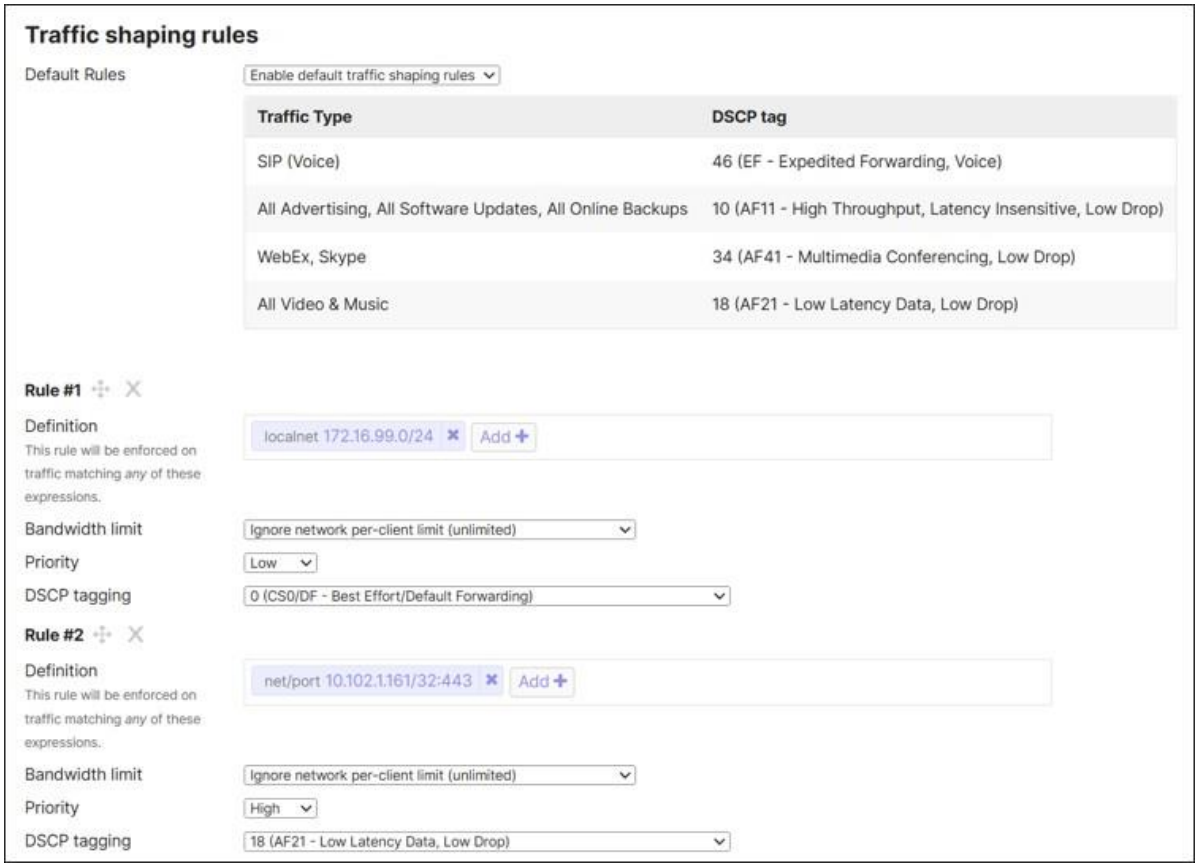
In this example, the default traffic shaping rules are kept and only two additional rules are added. The two rules are to give lower priority to guest traffic and give higher priority to the critical application traffic that was referenced in **SD-WAN polices>VPN traffic**. Next to **Default Rules**, ensure that **Enable default traffic shaping rules** is selected.

Under **Traffic shaping rules**, click **Add a new shaping rule**. Indicate what traffic should be matched, what bandwidth limit should be applied if any, what priority should the traffic be treated as, and any DSCP tagging requirements.

The following is configured for this example:

Rule #	Definition	Bandwidth Limit	Priority	DSCP Tagging
1	localnet 172.16.99.0/24 (guest)	Ignore network per-client limit (unlimited)	Low	0 (CS0/DF – Best Effort/Default Forwarding)
2	net/port 10.102.1.161/32:443	Ignore network per-client limit (unlimited)	High	18 (AF21 – Low Latency Data, Low Drop)

Click **Save Changes**.

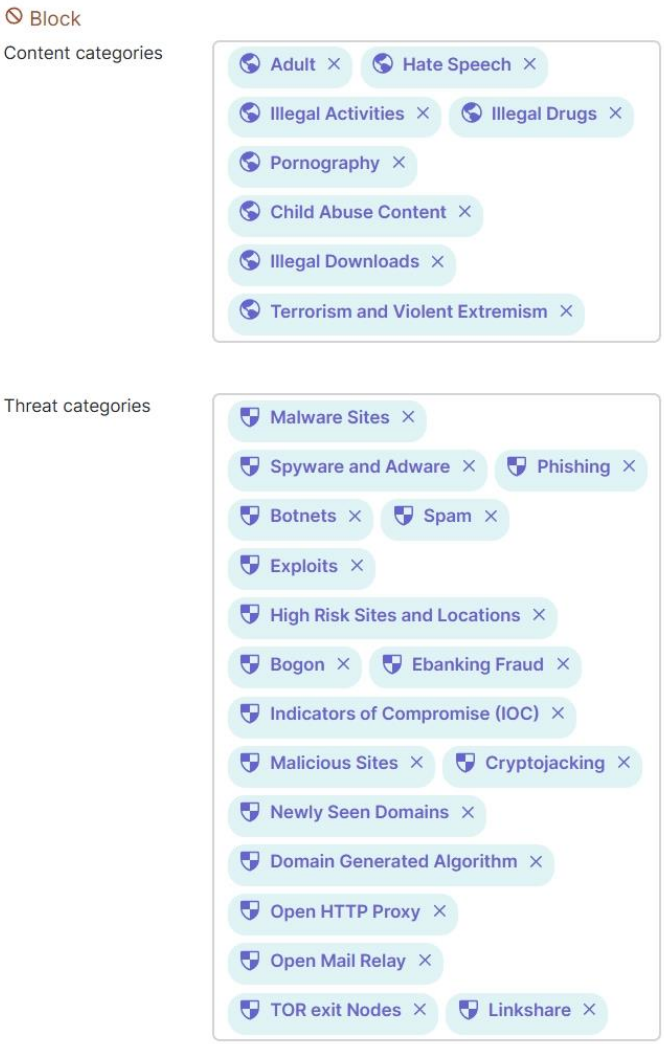


MX Secure Router: Configure Threat Protection

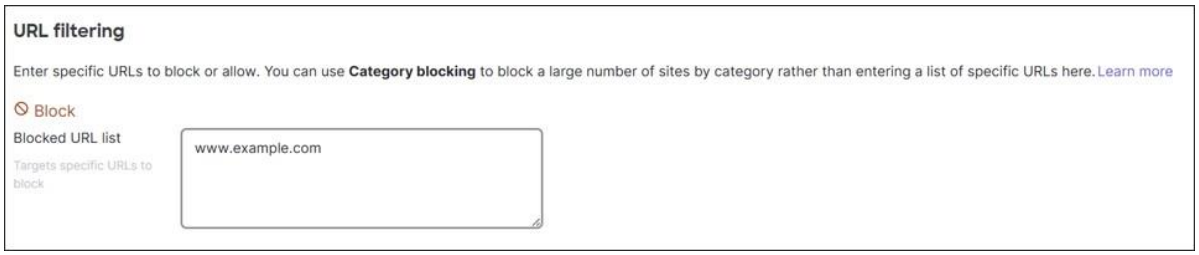
Under the **Security & SD-WAN>Configure>Threat Protection** page, Advanced Malware Protection (AMP) and Intrusion detection and prevention can be configured. Under **Advanced Malware Protection (AMP)**, ensure the **Mode** is set to **Enabled**. Under **Intrusion detection and prevention**, set the **Mode** to **Prevention** and choose **Balanced** next to **Ruleset**. Click **Save** or **Save Changes**.

MX Secure Router: Configure Content Filtering

Go to **Security & SD-WAN>Configure>Content Filtering**. Under **Category blocking**, select what content and threat categories should be blocked, as well as any URLs that should be allowed or blocked under **URL filtering**. In this example, the following was configured:



www.example.com is included in the URL filtering blocked URL list.

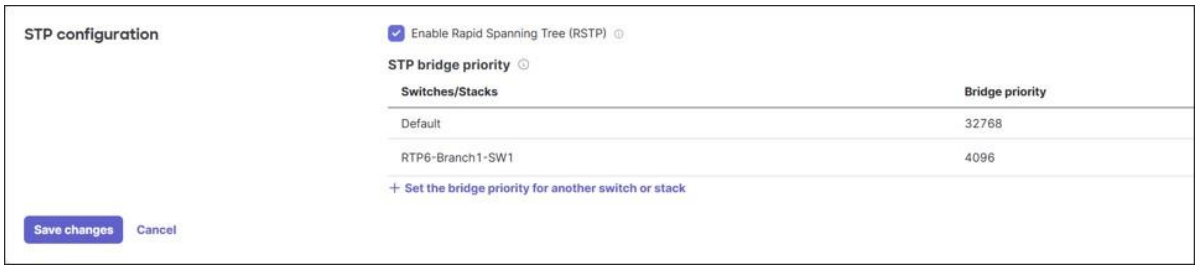


Click **Save**.

Switch: Configure the Spanning Tree Root

The switch is configured to be the root of spanning tree. Go to **Switching>Configure>Switch Settings** under **STP configuration**. Click **Set the bridge priority for another switch or stack**. A window may pop up warning that changing the STP bridge priority may cause a short disruption on all switches in the network as spanning tree is re-calculated. Click **Got it**.

Choose the **Switches/Stacks** name from the drop-down box (RTP6-Branch1-SW1) and select 4096 from the drop-down box under **Bridge priority**. Click **Confirm**.



Click **Save changes**.

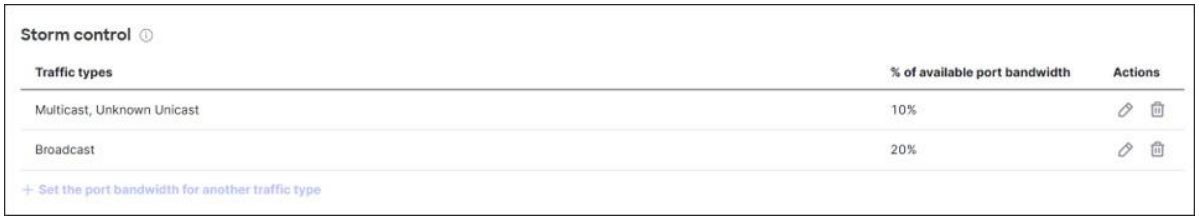
Switch: Configure Quality of Service

In this example, minimal Quality of Service configurations are made. Under **Switching>Configure>Switch Settings>Quality of service**, default DSCP-to-CoS mappings are retained. Guest traffic (VLAN 50) is untrusted with all traffic set to 0 (default), while incoming DSCP is trusted for Data (VLAN 10), Voice (VLAN 20), and IOT traffic (VLAN 30).

Switch: Configure Storm Control

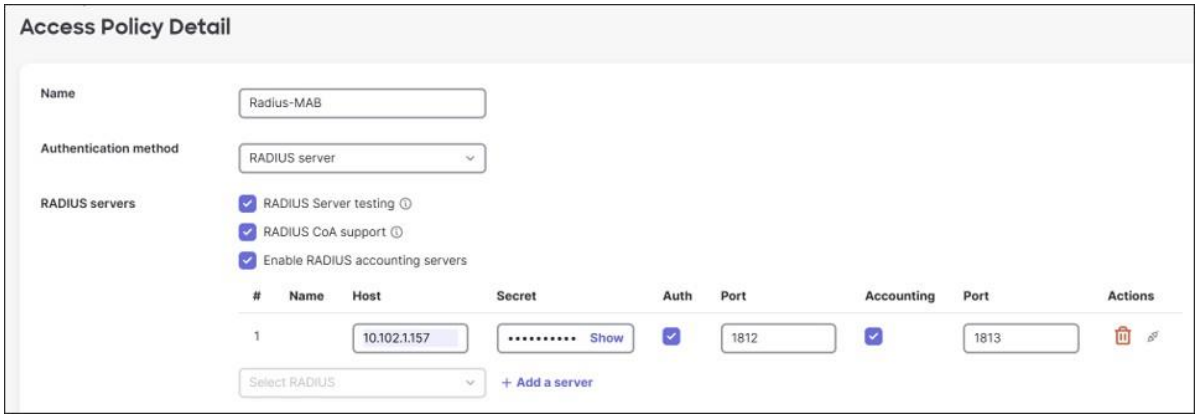
In this example, storm control is configured on the wired access ports. Go to **Switching>Configure>Switch Settings** and under **Storm control**, click **+ Set the port bandwidth for another traffic type**. Enter the **Traffic type** and **% of available port bandwidth**. Click **Confirm**. Repeat to finish the traffic types. When finished, click **Save changes**.

While percentages for what's normal traffic may vary for each network, in this example, Broadcast traffic is set to 20% while Multicast and Unknown Unicast is set to 10%.

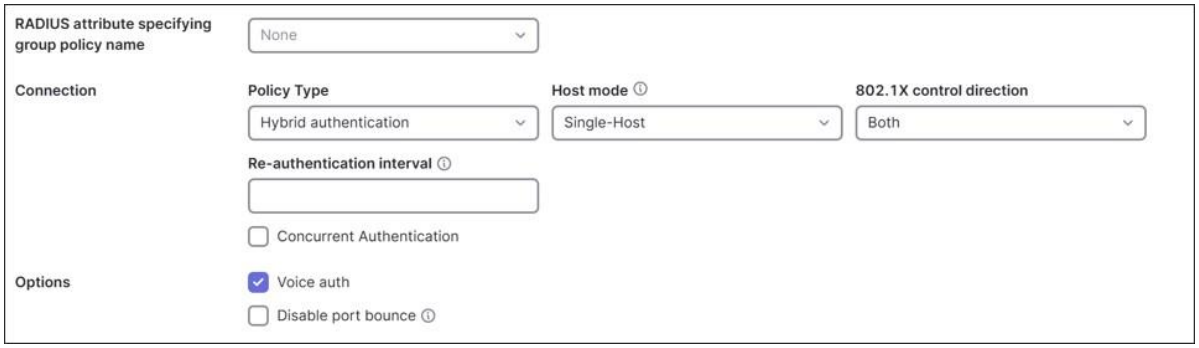


Switch: Configure Access Policies

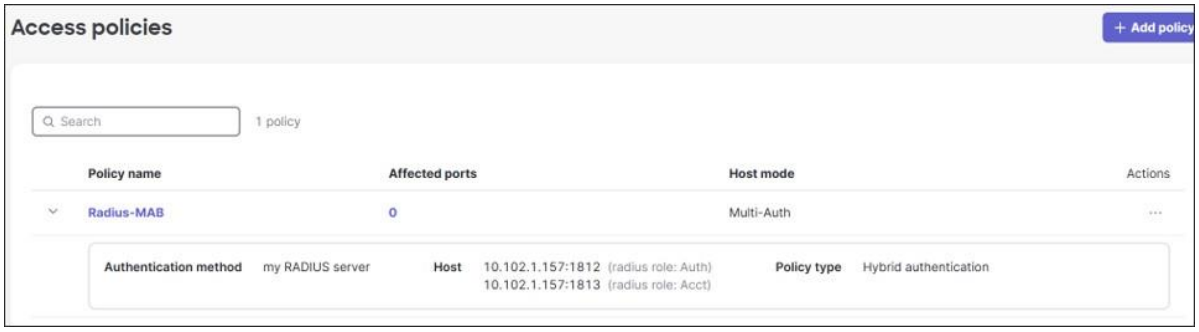
To configure 802.1x on the switch in this example, go to **Switching>Configure>Access Policies**. Click **+ Add policy**. Configure a **Name** (Radius-MAB) and **Authentication method** (RADIUS server). Enable **RADIUS Server testing**, **RADIUS CoA support**, and **RADIUS accounting servers**. Click **+ Add a server** and fill in the **Host**, **Secret**, and **Port** number for RADIUS Authentication. Repeat to add information on the RADIUS Accounting server.



Next to **Connection**, select **Hybrid authentication** since both 802.1x and Mac Authentication Bypass can be utilized. **Host mode** is set to **Single-Host** by default and **802.1x control direction** defaults to **Both**. Next to **Options**, select **Voice auth**.



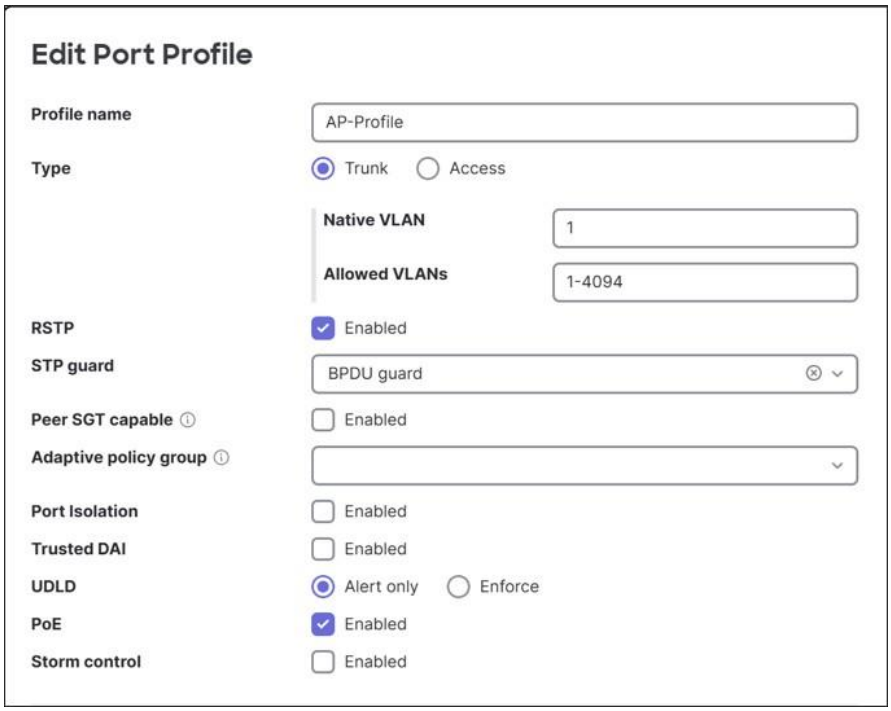
Click **Save**.



Switch: Configure Port Profiles

Port profiles can shortcut port configurations. In the example, one port profile is created for the ports connected to access points and another port profile is created for wired clients.

Go to **Switching>Configure>Port Profiles**. Click **+ Add profile**. Fill out the **Profile name**, specify the **Type** of port, **RSTP** enabled/disabled, **STP guard**, any SGT settings, **UDLD** setting, **PoE** setting, and **Storm control**. Then click **Save** and repeat for additional profiles.



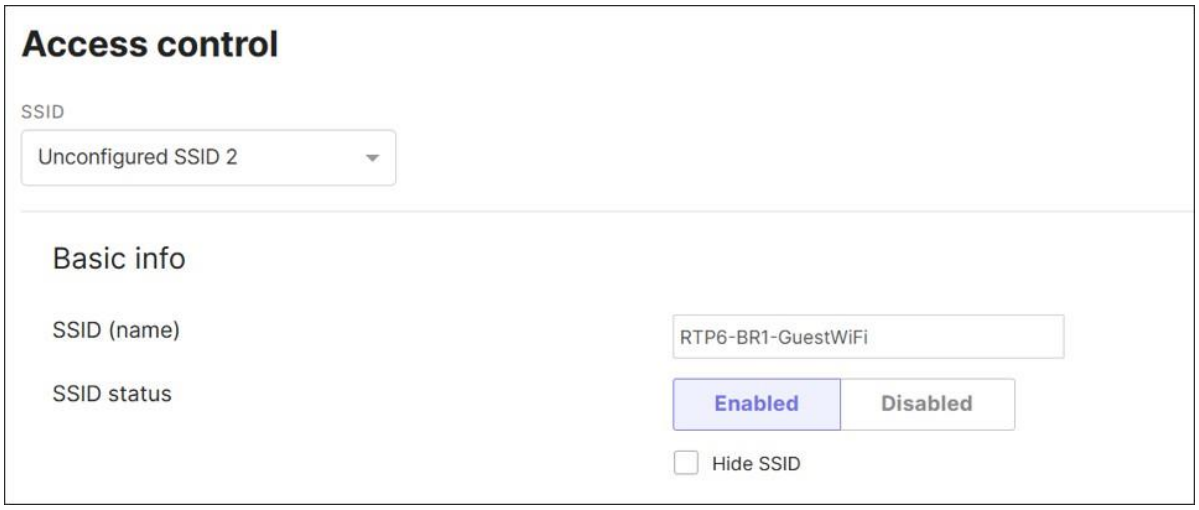
The following profiles are created in this example:

Profile Name	Type	RSTP	STP Guard	UDLD	PoE	Storm control
AP-Profile	Trunk • Native VLAN 1 • Allowed VLANs 1-4094	Enabled	BPDU guard	Alert only	Enabled	Disabled
Data-Profile	Access • Access policy: Radius-MAB • VLAN 10 • Voice VLAN 20	Enabled	BPDU guard	Alert only	Enabled	Enabled

Wireless Access Point: Configure Guest SSID

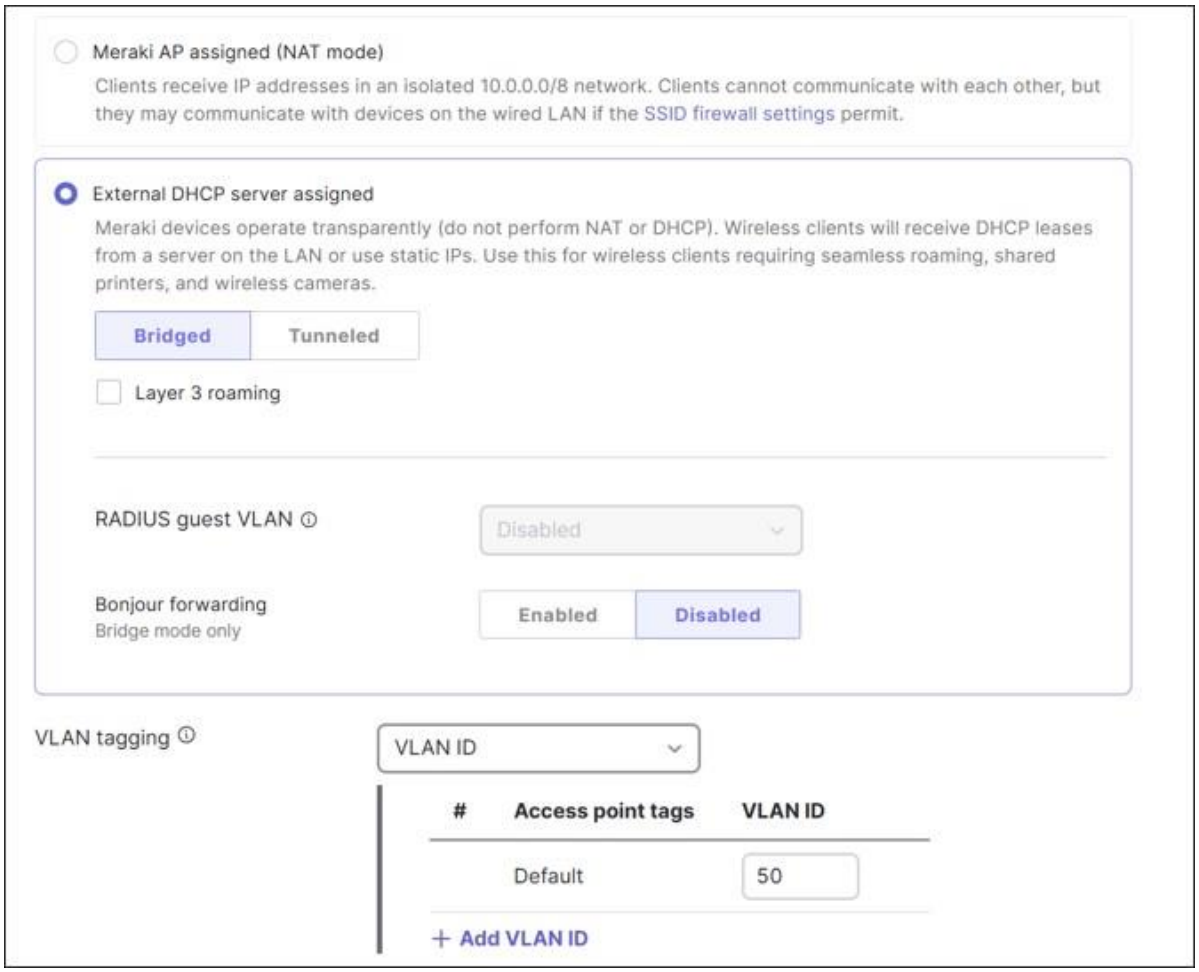
Access Control

Go to **Wireless>Configure>Access Control**. Select an unconfigured SSID from the drop-down box. Provide an **SSID name** (in this example RTP6-BR1-GuestWiFi), and next to **SSID status**, select **Enabled**. The SSID will not be hidden.



Select **Security** (Open (no encryption)), enable **Mandatory DHCP**, and under **Splash page**, choose **Click-through** – this requires guests to view and acknowledge a splash page before being allowed on the network.

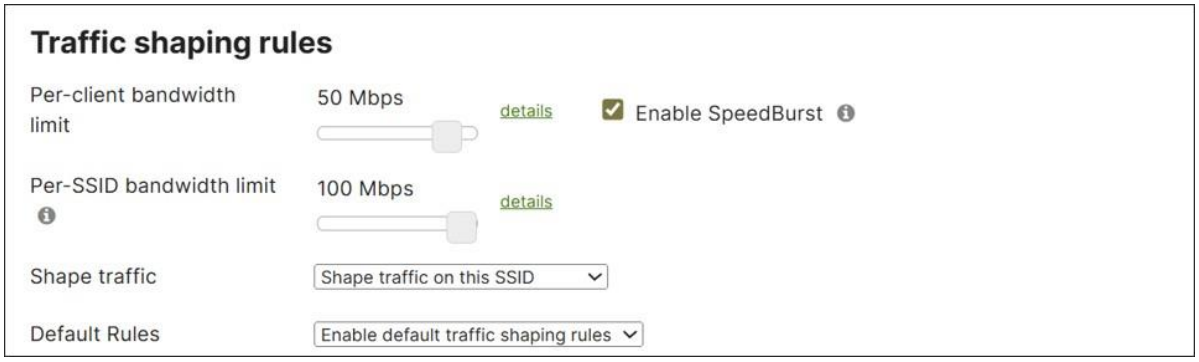
Under **Client IP and VLAN**, select **External DHCP server assigned** and leave the setting in **Bridged** mode. Next to **VLAN tagging**, choose **VLAN ID** from the drop-down box, and in the **VLAN ID** box, type 50, which is the Guest VLAN already defined on the MX router and carried on the trunk between the AP/switch and the MX router/switch. Click **Save**.



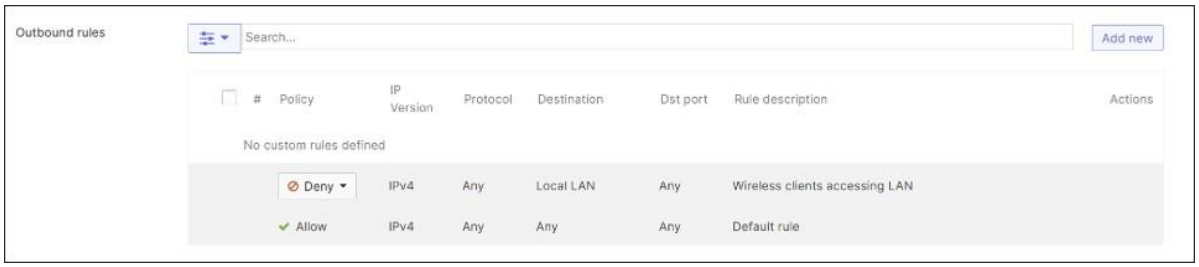
Firewall and Traffic Shaping

Under **Wireless>Firewall & traffic Shaping**, select the guest SSID from the drop-down box (RTP6-BR1-GuestWiFi). Under **Block IPs and ports** next to **Layer 2 LAN isolation**, select **Enabled**.

For this example, set the **Per-client bandwidth limit** to 50 Mbps and **Enable SpeedBurst**. Set the **Per-SSID bandwidth limit** to 100 Mbps. Next to **Shape traffic**, choose **Shape traffic on this SSID** and ensure next to **Default Rules** that **Enable default traffic shaping rules** is chosen.



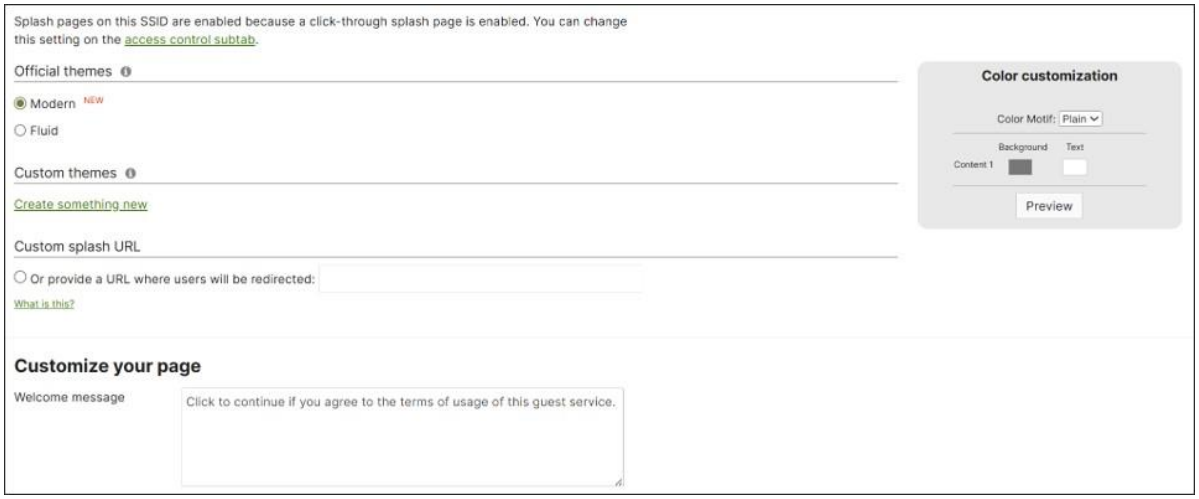
Under **Outbound rules**, ensure that **Deny** is selected for “IPv4 Any Local LAN Any” for the **Wireless clients accessing LAN** rule.



Click **Save Changes**.

Splash Page

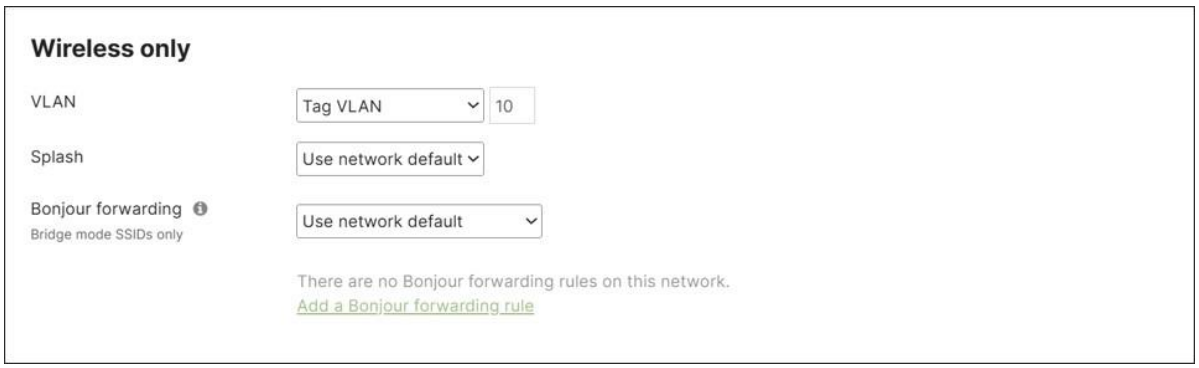
Go to **Wireless>Configure>Splash Page**. Under the Splash page, select the guest SSID (RTP6-BR1-GuestWiFi). Ensure **Modern** is chosen under **Official themes**. Under **Customize your page** next to **Welcome message**, type “Click to continue if you agree to the terms of usage of this guest service”. Click **Save Changes**.



Network-Wide: Configure Group Policy

In this example, group policy is applied after RADIUS authentication occurs. The RADIUS server passes back a filter-ID parameter, which corresponds to a group policy name and is applied to the wireless user accessing the network. In this example, there are 3 policy groups: Employees, Voice, and IOT.

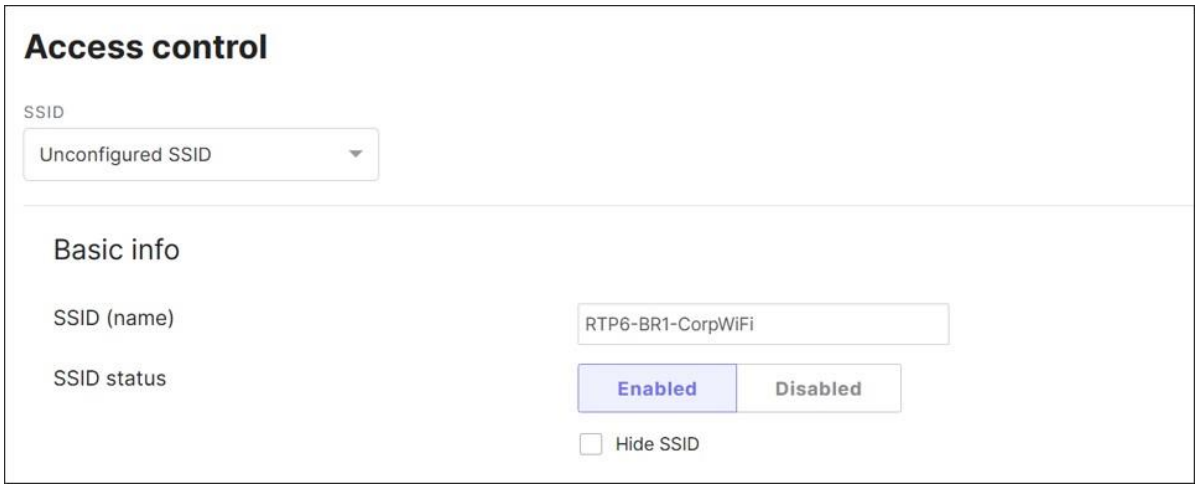
Go to **Network-wide>Group Policies** and click **Add a group**. Next to **Name**, type Employees and under **Wireless only** next to **VLAN**, select **Tag VLAN** from the drop-down box and type 10 in the box. Click **Save Changes**. Repeat for Voice (VLAN 20) and IOT (VLAN 30).



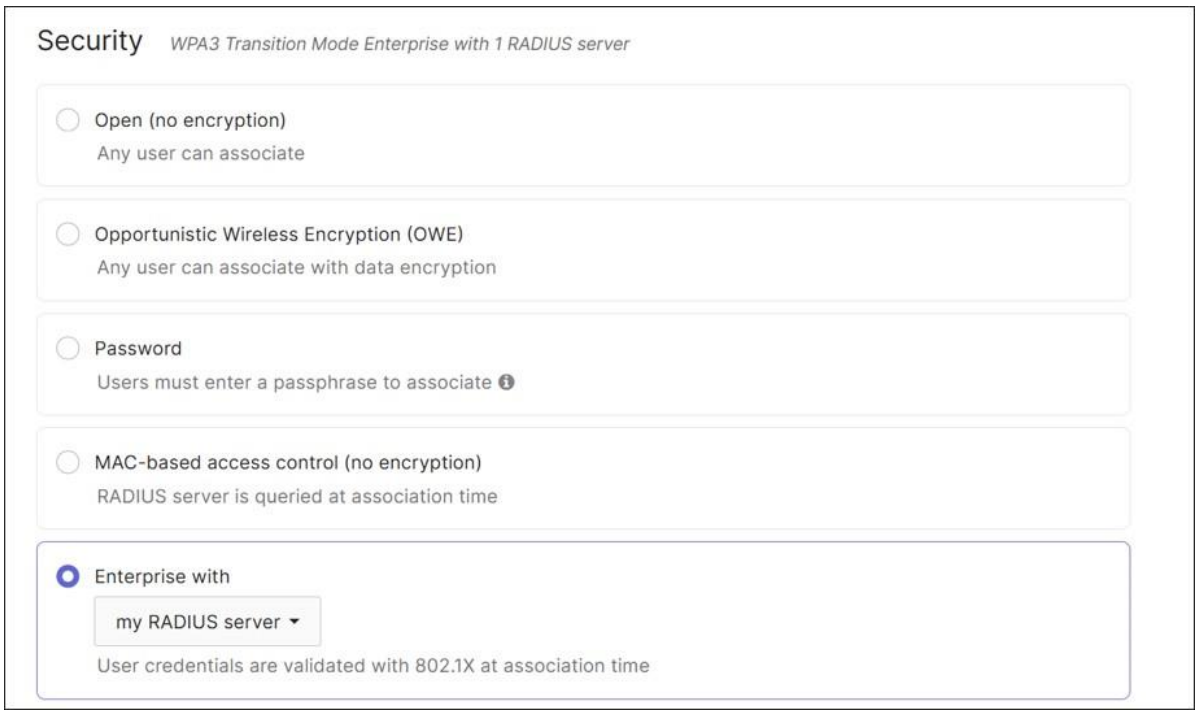
Wireless Access Point: Configure Corporate SSID

Access Control

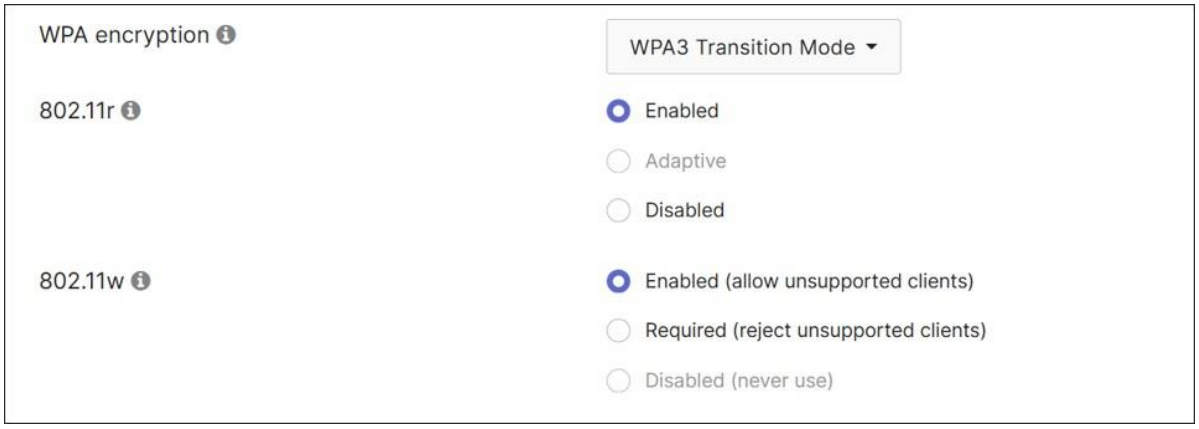
Go to **Wireless>Configure>Access Control**. Select an unconfigured SSID from the drop-down box. Provide an **SSID name** (in this example, RTP6-BR1-CorpWiFi) and next to **SSID status**, select **Enabled**. The SSID will not be hidden.



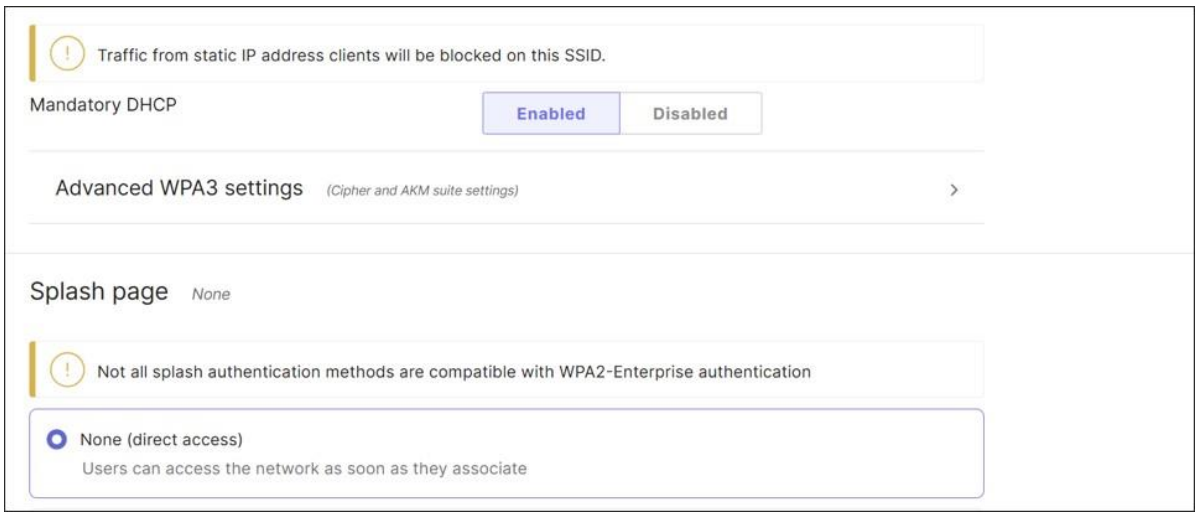
Under **Security**, choose **Enterprise with my RADIUS server**.



Next to **WPA encryption**, choose **WPA3 Transition Mode**. Next to **802.11r** (fast roaming) choose **Enabled**, and next to **802.11w** (management frame protection) choose **Enabled (allow unsupported clients)**.

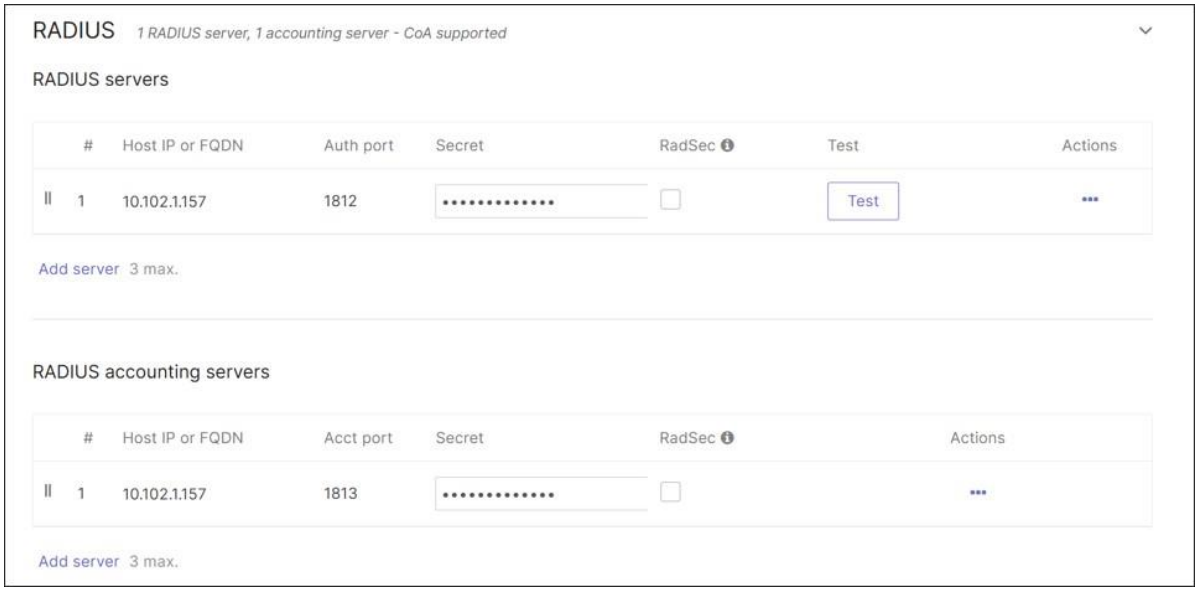


Next to **Mandatory DHCP**, select **Enabled**. Under **Splash page**, choose **None (direct access)**.



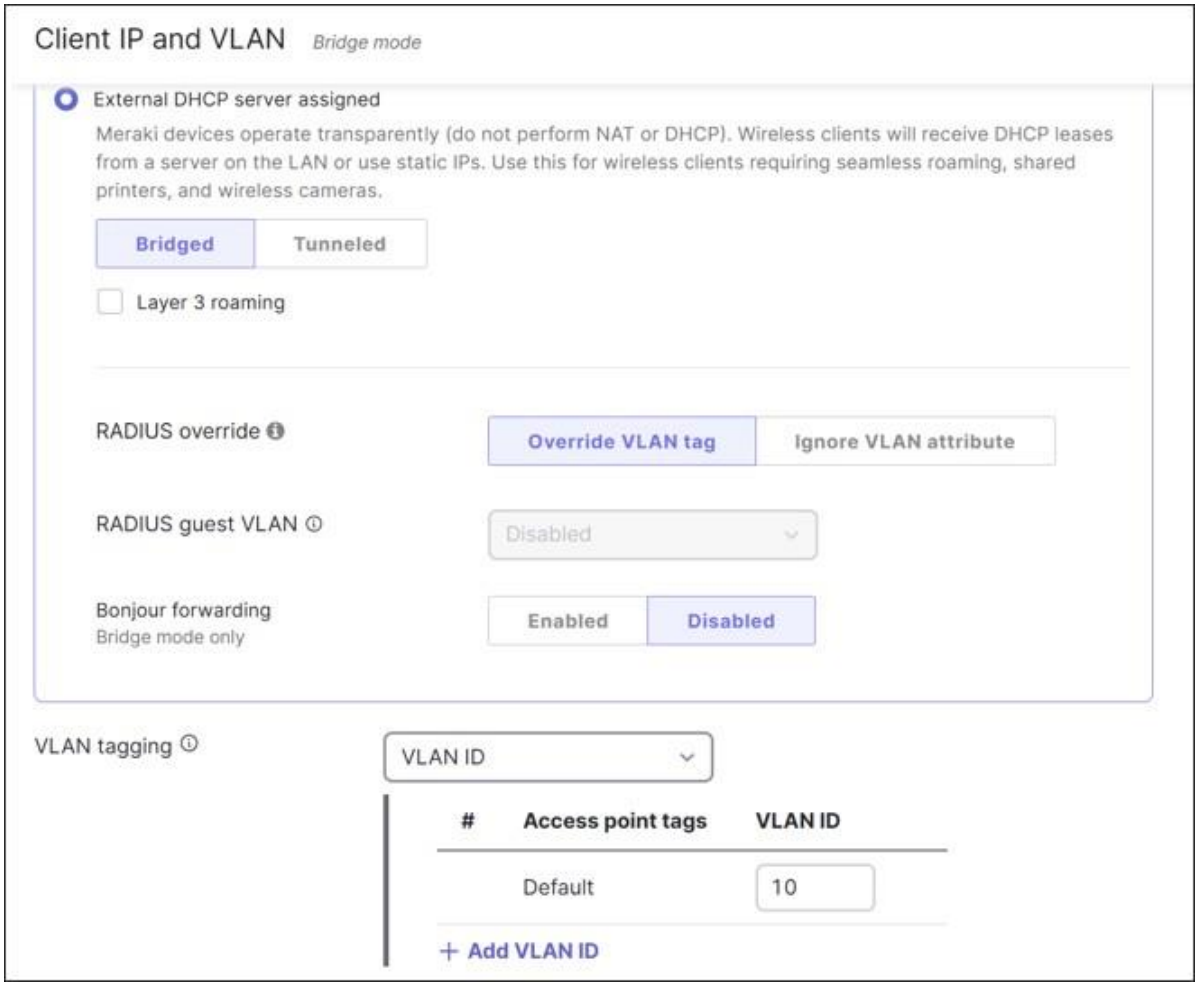
To prepare for Wi-Fi 7 mode in the future, under **Advanced WPA3 settings**, select **GCMP 256** next to **WPA3 Cipher Suite**.

Under **RADIUS** and **RADIUS servers**, click **Add server** and enter the **Host IP or FQDN**, **Auth** (Authentication) **port**, **Secret** password, and click **Done**. Under **RADIUS accounting servers**, select **Add server** and enter the **Host IP or FQDN**, **Acct** (Accounting) **port**, **Secret** password, and click **Done**.



RADIUS CoA is not enabled due to the enabling of the fast-roaming feature. Next to **RADIUS attribute specifying group policy name**, select **Filter-Id**.

Under **Client IP and VLAN**, select **External DHCP server assigned** and ensure **Bridged** mode is selected. Next to **RADIUS override**, ensure that **Override VLAN tag** is selected. Under **VLAN tagging**, select **VLAN ID**, and under **VLAN ID**, type in 10. This is the default VLAN for authenticated users if VLAN IDs or group policy names are not passed by RADIUS. VLAN 10 is the Data VLAN already defined on the MX router and carried on the trunk between the AP/switch and the MX router/switch. Click **Save**.

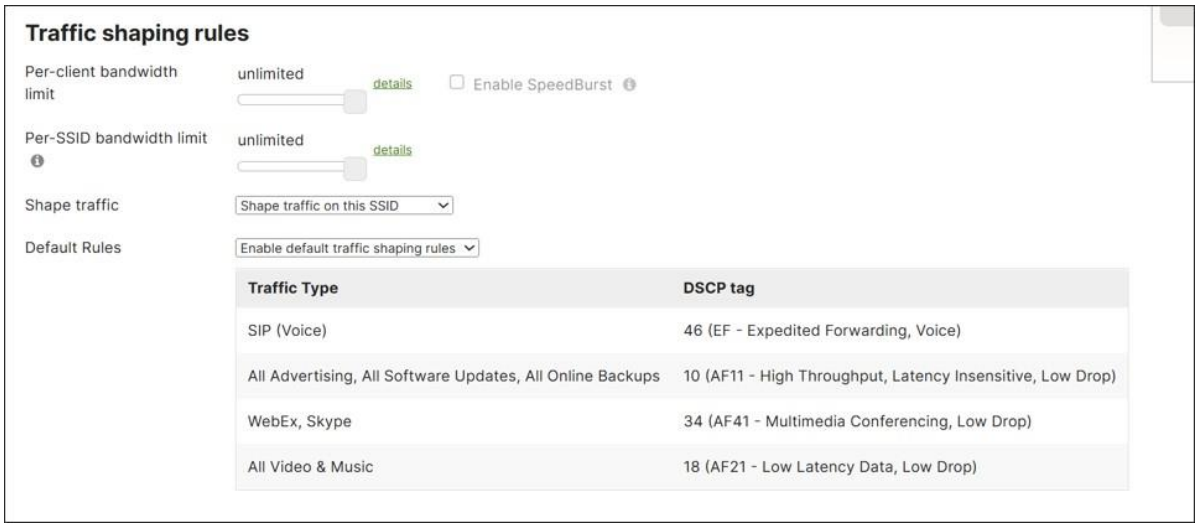


Firewall and Traffic shaping

Under **Wireless>Firewall & traffic shaping**, select the Corp SSID from the drop-down box (RTP6-BR1-CorpWiFi). Leave defaults. The configuration should look like:

- Layer 2 LAN isolation: disabled
- DHCP guard: Disabled

- RA guard: Enabled
- Outbound rules: Allow IPv4 Any Local LAN Any (Wireless clients accessing LAN)
- Outbound rules: Allow IPv4 Any Any Any (Default rule)
- Traffic shaping rules: Per-client bandwidth limit: unlimited
- Traffic shaping rules: Per-SSID bandwidth limit: unlimited
- Traffic shaping rules: Shape traffic: Shape traffic on this SSID
- Traffic shaping rules: Enable default traffic shaping rules

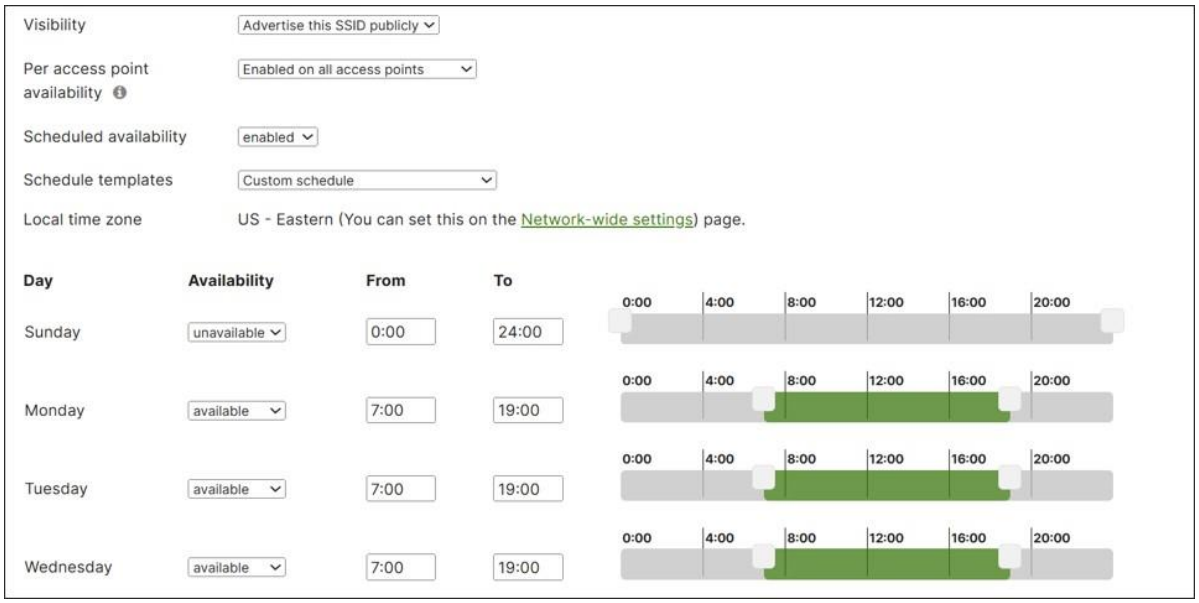


Wireless Access Point: Configure SSID Availability

In this section, SSID availability is configured. Go to **Wireless>SSID Availability** and select an **SSID** (RTP6-BR1-CorpWiFi). Next to **Scheduled availability**, select **enabled**. Next to **Schedule templates**, ensure **Custom schedule** is selected. Configure the following:

- Sunday, unavailable, From 0:00 to 24:00
- Monday-Friday, available, From 7:00 to 19:00
- Saturday, unavailable, From 0:00 to 24:00

Click **Save Changes**. Repeat for other SSIDs.



Configure Other Network Services

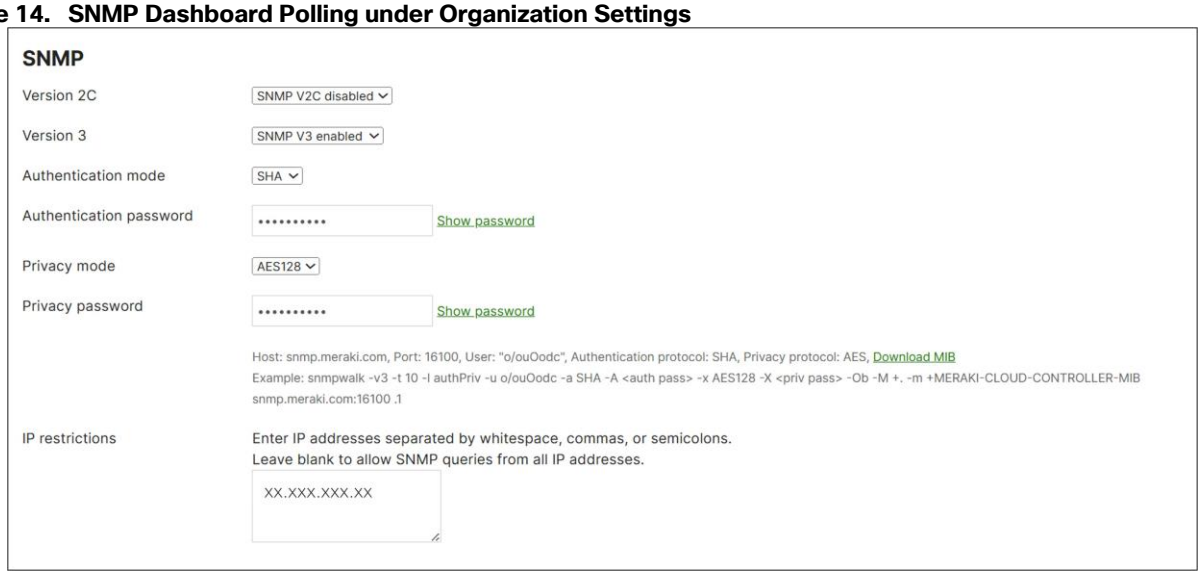
SNMP (Dashboard Polling)

Go to **Organization>Configure>Settings**. Under **SNMP**, ensure the following settings are configured:

- SNMP V2C disabled
- SNMP V3 enabled
- Authentication mode: SHA
- Privacy mode: AES128

Ensure strong passwords are chosen for Authentication and Privacy and configure any IP restrictions (IP address endpoints that are authorized to poll the dashboard).

Figure 14. SNMP Dashboard Polling under Organization Settings



SNMP (Dashboard Traps)

SNMP traps originating from the dashboard are configured at the network-level. Go to **Network-wide>Configure>Alerts>SNMP traps**. Next to **Access**, select **V3 (username/password)**. Click **Add an SNMP user** and fill out an SNMP **Username** and **Passphrase**. The same passphrase is used for authentication and privacy. The authentication protocol is SHA1, and privacy protocol is AES128.

Fill out the IP address of the server that will receive the SNMP traps and configure its receiving port as well.

Under **Alerts Settings**, add **SNMP** in the **Default recipients box** and select any conditions where alerts should be triggered. In this example, the following conditions have been selected to be alerted on:

- Network-wide: A rogue access point is detected
- WAN appliance: Malware is downloaded

SNMP (Device Polling)

The SNMP device polling configuration is done at the network level. Go to **Network-wide>General**. Under **Reporting** next to **SNMP access**, configure **V3 (username/password)**. Click **Add an SNMP user** and configure an SNMP **Username** and strong **Passphrase** that will be used for the authentication and privacy passwords. Select AES128 for **Privacy Mode** (the authentication protocol will be SHA1).

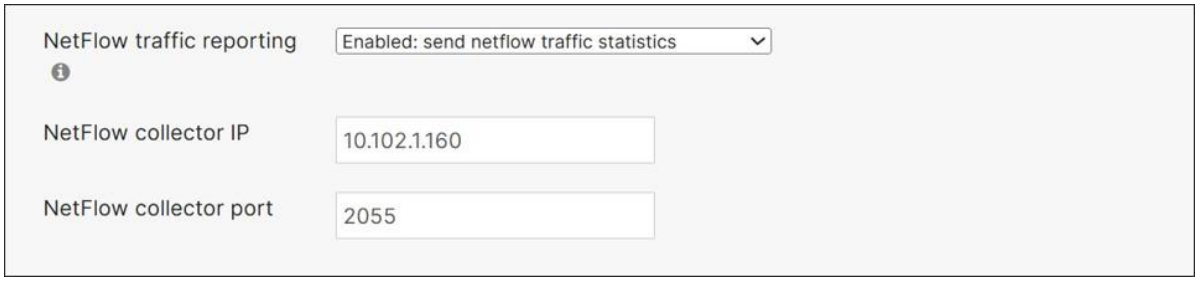
In this example, the SNMP server is in the data center and rules are already configured to allow the traffic in the outbound VPN firewall, so no further configuration is needed. If the server traffic is coming in from the WAN outside the VPN network, it would have to be allowed in the L3/L7 firewall settings as well as in the **WAN appliance services settings** located at **Security & SD-WAN>Firewall settings**.

Syslog

To configure syslog for the network devices, go to **Network-wide>General**. Under **Reporting>Syslog servers**, click **+ Add a syslog server**. Fill in the **Server address** (10.102.1.160), **Port** (514), and **Roles** (Air Marshal events, Appliance event log, Flows, Security events, Switch event log, URLs, Wireless event log). Click **Save Changes**.

NetFlow

To configure NetFlow, go to **Network-wide>General**. Under **Reporting** next to **NetFlow traffic reporting**, select **Enabled: send netflow traffic statistics**. Next to **NetFlow collector IP**, type the IP address of the NetFlow collector. Next to **NetFlow collector port**, type the port number of the NetFlow collector. Click **Save Changes**.

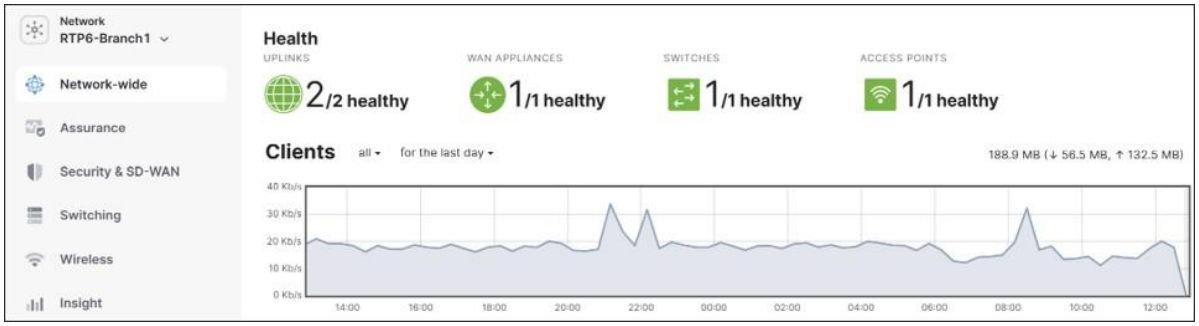


In this example, NetFlow is only enabled for the MX router since it is not supported on MS switches.

Onboard the Devices/Verify Device Operation

- Ensure the MX router can get a DHCP lease and Internet connectivity from the WAN connection.
- Power the MX router on and connect WAN interface 1 (RJ45 port 3 in this example) to its WAN transport. Once it reaches the dashboard, a firmware upgrade may take place. When the LED on the router turns solid white, the MX is connected to the dashboard, and its configuration should be downloaded. Connect WAN interface 2 (RJ45 port 4 in this example) to its WAN transport.

- Once the MX router is fully on board, power on the switch and connect the uplink of the switch (port 1 in this example) to the proper port on the MX router (port 5 in this example). Once it reaches the dashboard, a firmware upgrade may take place. When the LED on the switch is solid white, the switch is connected to the dashboard, and its configuration should be downloaded.
- Once the switch is fully on board, power on the access point and connect the uplink of the access point to the proper port on the switch (port 9 in this example). Once it reaches the dashboard, a firmware upgrade may take place. When the LED on the AP is solid white, the AP is connected to the dashboard, and its configuration should be downloaded.
- Verify the operation of the devices using the dashboard. Select the desired **Network** at the top left of the dashboard (RTP6-Branch1), then select **Network-wide>Monitor>Clients**.



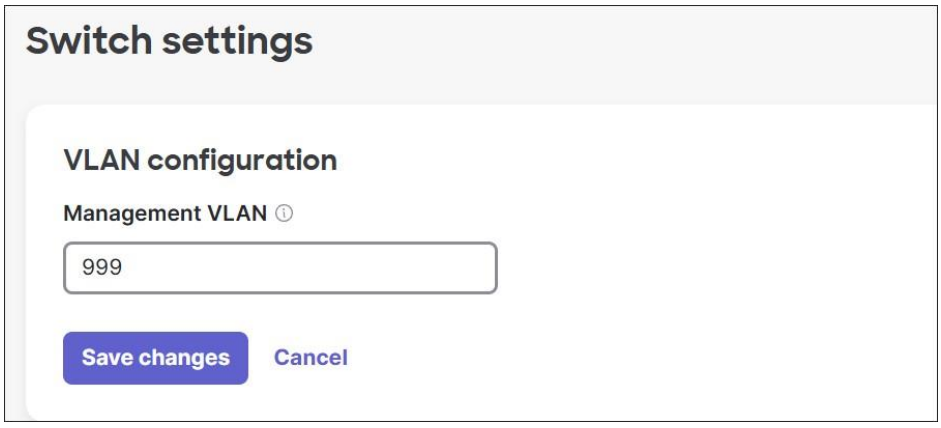
- Drill into any devices to review status, configurations, or troubleshoot issues.

Complete Device Configurations

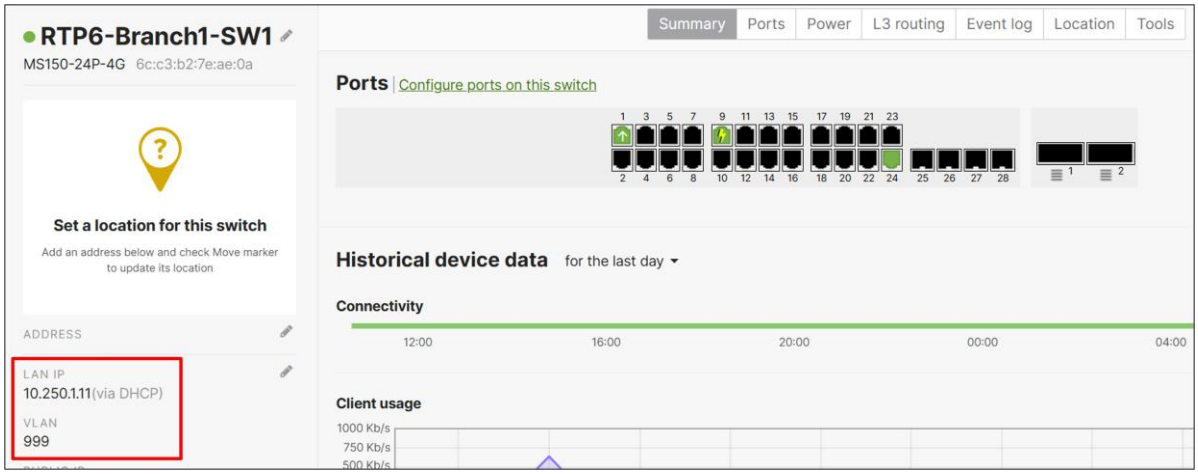
The final step is to complete any device configurations. In this example, port configurations for the MX router and switch and moving switch and AP management traffic into the INFRA VLAN was saved for last to ensure a smooth onboarding process.

Switch: Configure Switch Management VLAN

The switch management traffic is configured to be tagged with VLAN 999. Go to **Switching>Configure>Switch Settings** and under **VLAN configuration>Management VLAN**, configure 999. Click **Save changes**.

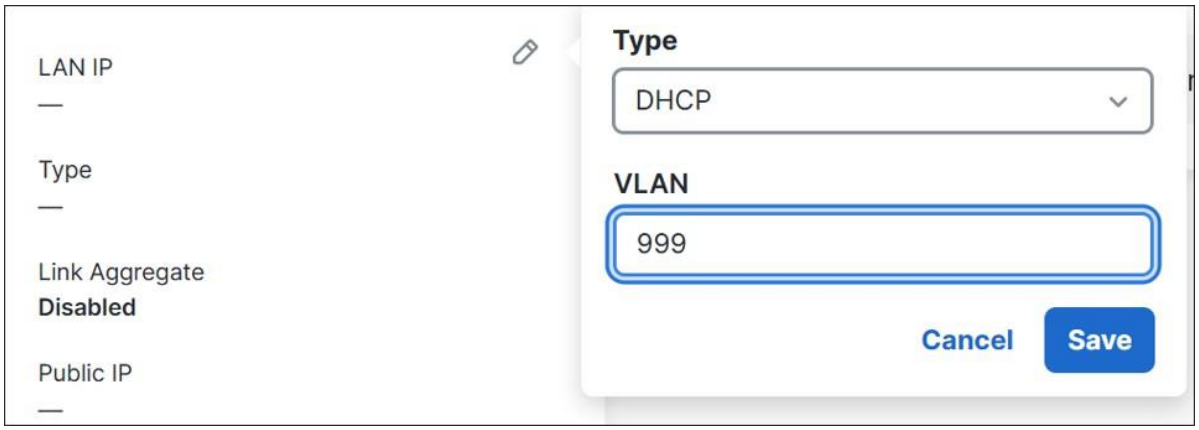


Once configured, go to **Switching>Monitor>Switches**, and select the switch to validate the changes.

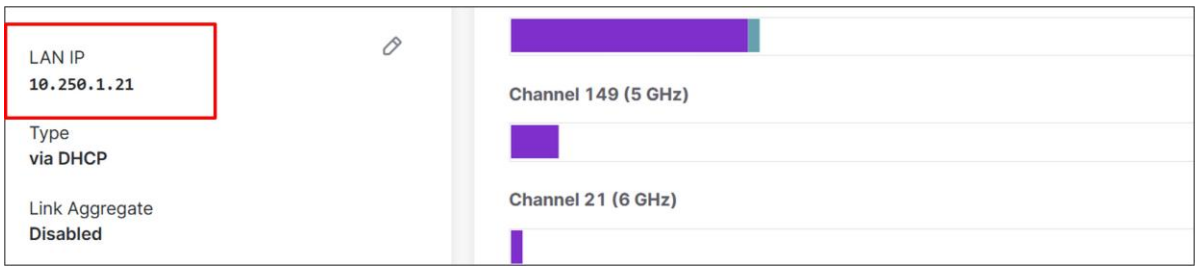


Wireless Access Point: Configure AP Management VLAN

Go to **Wireless>Monitor>Access Points**. Click the desired access point (named RTP6-Branch1-AP1). Click the edit symbol to the right of **LAN IP**. Fill in the **VLAN** (999) and click **Save**.

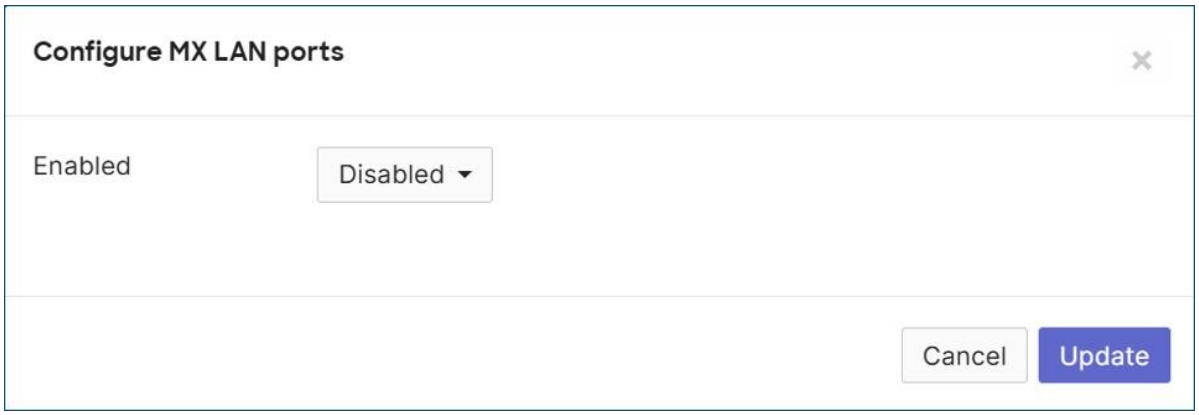


Once configured, go to **Wireless>Monitor>Access Points**, and select the access point to validate the changes.

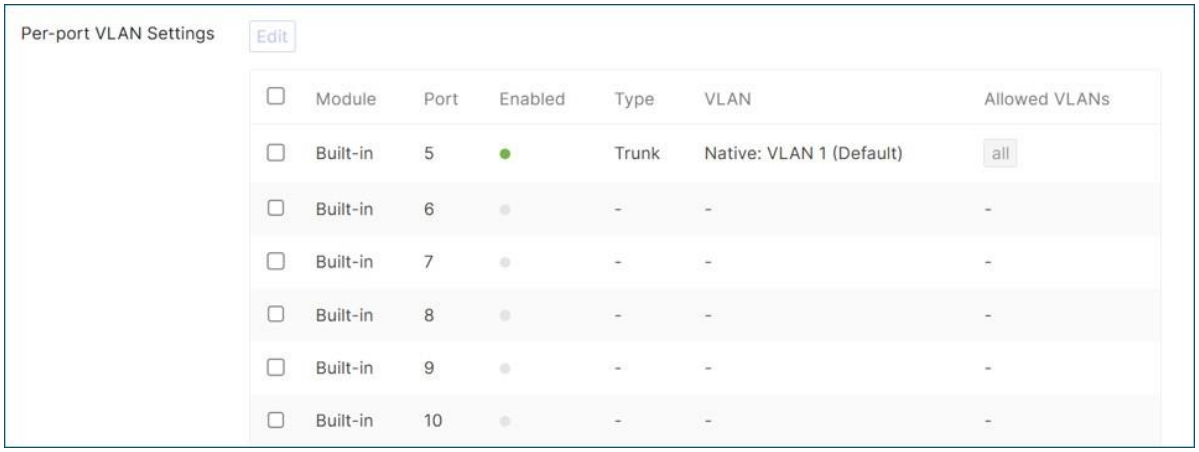


MX Router: Configure Ports

By default, all LAN ports are configured as 802.1Q trunk ports with VLAN 1 as the native/untagged VLAN. Go to **Security & SD-WAN>Configure>Addressing & VLANs>Routing** and under **Per-port VLAN Settings**, disable all unused ports (currently, only LAN port 5 is in use for the downstream switch). Click the checkbox to the left of port 6 and hold the shift button while clicking the checkbox to the left of port 14 to select the rest of the ports, then click **Edit**. Select **Disabled** from the drop-down box, then click **Update**.



Click **Save**.



Switch: Configure Ports

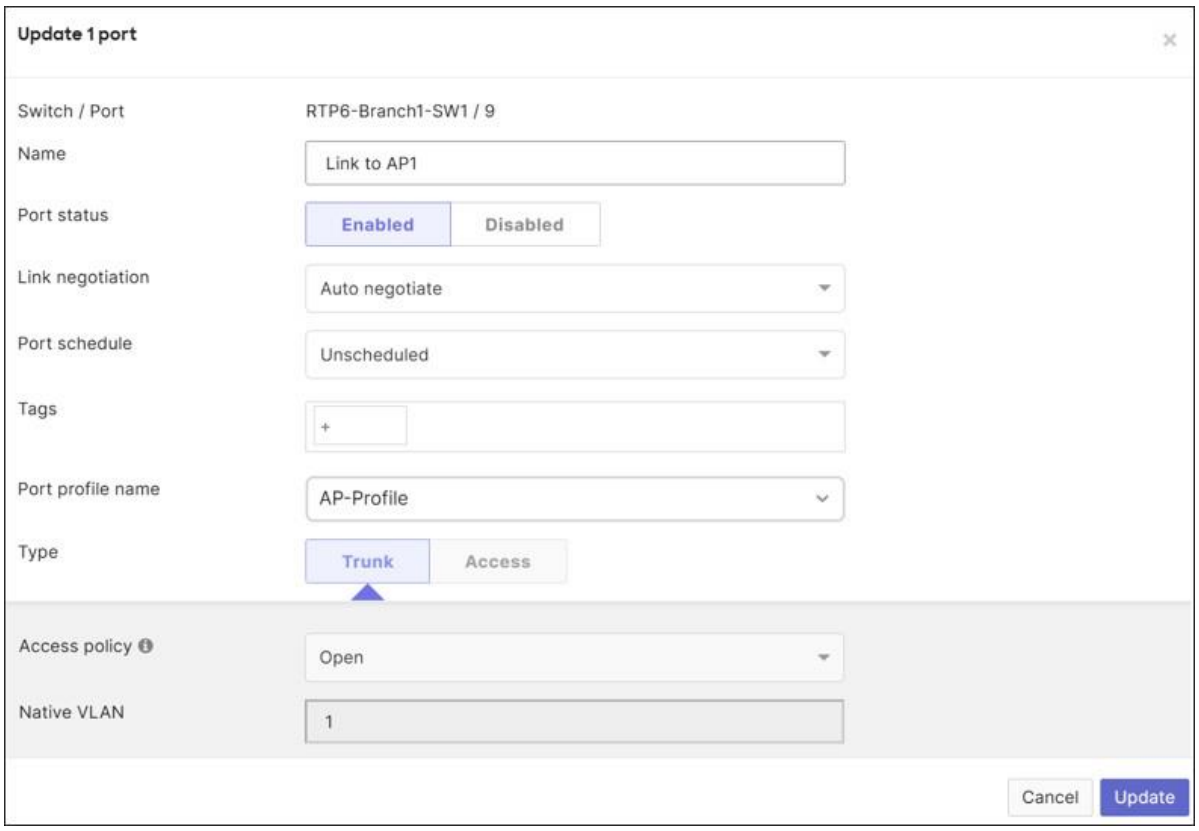
To apply the port profile configurations to the switch ports, go to **Switching>Monitor>Switch Ports**. Port 1 is the uplink to the MX router in our example and will remain at defaults. Click the port definition to the left of uplink details. The default settings are shown as follows:

- Port Status: Enabled
- Link negotiation: Auto negotiate
- Port schedule: Unscheduled
- Type: Trunk
  - Access policy: Open
  - Native VLAN: 1
  - Allowed VLANs: all
- RSTP: Enabled
- STP guard: Disabled
- Port isolation: Disabled
- Trusted DAI: Disabled
- UDLD: Alert only
- PoE: Enabled

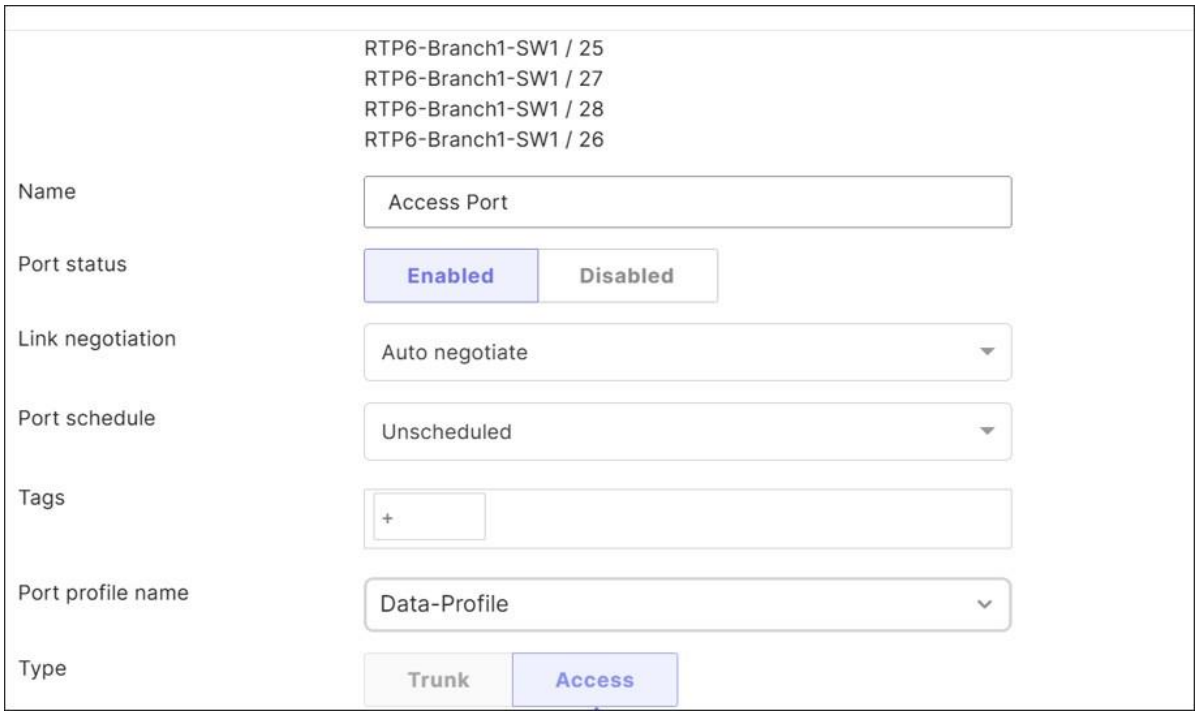
- Storm control: Disabled

Create a **Name** for the port. In this example, the name is set to Uplink to MX-Primary. Click **Update**.

In this example, Port 9 of the switch is connected to the access point. Click the port definition to the left of details. Configure the **Name** (Link to AP1) and select the **Port profile name** (AP-Profile). Click **Update**.



For the rest of the ports (ports 2-8, 10-28), select the check box to the left and click **Edit** at the top of the screen. Fill out an optional **Name** (Access Port) and select the **Port profile name** (Data-Profile). Click **Update**.



Appendix A: Example Deployment Settings

The following summarizes the configurations used in this example deployment. If a setting is not mentioned, the default has been taken. Some of the values below may reflect default values.

Organization Settings

Under Organization>Configure on the Dashboard

Main Menu	Section	Subsection	Values
Settings	SNMP	Version 2C Version 3 Authentication mode Authentication password Privacy mode Privacy password IP restrictions	SNMP V2C disable SNMP V3 enabled SHA <passphrase> AES128 <passphrase> <IP address>
Policy Objects	All objects	Corp SNMP Corp DNS-DHCP Corp Mgt Corp Radius	10.102.1.161 10.102.1.160 10.102.1.160 10.102.1.157
Policy Objects	All objects	Guest Subnet Infra Subnet IOT Subnet Voice Subnet Data Subnet	172.16.99.0/24 10.250.0.0/16 10.30.0.0/16 10.20.0.0/16 10.10.0.0/16
Policy Objects	All objects	Branch 1 Printer 1 Branch 1 Printer 2	10.30.1.101 10.30.1.102
Policy Objects	Groups	Corp Shared Services Branch 1 Printers	Corp DNS-DHCP, CORP Radius, Corp Mgt, Corp SNMP Branch 1 Printer 1, Branch 2 Printer 2

Network-wide Settings

Under Network-wide>Configure on the Dashboard

Main Menu	Section	Subsection	Values
General	General	Network name	RTP-Branch1
General	General	Local time zone	America – New York (UTC -4.0, DST)
General	Reporting	Syslog servers	10.102.1.160, port 514, Roles Air Marshal events, Appliance event log, Flows, Security events, Switch event log, URLs, Wireless event log

Main Menu	Section	Subsection	Values
General	Reporting	SNMP access SNMP users Privacy Mode	V3 (username/passwords) snmpuser, <passphrase>, privacy = AES128
General	Reporting	Network traffic reporting NetFlow collector IP NetFlow collector port	Enabled: send netflow traffic statistics 10.102.1.160 2055
Alerts	Alerts Settings	Default recipients	snmp
Alerts	Alerts Settings	Network-wide WAN appliance	Network-wide: A rogue access point is detected WAN appliance: Malware is downloaded
Alerts	SNMP traps	Access Users Receiving server IP Receiving server port	V3 (username/password) snmpuser, <passphrase> <IP address> 162
Group policies	Employees	Wireless only/VLAN	Tag VLAN 10
Group policies	Voice	Wireless only/VLAN	Tag VLAN 20
Group policies	IOT	Wireless only/VLAN	Tag VLAN 30

MX Router Settings

Under Security & SD-WAN>Configure on the Dashboard

Main Menu	Section	Subsection	Values
Site-to-site VPN	Site-to-site VPN	Type	Spoke
Site-to-site VPN	Site-to-site VPN	Hubs	RTP6-DC1 – appliance, IPv4 default route enabled RTP6-DC2 – appliance, IPv4 default route enabled
Addressing & VLANs	Deployment Settings	Mode	Routed
Addressing & VLANs	Routing	LAN Setting	VLANs
Addressing & VLANs	Routing	Subnets	• 999, INFRA, 10.250.1.1/24, VPN mode = Enabled • 50, GUEST, 172.16.99.1/24, VPN mode = Disabled • 30, IOT, 10.30.1.1/24, VPN mode = Enabled • 20, VOICE, 10.20.1.1/24, VPN mode = Enabled • 10, DATA, 10.10.1.1/24, VPN mode = Enabled • 1, Default, 192.168.128.1/24, VPN mode = Disabled
Addressing & VLANs	Routing	Per-port VLAN Settings	• Port 5 Enabled, Type Trunk, Native VLAN 1, Allowed VLANs = All • Ports 6-14 Disabled

Main Menu	Section	Subsection	Values
DHCP	VLAN 1 (Default)	Client addressing Mandatory DHCP DNS nameservers	Run a DHCP server Enabled Use OpenDNS
DHCP	VLAN 10 (DATA)	Client addressing DHCP server IPs Mandatory DHCP	Relay DHCP to another server 10.102.1.160 10.102.1.161 Disabled
DHCP	VLAN 20 (VOICE)	Client addressing DHCP server IPs Mandatory DHCP	Relay DHCP to another server 10.102.1.160 10.102.1.161 Disabled
DHCP	VLAN 30 (IOT)	Client addressing DHCP server IPs Mandatory DHCP	Relay DHCP to another server 10.102.1.160 10.102.1.161 Disabled
DHCP	VLAN 50 (GUEST)	Client addressing Mandatory DHCP DNS nameservers	Run a DHCP server Enabled Use OpenDNS
DHCP	VLAN 999 (INFRA)	Client addressing Mandatory DHCP DNS nameservers Custom nameservers Fixed IP assignments	Run a DHCP server Disabled Specify nameservers 10.102.1.160 10.102.1.161 RTP-Branch1-SW1, 6c:c3:b2:7e:se:0a, 10.250.1.11 RTP-Branch1-AP1, cc:6e:2a:dd:f8:c0, 10.250.1.12
Site-to-site VPN	Organization-wide settings	Site-to-site outbound firewall	• Shared Services: Allow prot:Any Src:[Data Subnet, IOT Subnet, Voice Subnet, Infra Subnet] Any Dest:Corp Shared Services Any • Shared Services: Allow prot:Any Src:Corp Shared Services Any Dest:[Data Subnet, IOT Subnet, Voice Subnet, Infra Subnet] Any • Data Access: Deny prot:Any Src:Data Subnet Any Dest:[IOT Subnet, Voice Subnet, Infra Subnet] Any • IOT Access: Deny prot:Any Src:IOT Subnet Any Dest:[Data Subnet, Infra Subnet, Voice Subnet] Any • Infra Access: Deny prot:Any Src:Infra Subnet Any Dest:[Data Subnet, IOT Subnet, Voice Subnet] Any • Voice Access: Deny prot:Any Src:Voice Subnet Any Dest:[IOT Subnet, Infra Subnet, Data Subnet] Any • Default rule: Allow prot:Any Src:Any Any Dest:Any Any
Firewall	Layer 3	Outbound rules	• Local Print Access: Allow prot:Any Src:[DATA VLAN] Any Dest:[Branch 1 Printers] Any • Allow DIA: Allow prot:Any Src:[INFRA VLAN, DATA VLAN, GUEST VLAN, Default VLAN] Any Dest:Any Any

Main Menu	Section	Subsection	Values
			• Deny All: Deny prot:Any Src:Any Any Dest: Any Any • Default Rule: Allow prot:Any Src: Any Any Dest: Any Any
Firewall	Layer 3	WAN appliance services	ICMP Any, Web None, SNMP None
SD-WAN & traffic shaping	Uplink configuration	WAN 1	400 Mbps
SD-WAN & traffic shaping	Uplink configuration	WAN 2	500 up/500 down
SD-WAN & traffic shaping	Uplink selection	Load balancing	Disabled
SD-WAN & traffic shaping	Uplink selection	Multi-Uplink AutoVPN	Enabled
SD-WAN & traffic shaping	SD-WAN policies	Internet traffic	• Prefer WAN 2. Fail over if uplink down • 10.250.1.0/24:any to any:any
SD-WAN & traffic shaping	SD-WAN policies	Internet traffic	• Prefer WAN 2. Fail over if poor performance for SaaS_Trafic • 10.10.1.0/24 to Office 365 or Webex
SD-WAN & traffic shaping	SD-WAN policies	VPN traffic	• Prefer WAN 2. Fail over if poor performance for VoIP • All VoIP & Video conferencing
SD-WAN & traffic shaping	SD-WAN policies	VPN traffic	• Prefer WAN 2. Fail over if poor performance for “Critical_Apps” • TCP from Any to 10.102.1.161/32:443
SD-WAN & traffic shaping	SD-WAN policies	VPN traffic	• Prefer WAN 1. Fail over if poor performance for “Default_SLA” • Any to Any
SD-WAN & traffic shaping	SD-WAN policies	Custom performance classes	• SaaS_Traffic, 150, 50, 5 • Critical_Apps, 150, 20, 2
SD-WAN & traffic shaping	Local internet breakout	VPN exclusion rules	• Office 365 Suite • Webex • Layer 3 udp from Any to 64.62.142.12/32 • Layer 3 udp from Any to 158.115.128.0/19 • Layer 3 udp from Any to 209.206.48.0 • Layer 3 udp from Any to 216.157.128.0/20
SD-WAN & traffic shaping	Global bandwidth limits	Per-client limit	unlimited
SD-WAN & traffic shaping	Traffic shaping rules	Default Rules	Enable default traffic shaping rules
SD-WAN & traffic shaping	Traffic shaping rules	Rule #1	• Definition: localnet 172.16.99.0/24 • Bandwidth limit: Ignore network per-client limit (unlimited) • Priority: Low • DSCP tagging: 0 (CS0/DF - Best Effort/Default Forwarding)
SD-WAN & traffic	Traffic shaping	Rule #2	• Definition: net/port 10.102.1.161/32

Main Menu	Section	Subsection	Values
shaping	rules		• Bandwidth limit: Ignore network per-client limit (unlimited) • Priority: High • DSCP tagging: 18 (AF21 – Low Latency Data, Low Drop)
Threat Protection	Advanced Malware Protection (AMP)	Mode	Enabled
Threat Protection	Intrusion detection and prevention	Mode Ruleset	Prevention Balanced
Content Filtering	Category blocking	Content categories	Adult, Hate Speech, Illegal Activities, Illegal Drugs, Pornography, Child Abuse Content, Illegal Downloads, Terrorism and Violent Extremism
Content Filtering	Category blocking	Threat categories	Malware Sites, Spyware and Adware, Phishing, Botnets, Spam, Exploits, High Risk Sites and Locations, Bogon, Ebanking Fraud, Indicators of Compromise (IOC), Malicious Sites, Cryptojacking, Newly Seen Domains, Domain Generated Algorithm, Open HTTP Proxy, Open Mail Relay, TOR exit Nodes, Linkshare
Content Filtering	URL filtering	Blocked URL list	www.example.com

Under Security & SD-WAN>Monitor on the Dashboard

Main Menu	Section	Subsection	Values
Appliance Status	Summary	Appliance name (top left, edit mac address)	RTP6-Branch1-MX

Switch Settings

Under Switching>Configure> on the Dashboard

Main Menu	Section	Subsection	Values
Switch Settings	Switch settings	VLAN configuration	999
Switch Settings	Switch settings	STP configuration	Enable Rapid Spanning Tree (RSTP): Enabled STP bridge priority: Switches/Stacks (RTP6-Branch1-SW1) STP bridge priority: Bridge priority (4096)
Switch Settings	Switch settings	Quality of service	VLAN: 50, Trust: Disabled, Set DSCP: 0 VLAN 10, Trust: Enabled VLAN 20, Trust: Enabled VLAN 30, Trust: Enabled
Switch Settings	Switch settings	Storm control	• Broadcast, 20% • Multicast, 10% • Unknown Unicast, 10%
Access Policies	Access Policies	Name	Radius-MAB

Main Menu	Section	Subsection	Values
		Authentication method Radius servers Radius servers Radius servers Connection Options	Radius server RADIUS Server testing RADIUS CoA support enabled Host 10.102.1.157, secret <secret>, Auth enabled, Port 1812 Hybrid authentication, Single-Host, Both Voice auth enabled
Port Profiles	Port Profiles	Profile name: Data-Profile	• Type: Access • Access policy: Radius-MAB • VLAN: 10 • Voice VLAN: 20 • RSTP: Enabled • STP guard: BPDU guard • UDLD: Alert only • PoE: Enabled • Storm control: Enabled
Port Profiles	Port Profiles	Profile name: AP-Profile	• Type: Trunk ◦ Native VLAN: 1 ◦ Allowed VLANs: 1-4094 • RSTP: Enabled • STP guard: BPDU guard • UDLD: Alert only • PoE: Enabled • Storm control: Disabled

Under Switching>Monitor> on the Dashboard

Main Menu	Section	Subsection	Values
Switches (select switch)	Summary	Switch name (top left, edit mac address)	RTP6-Branch1-SW1
Switch Ports	Switch Ports	RTP-Branch1-SW1/1 - uplink	• Name: Uplink to MX-Primary • Type: Trunk • Native VLAN: 1 • Allowed VLANs: all • Access policy: Open • RSTP: Enabled • PoE: Enabled • Storm control: Disabled
Switch Settings	Switch Ports	RTP-Branch1-SW1/2-8, 10-28	Name: Access Port Port profile name: Data-Profile
Switch Settings	Switch Ports	RTP-Branch1-SW1/9	Name: Link to AP1 Port profile name: AP-Profile

Access Point Settings

Under Wireless>Configure> on the Dashboard.

Main Menu	Section	Subsection	Values
Access Control	Basic info	SSID (name)	RTP6-BR1-GuestWiFi
Access Control	Security (Guest)		Open (no encryption)
Access Control	Security (Guest)	Mandatory DHCP	Enabled
Access Control	Splash page (Guest)		Click-through
Access Control	Client IP and VLAN (Guest)	External DHCP server assigned	Enabled/Bridged
Access Control	Client IP and VLAN (Guest)	VLAN tagging	VLAN ID: Default AP tag, VLAN ID 50
Access Control	Basic info	SSID (name)	RTP-BR1-CorpWiFi
Access Control	Security (Corp)		Enterprise with my RADIUS server
Access Control	Security (Corp)	WPA encryption	WPA3 Transition Mode
Access Control	Security (Corp)	802.11r	Enabled
Access Control	Security (Corp)	802.11w	Enabled (allow unsupported clients)
Access Control	Security (Corp)	Mandatory DHCP	Enabled
Access Control	Security (Corp)	Advanced WPA3 settings	WPA3 Cipher Suite: GCMP 256 enabled
Access Control	Splash Page (Corp)		None (direct access)
Access Control	RADIUS (Corp)	RADIUS servers	10.102.1.157, 1812, <secret>
Access Control	RADIUS (Corp)	RADIUS accounting servers	10.102.1.157, 1813, <secret>
Access Control	RADIUS (Corp)	RADIUS CoA support	Disabled
Access Control	RADIUS (Corp)	RADIUS attribute specifying group policy name	Filter-Id
Access Control	Client IP and VLAN (Corp)	External DHCP server assigned RADIUS override	Enabled/Bridged Override VLAN tag
Access Control	Client IP and VLAN (Corp)	VLAN tagging	VLAN ID: Default AP tag, VLAN ID 10
Firewall & traffic shaping	Block IPs and ports (Guest)	Layer 2 LAN isolation	Enabled
Firewall & traffic shaping	Block IPs and ports (Guest)	Outbound rules	• Deny IPv4 Any Local LAN Any Wireless clients access LAN

Main Menu	Section	Subsection	Values
			• Allow IPV4 Any Any Any Default rule
Firewall & traffic shaping	Traffic shaping rules (Guest)	Per-client bandwidth limit Enable SpeedBurst Per-SSID bandwidth limit Shape traffic Default Rules	50 Mbps Enabled 100 Mbps Shape traffic on this SSID Enable default traffic shaping rules
Firewall & traffic shaping	Block IPs and ports (Corp)	Outbound rules	• Allow IPv4 Any Local LAN Any Wireless clients access LAN • Allow IPV4 Any Any Any Default rule
Firewall & traffic shaping	Traffic shaping rules (Corp)	Per-client bandwidth limit Per-SSID bandwidth limit Shape traffic Default Rules	Unlimited Unlimited Shape traffic on this SSID Enable default traffic shaping rules
Splash page	Splash page (Guest)	Official themes	Modern
Splash page	Customize your page (Guest)	Welcome message	Click to continue if you agree to the terms of usage of this guest service.
Splash page	Splash behavior (Guest)	Splash frequency Where should users go after the splash page?	Every day The URL they were trying to fetch
SSID Availability	SSID availability (all SSIDs)	Visibility Per access point availability Scheduled availability Schedule templates	Advertise this SSID publicly Enabled on all access points Enabled Custom schedule (Sun/Sat unavailable, M-F available 7:00-19:00)
Radio Settings	RRM	AI-RRM	Enable
Radio Settings	RF profiles (Indoor/Outdoor default)	General/Band selection	Per SSID
Radio Settings	RF profiles (Indoor/Outdoor default)	RTP6-BR1-CorpWiFi RTP6-BR1-GuestWiFi	2.4/5/6/Band steering Enable 2.4/5 Enabled

Under Wireless>Monitor> on the Dashboard

Main Menu	Section	Subsection	Values
Access Points	Summary	Access point name (top left, edit mac address)	RTP6-Branch1-AP1
Access Points	RTP-Branch1-AP1	LAN IP (edit)	VLAN 999

Appendix B: ISE Deployment Settings

The ISE deployment settings for the example deployment are documented in the following table:

Main Menu	Section	Subsection	Values
Administration	Groups	Endpoint Identity Groups	MAB-IOT_Devices MAB-VOICE_Devices
Administration	Groups	User Identity Groups	Employee
Policy	Policy Elements/Results	Authorization Profiles/Employee_VLAN	• Access Type = ACCESS_ACCEPT • Tunnel-Private-Group-ID = 1:10 • Tunnel-Type = 1:13 • Tunnel-Medium-Type = 1:6
Policy	Policy Elements/Results	Authorization Profiles/Employee-GP	• Access Type = ACCESS_ACCEPT • Filter-ID = Employees
Policy	Policy Elements/Results	Authorization Profiles/Voice_VLAN	• Access Type = ACCESS_ACCEPT • Tunnel-Private-Group-ID = 1:20 • Tunnel-Type = 1:13 • Tunnel-Medium-Type = 1:6 • cisco-av-pair = device-traffic-class=voice
Policy	Policy Elements/Results	Authorization Profiles/Voice-GP	• Access Type = ACCESS_ACCEPT • Filter-ID = Voice
Policy	Policy Elements/Results	Authorization Profiles/IOT_VLAN	• Access Type = ACCESS_ACCEPT • Tunnel-Private-Group-ID = 1:30 • Tunnel-Type = 1:13 • Tunnel-Medium-Type = 1:6
Policy	Policy Elements/Results	Authorization Profiles/IOT-GP	• Access Type = ACCESS_ACCEPT • Filter-ID = IOT
Policy	Policy Sets (Wired Access)	Conditions: Wired_802.1X or Wired_MAB	• Authentication Policy: ◦ Wired_MAB (Internal Endpoints) ◦ Default (All_User_ID_Stores) • Authorization Policy: ◦ IdentityGroup:Name = Endpoint Identity Groups:MAB-IOT_Devices or IdentityGroup:Name = User Identity Groups:IOT, Profile=IOT_VLAN ◦ IdentityGroup:Name = Endpoint Identity Groups:MAB-VOICE_Devices or IdentityGroup:Name = User Identity Groups:Voice, Profile=Voice_VLAN ◦ IdentityGroup:Name = Employee, Profile=Employee_VLAN
Policy	Policy Sets (Wireless Access)	Conditions: Wireless_802.1X	• Authentication Policy: ◦ Default (All_User_ID_Stores) • Authorization Policy: ◦ IdentityGroup:Name = User Identity Groups:IOT,

Main Menu	Section	Subsection	Values
			Profile=IOT-GP ◦ IdentityGroup:Name = User Identity Groups:Voice, Profile=Voice-GP ◦ IdentityGroup:Name = User Identity Groups:Employee, Profile=Employee-GP

Appendix C: Hardware and Software Versions Used

The following hardware and software versions were used in this example deployment:

Hardware	Software
MX85	MX 18.211.6
MS150-24P-4G	MS 17.2.1.1
CW9172I	MR 31.1.7.1