

Extreme Automated Campus

Version 1.1



Contents

Preface	6
Extreme Validated Designs	6
Purpose of This Document	6
Target Audience	7
Authors	7
Document History	7
About Extreme Networks	7
Introduction	8
Technology Overview	9
Terminology	9
Extreme Automated Campus - Introduction	10
Functional Components of Extreme Automated Campus	11
Extreme Fabric Connect: Core and Aggregation.....	11
Access Layer	19
ExtremeWireless	20
Extreme Management Center	20
Validated Designs – Infrastructure & Topology	22
Automated Campus Reference Topology	22
Hardware and Software Matrix	23
Preconditions	23
Campus VLAN/I-SID and Subnet Scheme	25
I-SID scheme	25
Campus 1 (VLAN 1xx):.....	25
Campus 2 (VLAN 2xx):.....	26
Campus 3 (VLAN 3xx):.....	26
Server Room (VLAN 9xx):.....	26
Common Services:	27
Fabric Connect - Core Configuration.....	28
Overview	28
BCB-930 Configuration	28
BEB-910 Configuration.....	30

BEB-920 Configuration.....	31
Fabric Connect – Campus 2 Configuration	32
Overview	32
Core Interface Configuration	33
BEB-210 Configuration.....	34
Routing Policies - Overview	40
BEB-211 Configuration (Peer)	44
Fabric Extend (Fabric Connect over IP) – Campus 1 Configuration	49
Overview	49
Core Interface (Tunnel) Configuration.....	49
BEB-111 Configuration.....	51
BEB-110 Configuration.....	58
Fabric Connect – Campus 3 Configuration	65
Overview	65
Core Interface Configuration	66
BEB-310 Configuration.....	67
Routing Policies - Overview	73
BEB-311 Configuration (Peer)	77
Fabric Connect - Server Room Configuration	83
Overview	83
BEB-910 Configuration (DVR Controller)	84
BEB-920 Configuration (DVR Controller)	87
BEB-960 (DVR Leaf).....	90
BEB-970 (DVR Leaf).....	94
BEB-940 (DVR Leaf).....	98
BEB-950 (DVR Leaf).....	102
Route Table Verification	106
Extreme Management Center Configuration	109
Site Configuration	109
Adding an ExtremeControl Appliance to Extreme Management Center	111
Adding Fabric Switches to Extreme Management Center	112
Adding Wireless Controllers to Extreme Management Center.....	113

Extreme Policy and Extreme Control Configuration.....	116
Extreme Policy.....	116
ExtremeControl Configuration.....	155
Extreme Wireless Configuration.....	174
ExtremeWireless Controller Configuration.....	174
Guest Access (Captive Portal).....	208
Wired User Access.....	209
Summit Access Switch.....	209
ERS Access Switch.....	220
Authentication – Netlogin & RADIUS.....	231
Wireless User Access.....	235
AP Provisioning / Fabric Attach.....	235
ExtremeAnalytics Configuration.....	239
Adding Analytics to Extreme Management Center.....	239
ExtremeAnalytics Configuration.....	241
Extreme Analytics Verification.....	251
RF-Planning.....	255
Site Survey.....	255
ExtremeWireless RF Planning Tool.....	255
Visualization.....	257
Sharing and Exporting.....	258
Product Lifecycle – Exporting into Other Products.....	259
RF Survey Tools.....	259
Design Considerations.....	260
Network Time Protocol (NTP).....	260
DHCP/BOOTP Relay Agent.....	266
Link Layer Discover Protocol (LLDP).....	277
Simple Network Management Protocol (SNMPv3).....	278
Domain Name System (DNS).....	291
RADIUS (Login Management Configuration).....	292
Secure Shell (SSH).....	305
Multicast (IGMP).....	306

Loop Protection.....313

References.....316

Preface

This document provides design and guidance for implementing an Extreme Networks Automated Campus using Extreme Networks hardware and software. An Extreme Automated Campus consists of ExtremeSwitching products, ExtremeWireless, Extreme Management, ExtremeControl, and ExtremeAnalytics.

Extreme Validated Designs

Helping customers consider, select, and deploy network solutions for current and planned needs is our mission. Extreme Validated Designs offer a fast track to success by accelerating that process.

Validated designs are repeatable reference network architectures that have been engineered and tested to address specific use cases and deployment scenarios. They document systematic steps and best practices that help administrators, architects, and engineers plan, design, and deploy physical and virtual network technologies. Leveraging these validated network architectures accelerates deployment speed, increases reliability and predictability, and reduces risk.

Extreme Validated Designs incorporate network and security principles and technologies across the ecosystem of service provider, data center, campus, and wireless networks. Each Extreme Validated Design provides a standardized network architecture for a specific use case, incorporating technologies and feature sets across Extreme products and partner offerings.

All Extreme Validated Designs follow best-practice recommendations and allow for customer-specific network architecture variations that deliver additional benefits. The variations are documented and supported to provide ongoing value, and all Extreme Validated Designs are continuously maintained to ensure that every design remains supported as new products and software versions are introduced.

By accelerating time-to-value, reducing risk, and offering the freedom to incorporate creative, supported variations, these validated network architectures provide a tremendous value-add for building and growing a flexible network infrastructure.

Purpose of This Document

This Extreme validated design provides guidance for designing and implementing an Extreme Automated Campus using Extreme hardware and software, detailing the Extreme reference architecture and its configuration.

It should be noted that not all features such as automation practices, zero-touch provisioning, and monitoring of the Extreme Automated Campus with ExtremeWireless are included in this document. Future versions of this document are planned to include these aspects of the Automated Campus solution.

The design practices documented here follow the best-practice recommendations, but there are variations to the design that are supported as well.

Target Audience

This document is written for Extreme systems engineers, partners, and customers who design, implement, and support campus networks. This document is intended for experienced network architects and engineers. This document assumes that the reader has a good understanding of switching and routing features.

Authors

The authors have extensive experience testing Extreme Automated Campus products and solutions. At Extreme, they focus on developing and validating solution architectures that customers can use in deployments.

- James Georgopoulos, Staff QA Software Engineer
- Stephen Colarusso, Senior QA Software Engineer
- Shane May, Manager of QA Engineering

The authors would like to acknowledge the following individuals for their technical guidance in developing this validated design:

- Roger Lapuh, Senior Principal Software Applications Engineer
- Ludovico Stevens, Senior Systems Engineer
- Thomas Lewis, Principal Software Systems Engineer
- Elangomaran Kathirvel, Director of QA Engineering

Document History

Future revisions of this document will include upcoming Automated Campus products and technologies.

Date	Part Number	Description
October 2018	9035775	1.0 - Initial release
December 2018	9035775-01	1.1 – ERS Access support

About Extreme Networks

Extreme Networks® (NASDAQ: EXTR) networking solutions help the world's leading organizations transition smoothly to a world where applications and information reside anywhere. This vision is designed to deliver key business benefits such as unmatched simplicity, non-stop networking, application optimization, and investment protection.

Innovative Ethernet and storage networking solutions for data center, campus, and service provider networks help reduce complexity and cost while enabling virtualization and cloud computing to increase business agility.

To help ensure a complete solution, Extreme Networks (www.extremenetworks.com) partners with world-class IT companies and provides comprehensive education, support, and professional services offerings. (www.ExtremeNetworks.com)

Introduction

The Extreme Automated Campus design detailed in this document is targeted for both single and multi-site campuses. The configurations and design practices documented here are fully validated and conform to Extreme Best Practices and recommendations. The intention of this Extreme Validated Design document is to provide reference configurations and instruction for building a managed, secure campus network using Extreme Fabric Connect, Extreme Fabric Attach access switches, ExtremeWireless architectures and Extreme Management.

Other reference materials should be reviewed for a deeper understanding of the concepts described in this document.

Note

Refer to the Automated Campus At-A-Glance and Solutions Brief for overall solution information.

Technology Overview

Terminology

Term	Description
802.1X	IEEE Standard for port-based Network Access Control
AD	Active Directory
AP	Access Point
ARP	Address Resolution Protocol
BCB	Backbone Core Bridge
BEB	Backbone Edge Bridge
B-VLAN/B-VID	Backbone VLAN
CLI	Command-Line Interface
CoS	Class of Service for Layer 2
CVLAN	Customer VLAN
DHCP	Dynamic Host Configuration Protocol
DDD	Domain Data Distribution
EAPOL	Extensible Authentication Protocol Over LAN
ECMP	Equal Cost Multi-Path
EXOS	Extreme eXtensible Operating System (also ExtremeXOS)
FDB	Forwarding Database
GRT	Global Routing Table
IGMP	Internet Group Management Protocol
IP	Internet Protocol
I-SID	Individual Service Identifier
ISL	Inter-Switch Link
L2VSN	Layer 2 Virtual Service Network
L3VSN	Layer 3 Virtual Service Network
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
NAC	Network Access Control
NNI	Network to Network Interface
PoE	Power over Ethernet
QoS	Quality of Service
sFlow	Sampled Flow
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SPBM	Shortest Path Bridging (MAC)
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UNI	User to Network Interface
VLAN	Virtual Local Area Network
VM	Virtual Machine
VOSS	VSP Operating System
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding

Extreme Automated Campus - Introduction

The key benefit of an Extreme Automated Campus solution is the inherent end-to-end automation capabilities reducing installation and operations complexities dramatically. The zero-touch core capabilities together with the end-point-provisioning model simplifies network tasks greatly. It allows network operators to focus on new projects rather than spending time “keeping the lights on”. The Automated Campus spans from the wireless to the wired edge into the core aggregation layer and can also be extended into the server rooms.

Enterprise network operators are providing connectivity services to their internal customers. Like telecom service providers they can benefit from a model where there is a clear separation of infrastructure and connectivity services. With Automated Campus (AC), connectivity services are called Virtual Services Networks (VSNs). There are VSNs available for extending VLANs across an AC (L2 VSNs) as well as extending routing domains (VRFs) across an AC (L3 VSNs). Those services can run IPv4 and IPv6 routing functions. Also, it is very easy to provide a highly scalable and robust IP multicast solution, that is very easy to configure and maintain.

The tight integration of Extreme Access Switches and Extreme wireless and its consistent powerful role-based policy framework enables a highly capable end-to-end solution. Wireless or wired users can connect anywhere to the network and will get their appropriate network role and rules assigned as well as end up in the predefined network segment. This is particularly important when network segmentation has been deployed for security and or compliance purposes.

Interfacing an Automated Campus with any third-party network infrastructure can easily be achieved by connecting VLANs over 802.1Q tagged links and adding routing protocols such as RIP, OSPF or BGP to exchange IPv4 or IPv6 routes, or using PIM-SM with MSDP for Multicast domain connections.

In this EVD, the Extreme Automated Campus provides QOS, bandwidth, POE, Network Access Control, redundancy, and visibility across local or remote geographical locations. This gives the IT operator an opportunity to provide appropriate levels of access for different user groups without disrupting connectivity on a shared network.

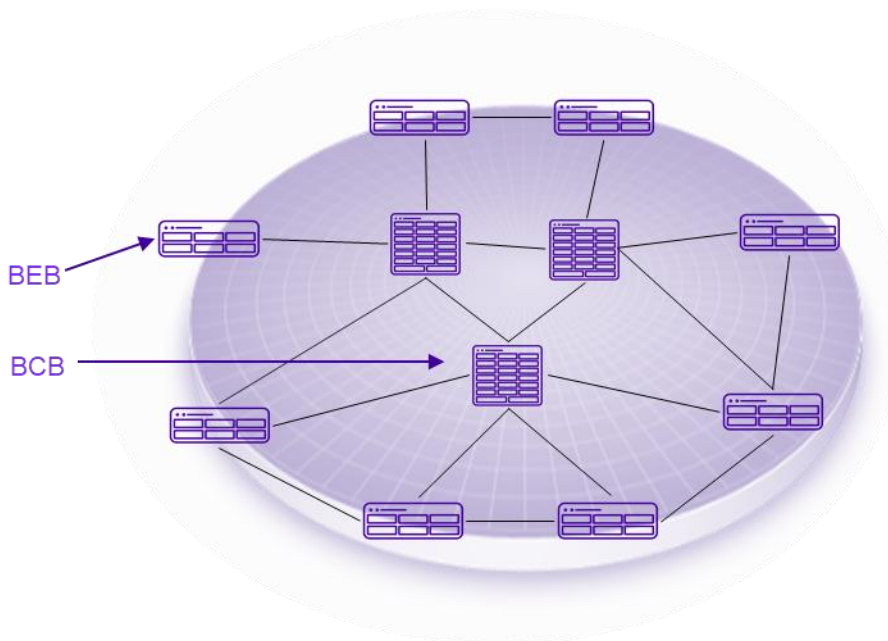
Functional Components of Extreme Automated Campus

An Extreme Automated Campus consists of three main functional areas:

- Extreme Fabric Connect and Fabric Attach
- ExtremeWireless
- Extreme Management Center's Policy and Network Access Control with Analytics

Extreme Fabric Connect: Core and Aggregation

The Automated Campus, utilizing Extreme's Fabric Connect technology, is comprised of two functional elements: An edge switch function, called a Backbone Edge Bridge (BEB) and a core switch function, called a Backbone Core Bridge (BCB). The fabric connecting these switches is SPB (Shortest Path Bridging), based on the IEEE 802.1aq standard. SPB uses IS-IS (RFC 6329) as the control plane routing protocol. A Fabric Connect capable switch supports all traditional network protocols and in addition the Fabric Connect SPB function. In typical designs switches operate as BEBs and BCBs concurrently.



Fabric Connect supports Layer 2 and Layer 3 virtualization. These virtualized Layer 2 (L2) and Layer 3 (L3) instances are referred to as Virtual Services Networks (VSNs). A Service Identifier (I-SID) is used to uniquely identify each of these service instances in a Fabric Connect domain and a User Network Interface (UNI) is the boundary or demarcation point between the "service layer" of traditional networks i.e. VLANs, VRFs and the Fabric Connect "service layer" i.e. L2 & L3 VSNs.

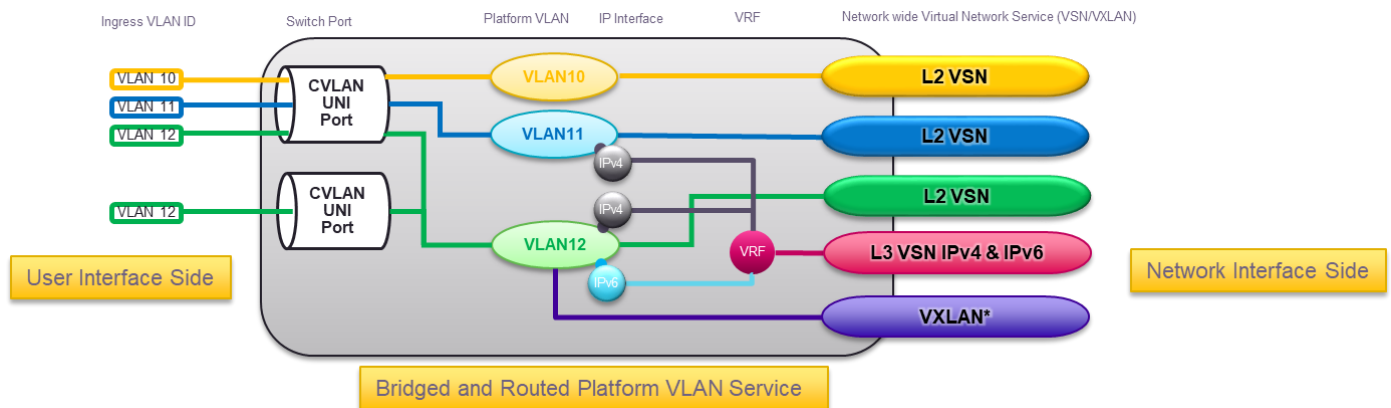
- Layer 2 VSNs form a virtual broadcast domain between UNI members that share the same L2 VSN ISID. MAC learning/aging is applied to all L2 VSNs individually.
- Layer 3 VSNs form a virtual routed L3 network (L3 VPN) leveraging IS-IS as the routing protocol between VRFs that share the same L3 VSN ISID.

Once the SPB infrastructure is created, the SPB network connectivity services (VLAN or VRF extensions) are configured on the BEB's at the edge of the network only. There is no provisioning required on the core SPB switches for network connectivity services. This provides an architecture where the configuration on the core switches never needs to be modified when adding any new services.

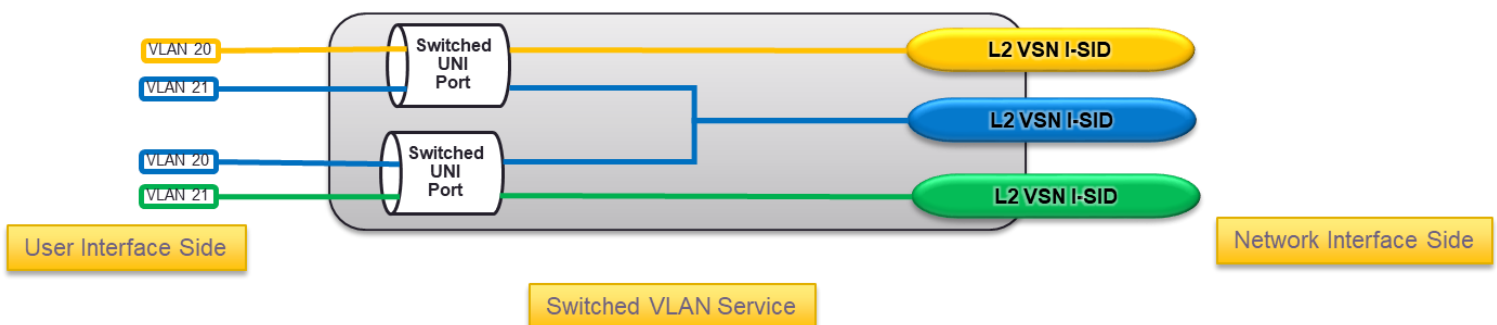
The boundary between the core SPB domain, which consist of Network-to-Network (NNI) interfaces and the access interfaces, is handled by a so-called User Network Interface (UNI). UNI interfaces tie VLANs or VRFs to Service Instance Identifier (I-SID). An I-SID is provisioned on the BEB UNI interface.

Fabric connect devices support the following UNI types:

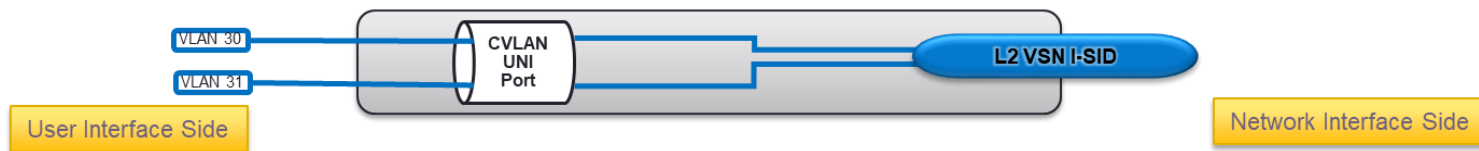
- VLAN UNI (CVLAN) a Platform VLAN-ID maps to a L2 VSN I-SID – all ports that are members of the VLAN are associated with the UNI.
 - CVLAN UNI interface can have an IPv4 or IPv6 address assigned to it to enable a routing function.



- Flex UNI interface has the following sub-types:
 - Switched UNI: maps a VLAN-ID on a given port (VID, port) into a L2 VSN ISID. With this UNI type VLAN-IDs can be re-used on other ports and map to different ISIDs.



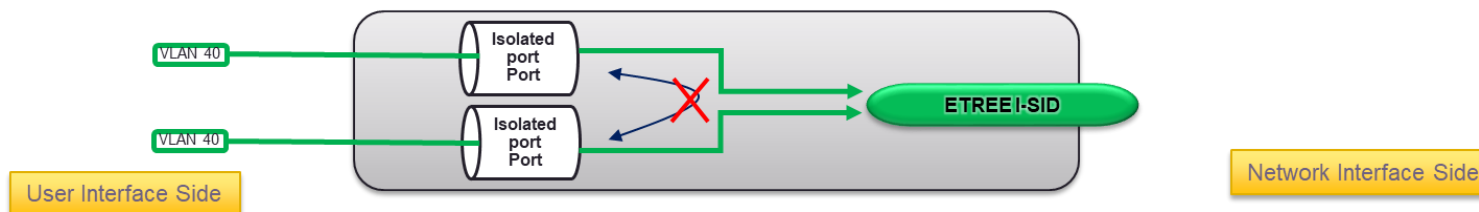
- Transparent Port UNI- a port maps to a L2 VSN I-SID (all traffic through that port, 802.1Q tagged or untagged, ingress and egress is part of the I-SID).



Warning

All VLANs on a transparent port UNI interface share the same SINGLE MAC learning table of the Transparent UNI ISID.

- E-Tree UNIs allow extending Private VLANs beyond one switch to form a network wide E-Tree service infrastructure. An E-Tree UNI is a L2 VSN where traffic flows from hub to spokes and from spokes to hubs, but not from spoke to spoke. E-Tree hub ports can be formed with a CVLAN or Switched VLAN UNI. E-Tree spokes need to be configured as private VLAN UNIs.



- L3 VSN UNI - a VRF maps to an I-SID. A L3 I-SID identifies, in the control plane, all L3 routes belonging to the same I-SID. All VRFs in a network sharing the same L3 I-SID form a L3 VSN. L3 VSNs support IP Unicast as well as IP Multicast simultaneously if configured to do so. A special case is VRF=0 which corresponds to the Global Routing Table (GRT), SPB based routing for GRT is called IP Shortcut routing.



Figure 1 L3 VSN

I-SID configuration is required only for virtual services such as L2 VSN and L3 VSN. With IP Shortcuts, no I-SID is required as forwarding is performed by utilizing the Global Routing Table (GRT).

Default Gateway Redundancy:

There are multiple ways to provide default gateway redundancy to users and hosts.

- VRRP
- RSMLT
- Distributed Virtual Routing

Note

In this EVD we have chosen to use RSMLT and DVR. They provide optimized traffic flows and robust deployment models, over a traditional chatty VRRP approach. But nothing is precluding the use of VRRP instead of RSMLT or DVR, especially in smaller deployments.

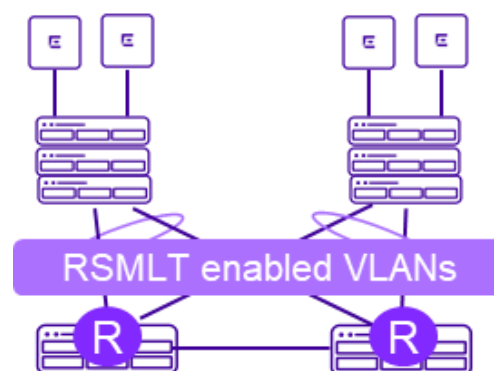
In this document, two of the three core switches, are also configured as DVR Controllers which distribute a routing instance to the switches in the server areas. Virtual machines, which can roam freely across any server, use their first hop Top of the Rack (ToR) switches (DVR Leaf nodes) to be their default gateways. In the wireless deployments, users can roam between “buildings” and each building provides default gateway routing capabilities for the users, thus distributing the load and optimizing traffic patterns. DVR avoids traffic “tromboning” and optimizes traffic paths and thus effectively reduces latency in real-time applications such as voice and video.

Each server area is comprised of two VSP-7xxx ToR switches, which are directly connected to the services required by all the clients connected to either campus. These services include production servers, storage, video servers as well as DHCP/DNS servers. These units are also configured as DVR Leaf nodes, which provide the flexible, low latency IP access roaming users require. In addition, this segment of the testbed contains the management application for the entire testbed, which is performed by XMC.

DVR controllers and DVR Leaf nodes can be extended based on port connectivity and bandwidth needs.

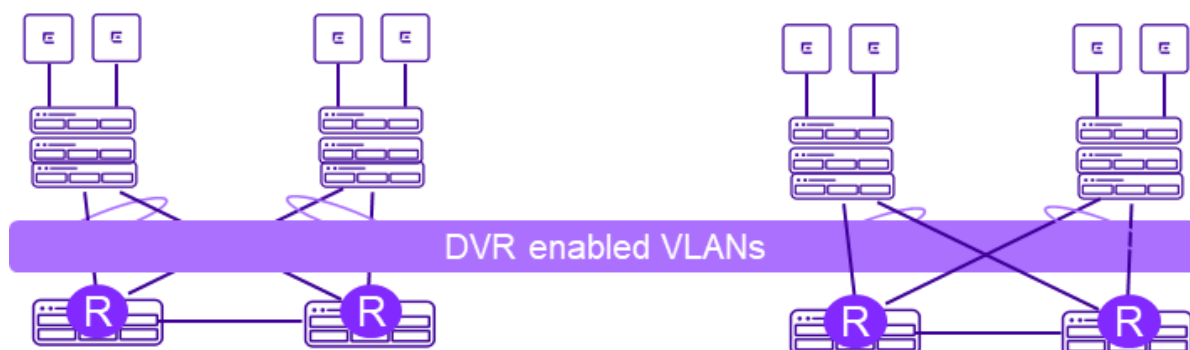
Routed Split Multi-Link Trunking (RSMLT)

One method for IP Gateway redundancy is available within each switch cluster at the campuses for VLAN's/hosts which do not require mobility. RSMLT ensures traffic can be routed off the VLAN by adding routed VLAN redundancy. RSMLT is similar in functionality to VRRP (providing router gateway redundancy), however it can scale beyond the maximum number of VRRP instances, it is a considerably less “chatty” protocol, thus reducing network overhead and it can provide sub-second failover performance without the need to modify any L3 protocol timers. RSMLT has a limit of two nodes per switch cluster.



Distributed Virtual Routing (DVR)

Distributed Virtual Routing (DVR) is a technology that provides a distributed default gateway functionality for access VLANs/IP subnets. It distinguishes itself from VRRP or RSMILT in the fact that it is highly effective when more than 2 default gateway routers are available in a VLAN/IP subnet.



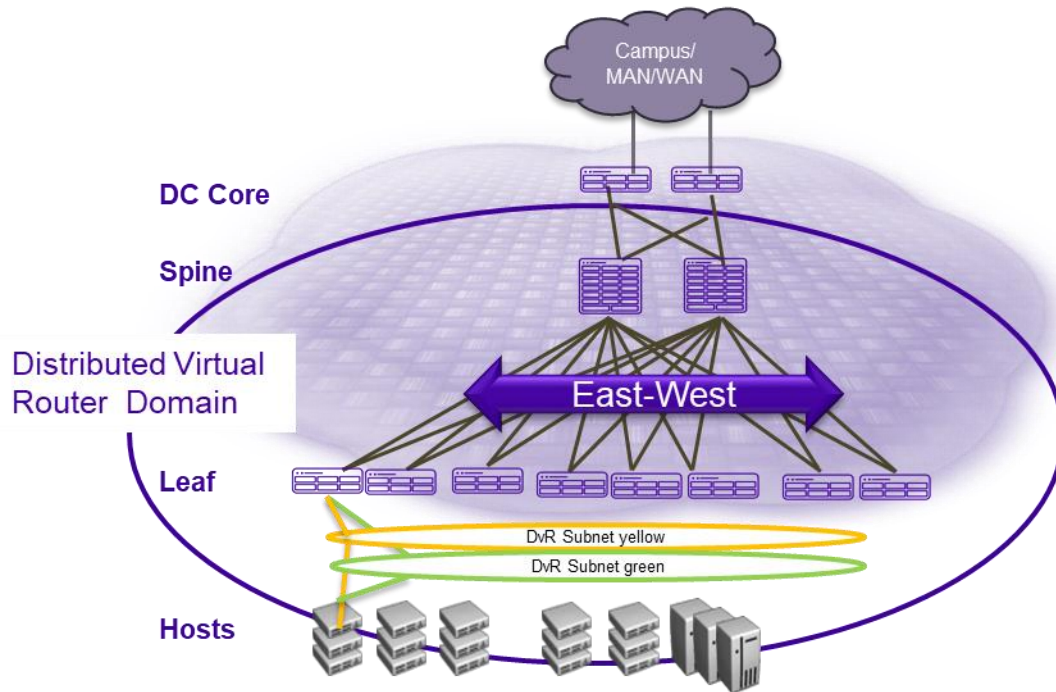
In addition, DVR optimizes traffic flows to avoid traffic "tromboning" due to inefficient routing, thereby increasing the total routing throughput. DVR also simplifies large scale server room deployments by introducing a Controller-Leaf architecture. In this architecture, Layer 3 IPv4 default gateway and VRF configuration is required only on the Controller nodes, whereas the Leaf nodes require only Layer 2 configuration. All Layer 3 configuration, including IP multicast configuration, is automatically distributed to the Leaf nodes by the Controller nodes.

DVR Domains

A DVR domain is a logical group of switches or nodes that are DVR enabled. These nodes are not physically connected but are connected over the SPB Fabric such that each node is aware of the BMAC addresses of all other nodes within the domain. A logical DVR domain cannot contain nodes that are not DVR enabled. However, those nodes can co-exist with other DVR enabled nodes within the same SPB Fabric network.

A common DVR domain ID is configured for all nodes belonging to a DVR domain. This domain ID translates internally to a Domain Data Distribution (DDD) I-SID. All switch nodes that share the same DVR domain ID or DDD ISID receive the Layer 3 information that is distributed from all other nodes belonging to that DVR domain.

A DVR domain can contain multiple Layer 3 VSNs and Layer 2 VSNs. Layer 2 and Layer 3 VSNs can span multiple DVR domains. DVR domains are typically introduced when multiple buildings come into play. Typically, a DVR domain spans one building which includes an access and distribution layer, this could be campus or data center. A remote building would be its own DVR domain. This ensures that the DVR controllers are local to the building and thus only local DVR Leaf nodes are served by the controllers. Up to 8 controllers can be used per domain. Up to 16 domains can be built with DVR. A DVR backbone is automatically established between the DVR controllers and is responsible for traffic and host information forwarding between domains.



Although not always, a DVR domain typically has the following components:

1. DVR Controllers
2. DVR Leaf nodes

DVR Controller

In a DVR domain, the Controller nodes are the central nodes on which Layer 3 is configured. They own all the Layer 3 configuration and push the configuration information to the Leaf nodes within the SPB network. A DVR domain can have one or more controllers for redundancy and you must configure every Layer 2 VSN (VLAN) and Layer 3 VSN within the domain, on the Controller(s). A node configured as a DVR Controller is considered the controller for all the Layer 2 and Layer 3 VSNs configured in its DVR domain. A Controller is configured with its own subnet IP address, for every DVR enabled Layer 2 VSN within the domain.

All Layer 2 VSNs on a DVR Controller need **not** be DVR enabled. A controller can be configured with individual Layer 2 VSNs that are DVR disabled and use VRRP for example. The Layer 3 configuration data that is pushed to the Leaf nodes include the Layer 3 IP subnet information for all Layer 2 VSNs within the DVR domain. Controllers also send information on whether Multicast is enabled on a specific DVR enabled Layer 2 VSN, and the version of IGMP. A Controller can only belong to one DVR domain, based on the domain ID configured on the node.

DVR Leaf

DVR Leaf nodes are typically data center top of the rack (ToR) Fabric switches that aggregate physical and virtual servers or storage devices. DVR Leaf nodes operate in a reduced configuration mode, where Layer 3 is not configured locally, but pushed to them from the DVR Controller(s) within the domain. You need to configure only the IS-IS infrastructure and the Layer 2 VSNs on the Leaf nodes.

Once on a controller a DVR virtual default gateway IP address is configured for a L2 VSN, DVR Leaf nodes monitor local host attachments and communicate updates about the current state of those host attachments to the DVR domain. All DVR nodes exchange host attachment information using the DVR host distribution protocol, which leverages a DVR domain ISID. DVR leaf nodes are managed in-band through a local loopback address, and management traffic is IP Shortcut routed.

A Leaf node will also distribute host route information within the DVR domain that it owns (i.e. ARPs). A Leaf node learns ARPs on its own UNI ports. It will own this locally learned ARP and will distribute those as host routes to all other DVR enabled nodes (all Controller nodes and Leaf nodes) within the DVR Domain. In this way, all the DVR enabled nodes will have all the L3 host reachability information of the entire DVR Domain. Hosts connected to Leaf nodes (ToRs) will know how to reach all other hosts in the DVR Domain directly via this distributed L3 data path. The Fabric is used to enable short cut routing.

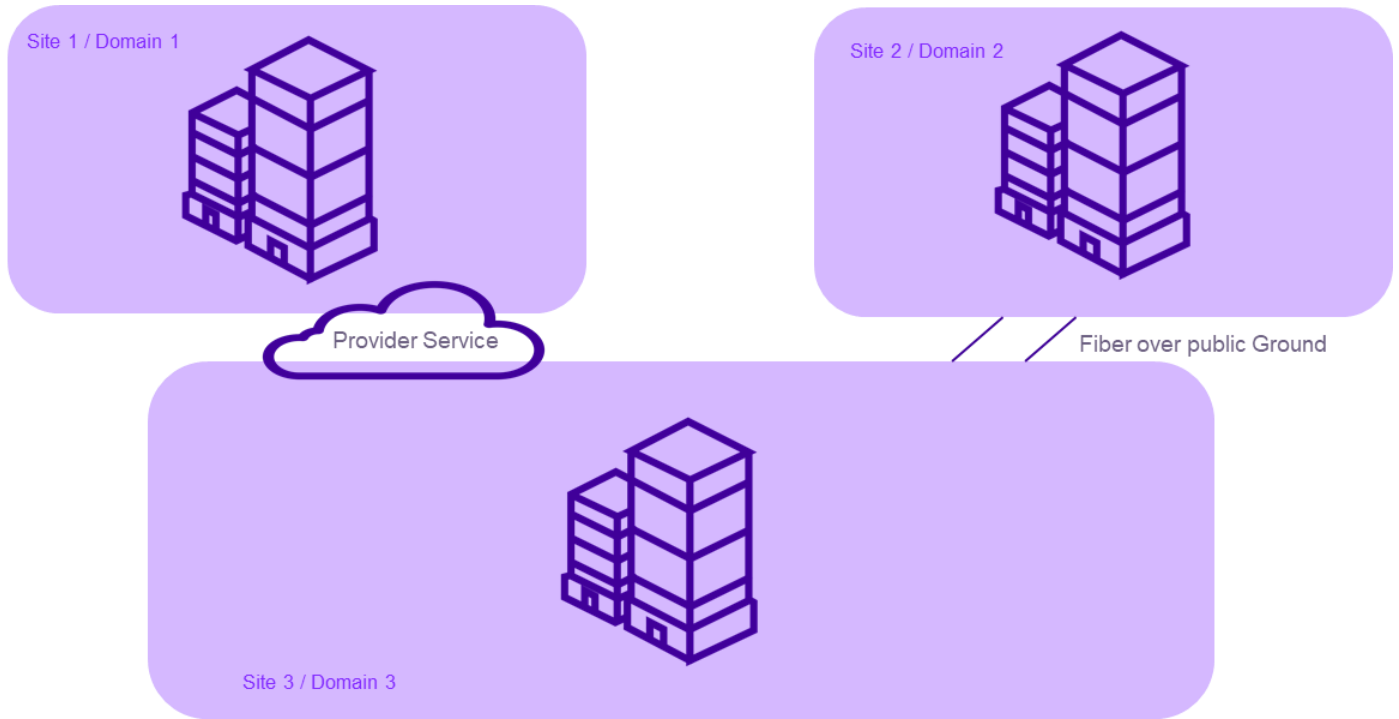
Leaf nodes will have limited manual configuration. SPB infrastructure will be manually configured. ISIDs will be manually configured for L2VSNs. There will be no platform VLANs configured on a Leaf that is DVR enabled. L3 configuration data will be learned from the Controller for IPv4 Unicast and IPv4 Multicast. For every L2VSN configured on the Leaf, it must also be configured on the Controllers in that DVR Domain.

DVR Backbone

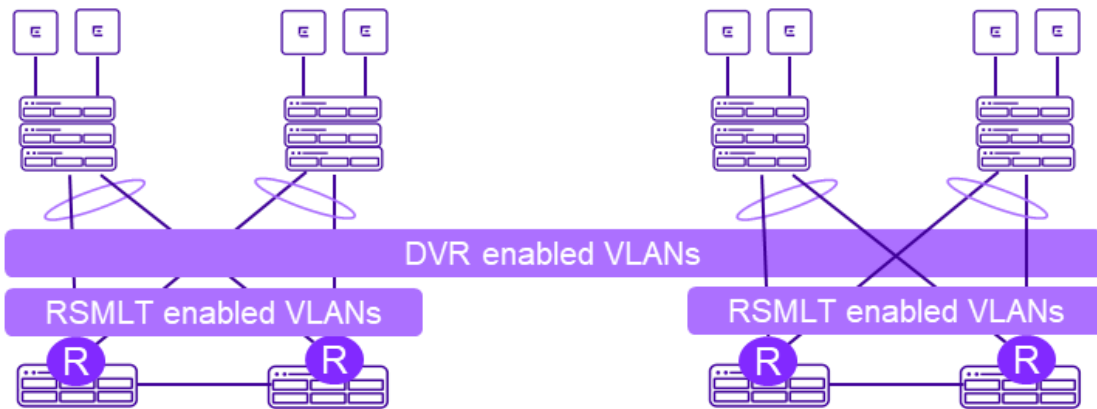
The DVR backbone is automatically established between all DVR controllers in a fabric. The DVR controllers exchange all host route information among themselves to ensure short-cut switching to the domains and hosts wherever they might connect. DVR controllers either forward directly to their local Leaf nodes, if the hosts are local to their domain, or forward traffic to the remote domain controllers, if the hosts are remote. The leaf nodes in contrary only know about their local hosts in their domain and forward to their controllers if traffic is not local to their domain.

The Automated Campus EVD DVR domains:

The Automated Campus EVD has three DVR domains: one encompassing both server rooms and one in each campus. As mentioned previously, it is best to create DVR domains so that controllers for a domain are local to their corresponding Leaf nodes if possible, such that in case of an isolation of a building, controllers are local to the building.

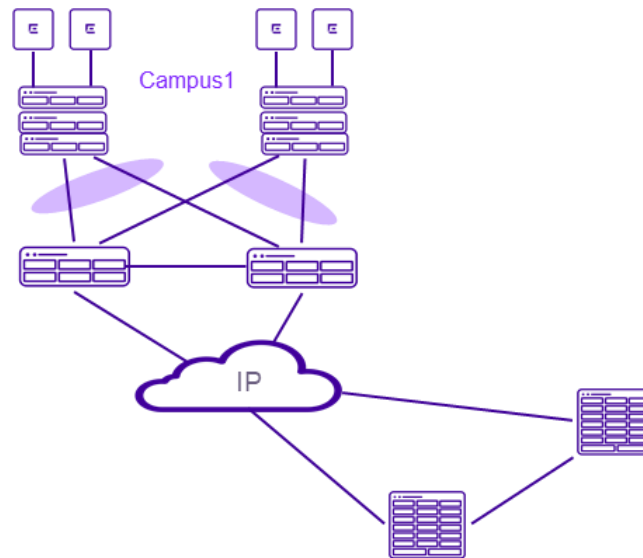


The IoT, Administrator and Campus User wireless VLANs are members of the DVR domains in the campuses. All subnets in the server rooms are members of the DVR Domain spanning across both server room locations.



Fabric Extend

Fabric Extend provides the ability to extend the Fabric Connect Ethernet Fabric over an IP routed network. This IP routed network can be any type of IP routed connectivity for example a campus router or an MPLS IP VPN connectivity. What must be ensured is that this routed network supports larger IP packets with minimum frame size of 1594 bytes. A good guidance is to ensure that minimum packet size support is 1600 bytes. If a third-party device is used for connecting Fabric Connect over the internet, it should support encryption as well as fragmentation and reassembly. It is necessary to ensure IP packets are not only fragmented but also re-assembled after the secure tunnel to ensure that Fabric Connect Ethernet packets are reconstructed after the secure tunnels.



Access Layer

The Access layer for the Automated Campus EVD can be comprised of Summit or ERS access switches. Both access switch models in this EVD support stacking mode and are operating as FA proxy devices.

Summit Access

The Summit access switches are in separate stack formations. Combining the switches in stack formation allowed for easier administration of the switches.

Among other features, the Summit access switch supports Policy and Fabric Attach, both of which are required in the overall functionality of this topology. With defined Policy roles, rules can be created based upon up to 15 traffic classification types for traffic drop or forwarding. A CoS (Class of Service) can be associated with each role for purposes of setting priority, forwarding queue, rate limiting, and rate shaping. The Extreme Management Center is ideal for creating and maintaining Policy rules within the access switches and is used in this topology. Fabric Attach facilitates automated network device discovery and the automatic configuration and teardown of Network Services Identifier (NSI)/Individual Service Identifier (ISID) to VLAN associations at the edge of the network, which eliminates time-consuming hop-by-hop provisioning.

At least one switch in each stack is capable of PoE (Power over Ethernet). PoE supplies 48 VDC power to certain types of powered devices through Category 5, Category 5E and Category 6 twisted pair Ethernet cables. Devices such as wireless access points, IP telephones, laptop computers, and web cameras do not require separate power cabling and supply with these PoE-capable switches.

ERS Access

The ERS access series integrates Fabric Attach and Extensible Authentication Protocol (EAP) capabilities in an efficient and easy way. Fabric Attach (FA) provides automated VLAN and SPB virtual service connection from ERS switches running in FA Proxy mode or from any end device supporting FA Client mode of operation, such as Extreme WLAN Access Points.

The ERS series is also offered with the Universal Power-over-Ethernet models that can offer twice the power of PWR+ providing up to 60 Watts of power on access ports. This capability can be used to support a greater range of high power devices through a single standard Ethernet cable, such as premium telepresence systems, multi-radio Wireless Access Points, VDI Thin Clients and monitors, downstream compact Switches, and even PoE-power smart lighting systems.

Note

Although not part of this EVD, the ERS 36xx access switch has full FA proxy functionality, and would also be supported in this design.

ERS 59xx/ERS 49xx are SPBM-capable network devices and can also run as a FA Server or FA Proxy. For the purpose of this EVD, ERS access switches are configured as FA Proxy devices.

ExtremeWireless

ExtremeWireless is simple, fast, and smart, delivering a user experience in unmatched scale and density at an exceptional level. Intuitive Dashboards allow effortless management of the network. With a single click, deliver services and new applications with ease. Enable fast roaming with seamless mobility while delivering more throughput with fewer APs. Able to be agile through an advanced architecture that assures security with enforcement. Through analytics, user experience can be measured in true detail.

Access Points can initialize and configure themselves from a centralized appliance. Deployed APs automatically discover the appliance through DHCP and retrieve its configuration. Policy and QoS are performed at the AP for clients connecting to a SSID. RF Characteristics can be automatically configured by the AP through automatic power or channel selection. Band-Steering and Airtime Fairness are also controlled by the AP.

The ExtremeWireless designs provide the same availability that everyone has come to expect with wired networks. Appliances have built-in resiliency through the ability to pair controllers together for full redundancy.

Extreme Management Center

What makes the Extreme Automated Campus possible is the deployment of Extreme Management Center, consisting of Extreme Management, ExtremeControl, and ExtremeAnalytics. These tools are the backbone to managing and configuring the functionality of the Extreme Automated Campus solution.

Extreme Management

Extreme Management Center is a single pane of glass management system that provides wired/wireless visibility and control from the data center to the mobile edge. The intelligence, automation, and integration of this management software enables the IT organization to optimize the efficiency of network operations and reduce total cost of ownership. Most important, Extreme Management Center provides advanced network configuration and change management for the wired and wireless infrastructure and allows centralized creation of policies that follow users and devices across the network. These are not tied to the physical network and can change based on user, device, time of day, location, and connection type.

ExtremeControl

Extreme's Network Access Control engine, or ExtremeControl, lets you manage secure and automated access for both BYOD and IoT devices from one convenient dashboard. It makes it easy to roll out granular policies across your wired and wireless networks to meet industry and company compliance obligations. Identity-based network access control keeps unauthorized users and devices from accessing your network. ExtremeControl is integrated with Extreme Management Center to allow for simple and seamless authentication control and modification in one single application.

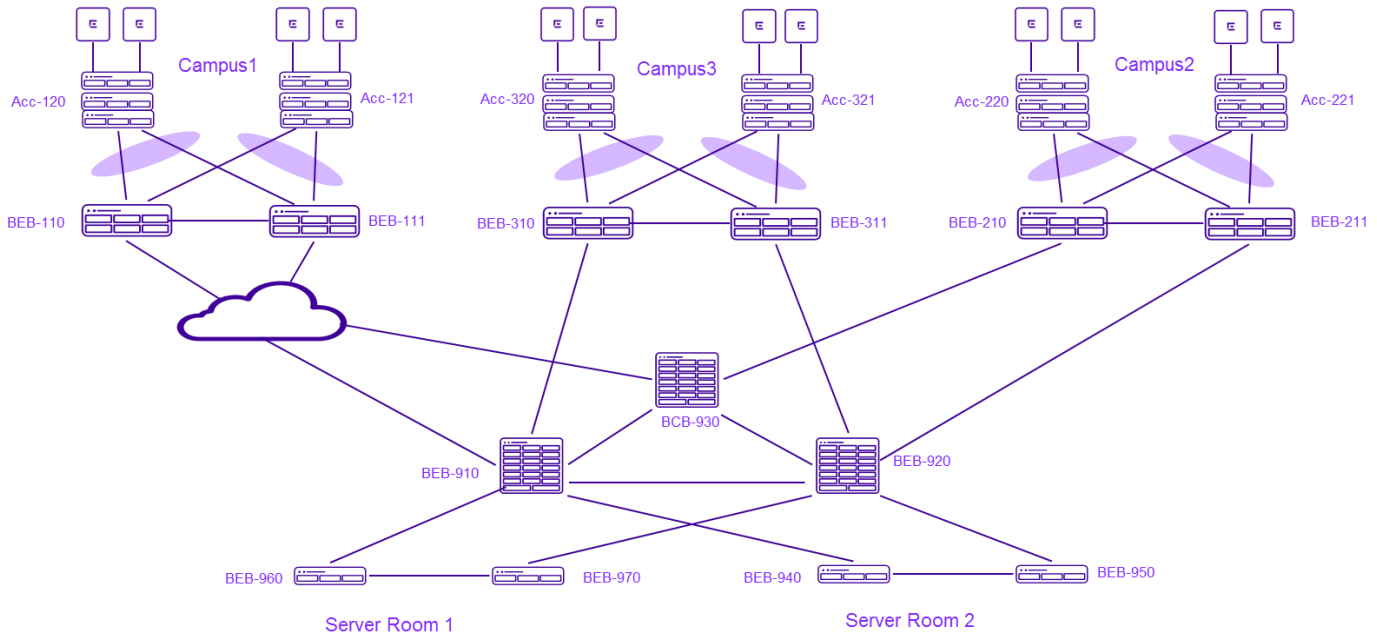
ExtremeAnalytics

ExtremeAnalytics helps administrators understand what applications are running on the network, who is using them and what the response time is for each application. It gives granular visibility into network and application performance, users, locations, and devices. Information from the network and the applications empowers you to make data-driven decisions.

Validated Designs – Infrastructure & Topology

Automated Campus Reference Topology

The reference topology is comprised of three “campus” areas and two “server room” areas. The key technology is Extreme Fabric Connect with Fabric Attach and Fabric Extend. Each of the campuses are composed of two, linked VSP-8xxx units, configured as BEB’s, which are directly connected to dual homed Summit or ERS switches, functioning as the Access layer.



The uplinks of the access switches to the VSP BEB’s is accomplished via the configuration of link aggregation. Fabric Attach technology fully automates the process of client authentication and service (L2VSN/L3VSN) assignment. Routing redundancy is also enhanced via the use of both DVR (Distributed Virtual Routing) as well as RSMLT (Routed Split Multilink Trunk).

The connectivity to the core on each campus varies and encompasses different Fabric Connect capabilities. Campus 1 is linked to the core BCB switches via technology known as Fabric Extend, which is in effect an L3 tunnel used to facilitate connectivity of two SPB networks over a traditional IP network.

The core area utilizes three VSP-8xxx units, configured as BCB’s and linked directly via point-to-point 40Gb connections, except for the L3 tunnel links to Campus 1 which are configured via 10Gb links. The core topology can consist of any number of backbone nodes, depending on the actual fiber plant layout and port count requirements. The three-node core setup has only been chosen to illustrate the topology flexibility.

Hardware and Software Matrix

Product	FW Version	Enabled License Level	Enabled Feature Packs
X460-G2	22.6.1.4	Advanced Edge	Direct Attach
ERS-4950GTS	7.6.1.033		
ERS-5928GTS	7.6.1.033		
VSP-8404C	7.1.0.0.GA	Premier	
VSP-8284	7.1.0.0.GA	Premier	
VSP-7200	7.1.0.0.GA	Premier	
EWC V2110	10.41.11.0009		
AP3912i-FCC	10.41.11.0009		
AP3915e-FCC	10.41.11.0009		
AP3915i-FCC	10.41.11.0009		
AP3916ic-FCC	10.41.11.0009		
AP3917e-FCC	10.41.11.0009		
AP3935e-FCC	10.41.11.0009		
AP3935i-FCC	10.41.11.0009		
Extreme Management Center	8.1.4.40		
ExtremeControl	8.1.4.40		
ExtremeAnalytics	8.1.4.40		

Preconditions

Before beginning the configuration of any device in the Extreme Automated Campus Validated Design, verify that the following preconditions have been met:

Summit Access Switches

```
Slot-1 Stack.1 # show license
Enabled License Level:
  Advanced Edge
Enabled Feature Packs:
  DirectAttach
Effective License Level:
  Advanced Edge
```

There is no minimum license level requirement on Summit switches for this EVD.

ERS Access Switches

```
5900_STACK(config)#show license
No license installed
5900_STACK(config)#
```

No minimum license level requirement on ERS switches for this EVD.

Fabric Connect Switches

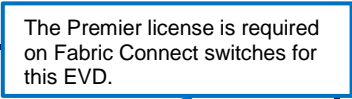
```
BEB-8284-110:1(config)#show license
```

```

License file name      : /intflash/VSP8284_B0ADAA47BC00.xml
License Type          : PREMIER (includes Base features) +PORT
MD5 of Key            : 00000000 00000000 00000000 00000000
MD5 of File           : 00000000 00000000 00000000 00000000
Generation Time       : 2018/05/22 02:21:13
Expiration Time       :
Base Mac Addr         : b0:ad:aa:47:bc:00
flags                 : 0x00000001 SINGLE
memo                  :

```

The Premier license is required on Fabric Connect switches for this EVD.



```
BEB-7254-960:1(config)#show license
```

```

License file name      : /intflash/VSP7254_D47856945C00.xml
License Type          : PREMIER (includes Base features) +PORT
MD5 of Key            : 00000000 00000000 00000000 00000000
MD5 of File           : 00000000 00000000 00000000 00000000
Generation Time       : 2018/05/22 02:21:13
Expiration Time       :
Base Mac Addr         : d4:78:56:94:5c:00
flags                 : 0x00000001 SINGLE
memo                  :

```


Campus VLAN/I-SID and Subnet Scheme

Several functional groups were created to simulate common generic services on the network. It's also a common best practice to have separate VLANs for wired and wireless networks to avoid unneeded broadcasts saturating the wireless network, illustrated in the campus/common VLAN scheme.

The same VLAN services are available in both campuses, however different features are illustrated to demonstrate levels of redundancy and mobility for these services.

I-SID scheme

It's a good practice to have a VLAN/I-SID scheme that is logically laid out in a way that easily identifies the network/services and allows growth. The 24-bit I-SID header field allows for 16 million services.

Digit 1: Campus System Identifier

- This Automated Campus EVD is designating the first digit to identify this particular autonomous system or fabric (which includes both Server rooms and Campuses = 1).
- If another large campus is acquired or created, and some delineation wanted to be made between them, this digit could be increased to "2" to identify it.

Digits 2-3: Service Type/Location

- Services tied to specific sites are denoted "0x" (campuses = 01/02/03, server rooms = 09).
 - o Services extending from the campuses to the Server Rooms (i.e. Wired IoT-Bridged, Guest) will use the location id of the Server Room (09), as that is their common point.
- "Common" VLANs (existing in both campuses) as a result of DVR = 50.
- VRF I-SID = 80

Digits 4-7: VLAN id

- A 4-digit value was allocated for the VLAN.
- The VLAN IDs within a VRF I-SID will reflect the corresponding VLAN ID in the server rooms.

Campus 1 (VLAN 1xx):

Role/Segment	VLAN	ISID	Subnet	Def Gateway	VRF	VRF ISID
FA Mgmt. VLAN	100	1010100	172.10.10.0/24	RSMLT	GRT	N/A
Wired IoT (routed)	101	1010101	172.10.20.0/22	RSMLT	VRF 1	1800911
Net Admin (wired)	102	1010102	172.10.24.0/22	RSMLT	GRT	N/A
Campus User(wired)	103	1010103	172.10.28.0/22	RSMLT	GRT	N/A
Surveillance	104	1010104	172.10.32.0/22	RSMLT	VRF 2	1800904

Campus 2 (VLAN 2xx):

Role/Segment	VLAN	ISID	Subnet	Def Gateway	VRF	VRF ISID
FA Mgmt. VLAN	200	1020200	172.20.10.0/24	RSMLT	GRT	N/A
Wired IoT (routed)	201	1020201	172.20.20.0/22	RSMLT	VRF 1	1800911
Net Admin (wired)	202	1020202	172.20.24.0/22	RSMLT	GRT	N/A
Campus User(wired)	203	1020203	172.20.28.0/22	RSMLT	GRT	N/A
Surveillance	204	1020204	172.20.32.0/22	RSMLT	VRF 2	1800904

Campus 3 (VLAN 3xx):

Role/Segment	VLAN	ISID	Subnet	Def Gateway	VRF	VRF ISID
FA Mgmt. VLAN	300	1030300	172.30.10.0/24	RSMLT	GRT	N/A
Wired IoT (routed)	301	1030301	172.30.20.0/22	RSMLT	VRF 1	1800911
Net Admin (wired)	302	1030302	172.30.24.0/22	RSMLT	GRT	N/A
Campus User(wired)	303	1030303	172.30.28.0/22	RSMLT	GRT	N/A
Surveillance	304	1030304	172.30.32.0/22	RSMLT	VRF 2	1800904

Server Room (VLAN 9xx):

Role/Segment	VLAN	ISID	Subnet	Def Gateway	VRF	VRF ISID
Production Servers	900	1090900	172.90.1.0/24	DVR	GRT	N/A
Test Servers	901	1090901	172.90.2.0/24	DVR	GRT	N/A
Storage Servers	902	1090902	172.90.3.0/24	DVR	GRT	N/A
Storage Test	903	1090903	172.90.4.0/24	DVR	GRT	N/A
Network Mgmt.	999	1090999	172.9.99.0/24	DVR	GRT	N/A
Network Mgmt. (EWC)	998	1090998	172.9.98.0/24	DVR	GRT	N/A
Wired IoT (routed)	911	1090911	172.90.20.0/22	DVR	VRF 1	1800911

Surveillance	904	1090904	172.90.14.0/22	DVR	VRF 2	1800904
Wired IoT (bridged)	907	1090907	N/A	N/A	L2VSN	N/A

Common Services:

Role/Segment	VLAN	ISID	Subnet	Def Gateway	VRF	VRF ISID
Net Admin(wireless)	1050	1501050	172.105.0.0/24	DVR	GRT	N/A
Campus Users (wireless)	1051	1501051	172.105.1.0/24	DVR	GRT	N/A
IoT Devices (wireless)	1052	1501052	172.105.2.0/24	DVR	VRF 1	1800911
Guest (wireless)	906	1090906	172.90.40.0/24	EWC	Tunnel	N/A
Wired IoT(bridged)	907	1090907	N/A	N/A	L2VSN	N/A

Fabric Connect - Core Configuration

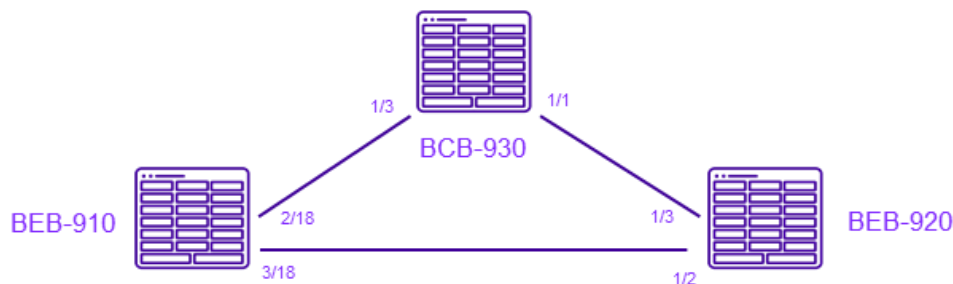
Overview

The initial SPBM/IS-IS configuration is identical for both BCB and BEB switches. Most Ethernet-based networks use 802.1Q tagged interfaces between the routing switches. SPBM uses two Backbone VLANs (B-VLANs) that are used as the transport instance. A B-VLAN is not a traditional VLAN in the sense that it does not flood unknown, broadcast or multicast traffic, but only forwards based on IS-IS provisioned backbone MAC (B-MAC) tables. After configuring the B-VLANs and the IS-IS protocol is operational, services can be mapped to service instances.

The Fabric Connect switches are managed via XMC in-band through the default routing instance (GRT), using configured loopback addresses, illustrated in the following sections. Network discovery/management will be performed using these addresses, by means of the “**clipld-topology-IP**” command.

Note

Please refer to **Design Considerations** for other features that are required or will enhance and optimize the Automated Campus Solution.



BCB-930 Configuration

1. Globally enable 'SPBM', and configure a loopback interface used for in-band management of the switch:

```
config terminal
prompt "CORE-8404-930"
spbm

interface loopback 1
ip address 1 10.0.0.30/255.255.255.255
exit
```

Globally enable SPBM.

Configure the loopback IP address to be used for in-band

2. Configure IS-IS parameters:

```

router isis
  spbm 1
  spbm 1 nick-name 0.09.30
  spbm 1 b-vid 4051-4052 primary 4051

  ip-source-address 10.0.0.30
  spbm 1 ip enable

  sys-name "CORE-8404-930"
  system-id 00bb.0000.3000
  manual-area 49.0000
  exit
  
```

Enter an IS-IS instance and "nick-name" for this switch (format: x.xx.xx).

Assign the Backbone VLANs to SPBM.

Enable IP on SPBM to allow IP Shortcut routing across the GRT.

Set the switch's sys-name and change the IS-IS system ID from the default B-MAC value to a recognizable address (format: xxxx.xxxx.xxxx).

Configure the SPBM autonomous system number for this Fabric

3. Create a loopback interface which will be used for in-band management of the switch, and enable IP Shortcut functionality:

```

vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan
vlan member remove 1 1/1-1/3

sys clipId-topology-ip 1
sys force-topology-ip-flag
  
```

Create and identify the Backbone VLANs to be used for SPBM instance 1.

Remove ISL interfaces from the default VLAN.

Sets loopback as the topology IP for XMC, and activating it via the flag setting,

4. Enable 802.1Q and IS-IS on the participating Ethernet interfaces:

```

interface GigabitEthernet 1/1
  encapsulation dot1q
  isis
  isis spbm 1
  isis enable
  no shutdown
  exit
interface GigabitEthernet 1/3
  encapsulation dot1q
  isis
  isis spbm 1
  isis enable
  no shutdown
  exit
router isis enable
  
```

Assign 802.1q and the SPBM instance and enable IS-IS on all ISL interfaces.

Globally enable IS-IS.

BEB-910 Configuration

As noted in the overview, BEB-910 and BEB-920 will be configured identically, with the exception of switch “identifiers” (sys-name, nick-name, IP addresses, etc.).

```
config terminal
prompt "CORE-8404-910"
spbm

interface loopback 1
ip address 1 10.0.0.10/255.255.255.255
exit

router isis
spbm 1
spbm 1 nick-name 0.09.10
spbm 1 b-vid 4051-4052 primary 4051
sys-name "CORE-8404-910"
system-id 00bb.0000.0910
manual-area 49.0000
ip-source-address 10.0.0.10
spbm 1 ip enable
exit

vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan
vlan member remove 1 2/18,3/18

sys clipId-topology-ip 1
sys force-topology-ip-flag

interface GigabitEthernet 2/18
encapsulation dot1q
isis
isis spbm 1
isis enable
no shutdown
exit
interface GigabitEthernet 3/18
encapsulation dot1q
isis
isis spbm 1
isis enable
no shutdown
exit
router isis enable
```

BEB-920 Configuration

As noted in the overview, BEB-910 and BEB-920 will be configured identically, with the exception of switch “identifiers” (sys-name, nick-name, IP addresses, etc.).

```

config terminal
prompt "BEB-8404-920"
spbm

interface loopback 1
ip address 1 10.0.0.20/255.255.255.255
exit

router isis
spbm 1
spbm 1 nick-name 0.09.20
sys-name "BEB-8404-920"
system-id 00bb.0000.0920
spbm 1 b-vid 4051-4052 primary 4051
manual-area 49.0000
ip-source-address 10.0.0.20
spbm 1 ip enable
exit

vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan
vlan member remove 1 1/2,1/3
sys clipId-topology-ip 1
sys force-topology-ip-flag

interface GigabitEthernet 1/2
encapsulation dot1q
isis
isis spbm 1
isis enable
no shutdown
exit
interface GigabitEthernet 1/3
encapsulation dot1q
isis
isis spbm 1
isis enable
no shutdown
exit

router isis enable

```

- Verification

When complete, the IS-IS adjacencies between the core devices should be up:

```

CORE-8404-930:1(config)#show isis adjacencies
=====
ISIS Adjacencies
=====
INTERFACE          L STATE      UPTIME PRI  HOLDTIME  SYSID          HOST-NAME      STATUS
-----
Port1/1            1 UP         04:40:30 127      23 00bb.0000.0920  BEB-8404-920  ACTIVE
Port1/3            1 UP         04:37:51 127      26 00bb.0000.0910  BEB-8404-910  ACTIVE

```

Fabric Connect – Campus 2 Configuration

Overview

This section will illustrate configuring the Campus 2 BEB switches (-210 and -211), and the interconnection to the Fabric Connect core.

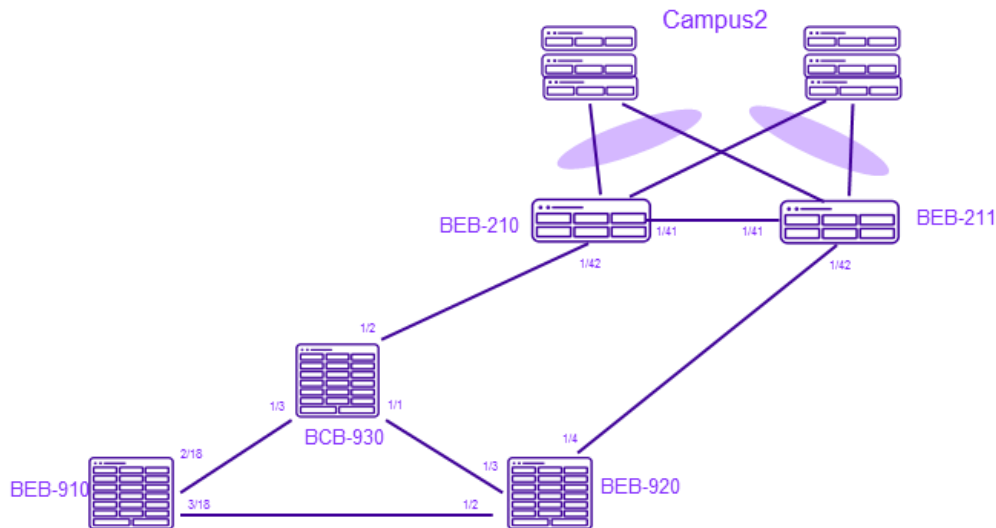
The BEB Fabric nodes are where the access data VLANs are created and assigned to a service. There are no L2/L3 configurations on the BCB switch, which allows for the core to be totally independent of any changes or modifications on the edge of the network.

After the initial SPB configuration, the process consists of the following steps:

- VRF creation for L3VSN services.
- VLAN creation, I-SID mapping, and VRF assignment.
- Enabling global VRF I-SID and VSN.
- Default Gateway protocol configuration (RSMLT and DVR).
- Redistribution/routing policies.

Note

- An L2VSN will be used for the Wired IOT Bridged VLAN (907).
- L3VSNs will be used for the IoT and Surveillance VLANs.
- The remaining VLANs will be routed on the Global Routing Table via IP Shortcuts.



Campus 2 (VLAN 2xx):

Role/Segment	VLAN	ISID	Subnet	Def Gateway	VRF	VRF ISID
FA Mgmt. VLAN	200	1020200	172.20.10.0/24	RSMLT	GRT	N/A
Wired IoT (routed)	201	1020201	172.20.20.0/22	RSMLT	VRF 1	1800911
Administrator (wired)	202	1020202	172.20.24.0/22	RSMLT	GRT	N/A
Campus User(wired)	203	1020203	172.20.28.0/22	RSMLT	GRT	N/A
Surveillance	204	1020204	172.20.32.0/22	RSMLT	VRF 2	1800904

Common Services:

Role/Segment	VLAN	ISID	Subnet	Def Gateway	VRF	VRF ISID
Administrator(wireless)	1050	1501050	172.105.0.0/24	DVR	GRT	N/A
Campus Users (wireless)	1051	1501051	172.105.1.0/24	DVR	GRT	N/A
IoT Devices (wireless)	1052	1501052	172.105.2.0/24	DVR	VRF 1	1800911
Guest (wireless)	906	1090906	172.90.40.0/24	EWC	Tunnel	N/A
Wired IoT(bridged)	907	1090907	N/A	N/A	L2VSN	N/A

Core Interface Configuration

As the base IS-IS configuration is already complete on the core Fabric Connect switches, all that's required on the core switches to connect the campus is to enable IS-IS on the connecting interfaces.

- To connect Campus 2 to the core Fabric Connect nodes:

BCB-930 Configuration:

```
Vlan member remove 1 1/2
interface GigabitEthernet 1/2
encapsulation dot1q
isis
isis spbm 1
isis enable
no shutdown
exit
```

BEB-920 Configuration:

```
Vlan member remove 1 1/4
interface GigabitEthernet 1/4
encapsulation dot1q
isis
isis spbm 1
isis enable
no shutdown
exit
```

BEB-210 Configuration

Note

An L2 VSN will be used for VLAN 907. The L2 VSN in the Automated Campus is created dynamically based on Fabric Attach requests from the FA client, therefore no manual configuration is necessary on the BEBs. When an end-user authenticates and is assigned to this VLAN/ISID, VLAN 907 will dynamically be added to the access and uplink ports.

As FA is not used in the server room, L2VSN configuration is required on those switches.

IS-IS and VLAN Configuration

1. Enter the base IS-IS configuration (from previous section) and loopback interfaces:

```
config terminal
prompt "BEB-8284-210"
spbm
interface loopback 1
ip address 1 10.0.0.210/255.255.255.255
ipv6 interface address 8200:0:0:0:0:0:210/128
exit

router isis
spbm 1
spbm 1 nick-name 0.02.10
spbm 1 b-vid 4051-4052 primary 4051
sys-name "BEB-8284-210"
system-id 00bb.0000.0210
manual-area 49.0000
ip-source-address 10.0.0.210
ipv6-source-address 8200:0:0:0:0:0:210
spbm 1 ip enable
spbm 1 ipv6 enable
exit
vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan
vlan member remove 1 1/1-1/2,1/41-1/42
sys clipId-topology-ip 1
sys force-topology-ip-flag

interface GigabitEthernet 1/41
isis
isis spbm 1
isis enable
no shutdown
exit
interface GigabitEthernet 1/42
isis
isis spbm 1
isis enable
no shutdown
exit
```

As both IPv4/v6 are requirements for the Campus User VLAN, enable IPv6 and set an IPv6 loopback on fabric nodes routing IPv6 subnets.

Set advertised IP addresses and globally enable IP Shortcut functionality.

2. Create the VRFs and enable the L3VSN services:

```
ip vrf iot vrfid 1
ip vrf surveillance vrfid 2

router vrf iot
  ipvpn
  i-sid 1800911
  ipvpn enable
exit

router vrf surveillance
  ipvpn
  i-sid 1800904
  ipvpn enable
exit
```

Provide a name and VRF id.

Assign the VRF I-SID to the L3VSN, and enable the service.

3. Create VLANs, I-SIDs and IP interfaces for the L3VSNs:

- The IoT Campus wired (201) and wireless (1052) VLANs are created and added to the IoT VRF.
- The Surveillance (204) VLAN is created and added to the Surveillance VRF.

```
vlan create 201 type port-mstprstp 0
vlan i-sid 201 1020201
interface Vlan 201
  vrf iot
  ip address 172.20.20.1 255.255.252.0
exit

vlan create 1052 type port-mstprstp 0
vlan i-sid 1052 1501052
interface Vlan 1052
  vrf iot
  ip address 172.105.2.4 255.255.255.0
exit

vlan create 204 type port-mstprstp 0
vlan i-sid 204 1020204
interface Vlan 204
  vrf surveillance
  ip address 172.20.32.1 255.255.252.0
exit
```

Create VLAN, map VLAN to associated I-SID

Assign VLAN to VRF for L3VSN service

Configure IP interface.

4. Create the VLANs and interfaces for networks that will use the Global Routing Table:

- The Device Mgmt (200), Administrator (202,1050) and Campus User (203,1051) VLANs are created and I-SIDs assigned.

```

vlan create 200 type port-mstprstp 0
vlan i-sid 200 1020200
interface Vlan 200
ip address 172.20.10.1 255.255.255.0
exit

vlan create 202 type port-mstprstp 0
vlan i-sid 202 1020202
interface Vlan 202
ip address 172.20.24.1 255.255.252.0
exit

vlan create 203 type port-mstprstp 0
vlan i-sid 203 1020203
interface Vlan 203
ip address 172.20.28.1 255.255.252.0
ipv6 interface enable
ipv6 interface address 8200:203:0:0:0:0:1/64
exit

vlan create 1050 type port-mstprstp 0
vlan i-sid 1050 1501050
interface Vlan 1050
ip address 172.105.0.4 255.255.255.0
exit

vlan create 1051 type port-mstprstp 0
vlan i-sid 1051 1501051
interface Vlan 1051
ip address 172.105.1.4 255.255.255.0
exit

```

Callout boxes:

- Create VLAN, map VLAN to associated I-SID
- Configure IPv6 interfaces on VLAN 203, as this VLAN requires dual-stack support.
- Configure IP interfaces on the VLANs.

- Verification of VLAN I-SIDs:

```

BEB-8284-210:1#show vlan i-sid
=====
Vlan I-SID
=====
VLAN_ID    I-SID
-----
1
200        1020200
201        1020201
202        1020202
203        1020203
204        1020204
1050       1501050
1051       1501051
1052       1501052
4051
4052

```

RSMLT Configuration

- Configure RSMLT on BEB-210 to peer to BEB-211 in Campus2, forming a redundant router gateway for the specified VLANs from the access switches.

```
vlan create 2 type port-mstprstp 0
vlan i-sid 2 2000
interface Vlan 2
ip address 2.1.1.1 255.255.255.0
exit

virtual-ist peer-ip 2.1.1.2 vlan 2
```

Configure VLAN/IP/I-SID used for vIST control communication between the MLT peers. This is locally significant for the MLT only.

Configure BEB-211's IP, designated as the vIST IP address.

```
router isis
spbm 1 smlt-virtual-bmac 00:00:82:00:21:10
spbm 1 smlt-peer-system-id 00bb.0000.0211
exit
```

Configure shared MLT virtual MAC (same on both peers) and the MLT peer system id address of BEB-211.

```
router isis enable
```

Once smlt parameters are configured, globally enable ISIS.

```
interface GigabitEthernet 1/1
no spanning-tree mstp
no shutdown
exit
```

```
interface GigabitEthernet 1/2
no spanning-tree mstp
no shutdown
exit
```

Disable spanning tree on the gig interfaces to be used for the MLT.

```
mlt 1 enable
mlt 1 member 1/1
mlt 1 encapsulation dot1q
```

Configure the MLT instances, and assign the corresponding ports to each.

```
mlt 2 enable
mlt 2 member 1/2
mlt 2 encapsulation dot1q
```

```
interface mlt 1
smlt
exit
```

Under each MLT interface, configure Split multi-link trunking (smlt) to allow the LAG to be distributed across both BEBs to the access switch.

```
interface mlt 2
smlt
exit
```

- Enable RSMLT on the desired VLANs:

```
interface vlan 200
ip rsmlt
ip rsmlt holdup-timer 9999
exit
```

Enable RSMLT on associated VLANs, indicating these VLANs will function as an RSMLT gateway.

```
interface Vlan 201
ip rsmlt
ip rsmlt holdup-timer 9999
exit
```

Configure RSMLT holdup-timer to "9999" (infinity). This allows the redundant switch to forward the other switch's traffic indefinitely if its unreachable.

```
interface Vlan 202
ip rsmlt
ip rsmlt holdup-timer 9999
exit
```

```
interface Vlan 203
ip rsmlt
ip rsmlt holdup-timer 9999
exit

interface Vlan 204
ip rsmlt
ip rsmlt holdup-timer 9999
exit

ip rsmlt edge-support
```

When enabling Edge-Support, each RSMLT peer will learn the other's IP and MAC address information, allowing one to resume the routing duties for the other in case of an outage.

- Once the peer switch is also configured on the corresponding VLANs, they will communicate over the vIST to discover the peer's information:

```
BEB-8284-210:1(config)#show ip rsmlt local

=====
Ip Rsmlt Local Info - GlobalRouter
=====

VID      IP              MAC              ADMIN  OPER  HDTMR  HUTMR
-----
200      172.20.10.1    b0:ad:aa:47:bd:01  Enable Up    60     infinity
202      172.20.24.1    b0:ad:aa:47:bd:03  Enable Up    60     infinity
203      172.20.28.1    b0:ad:aa:47:bd:04  Enable Up    60     infinity

VID      SMLT ID
-----
200      1, 2
202      1, 2
203      1, 2

VID      IPv6              MAC              ADMIN  OPER  HDTMR  HUTMR
-----
203      8200:203:0:0:0:0:0:0/64
          8200:203:0:0:0:0:0:1/64
          fe80:0:0:0:b2ad:aaff:fe47:bd04/128

VID      SMLT ID
-----
203      1, 2
```

```
BEB-8284-210:1(config)#show ip rsmlt peer

=====
Ip Rsmlt Peer Info - GlobalRouter
=====

VID      IP              MAC              ADMIN  OPER  HDTMR  HUTMR
-----
200      172.20.10.2    e4:5d:52:42:0d:01  Enable Up    60     infinity
202      172.20.24.2    e4:5d:52:42:0d:03  Enable Up    60     infinity
203      172.20.28.2    e4:5d:52:42:0d:04  Enable Up    60     infinity

VID      HDT REMAIN  HUT REMAIN  SMLT ID
-----
```

```

200 60 infinity 1, 2
202 60 infinity 1, 2
203 60 infinity 1, 2

VID IPv6 MAC ADMIN OPER HDTMR HUTMR
-----
203 e4:5d:52:42:0d:04 Enable Up 60 infinity
8200:203:0:0:0:0:0/64
8200:203:0:0:0:0:0:2/64
fe80:0:0:0:e65d:52ff:fe42:d04/128

VID HDT REMAIN HUT REMAIN SMLT ID

```

DVR Configuration (Controllers only)

DVR is configured in both campuses for the wireless networks (IoT, Administrator and Campus User), specifying the BEBs as Controllers. Although the Server Rooms will have a full Controller-Leaf configuration, no Leaf configuration is required for the Campus DVR deployment.

Configuring DVR in the campuses for wireless networks extends those VLANs and subnets across the campuses, allowing for seamless roaming.

- Configure the DVR instance and enable DVR on the desired IP interfaces.

```

dvr controller 20

interface Vlan 1050
dvr gw-ipv4 172.105.0.1
dvr enable
exit

interface Vlan 1051
dvr gw-ipv4 172.105.1.1
dvr enable
exit

interface vlan 1052
dvr gw-ipv4 172.105.2.1
dvr enable
exit

```

From Global mode, configure the DVR domain id. BEB-210 and -211 will share this id. The BEBs in Campus1 will have a different domain id.

Enable DVR for each Access VLAN, specifying the shared Default GW IP to be used,

- Verification:

```
BEB-8284-210:1#show dvr interfaces
```

```

=====
DVR Interfaces
=====
Admin SPBMC
IGMP
Interface Mask L3ISID VRFID L2ISID VLAN GW IPv4 State
State Version
-----
172.105.0.4 255.255.255.0 0 0 1501050 1050 172.105.0.1 enable
disable 2
172.105.1.4 255.255.255.0 0 0 1501051 1051 172.105.1.1 enable
disable 2
172.105.2.4 255.255.255.0 1800911 1 1501052 1052 172.105.2.1 enable
disable 2

3 out of 3 Total Num of DVR Interfaces displayed
=====

```

Routing Policies - Overview

One of the benefits of Virtual Service Networks is the security and traffic isolation that occurs between them. However, network environments still require some controlled access between subnets, VRFs and DVR domains. Route Maps and IS-IS accept policies allow routes to be advertised across these boundaries.

The following are the current route policies applied on BEBs in the Automated Campus EVD.

Note

Given the security and traffic isolation inherent in Fabric Connect, routing policy and redistribution are vital concepts in allowing inter-domain communication and may require further research and assistance than the overview in this document.

The GRT and VRF instances that are created become separate routing domains and therefore have separate, isolated routing tables. DVR domains (which are created within one or both) also act as a separate routing domain (i.e. a domain within a domain).

Routing Policies - Redistribution

Fabric Connect uses one global IS-IS instance for reachability information. When vln interfaces are created on fabric nodes within the same domain (GRT or VRF) in different parts of the network, those directly connected routes need to be redistributed into IS-IS for reachability WITHIN that routing domain.

```

router isis
redistribute direct
redistribute direct enable
ipv6 redistribute direct enable
exit

router vrf iot
isis redistribute direct
isis redistribute direct enable
exit

router vrf surveillance
isis redistribute direct
isis redistribute direct enable
exit

isis apply redistribute direct
isis apply redistribute direct vrf iot
isis apply redistribute direct vrf surveillance

```

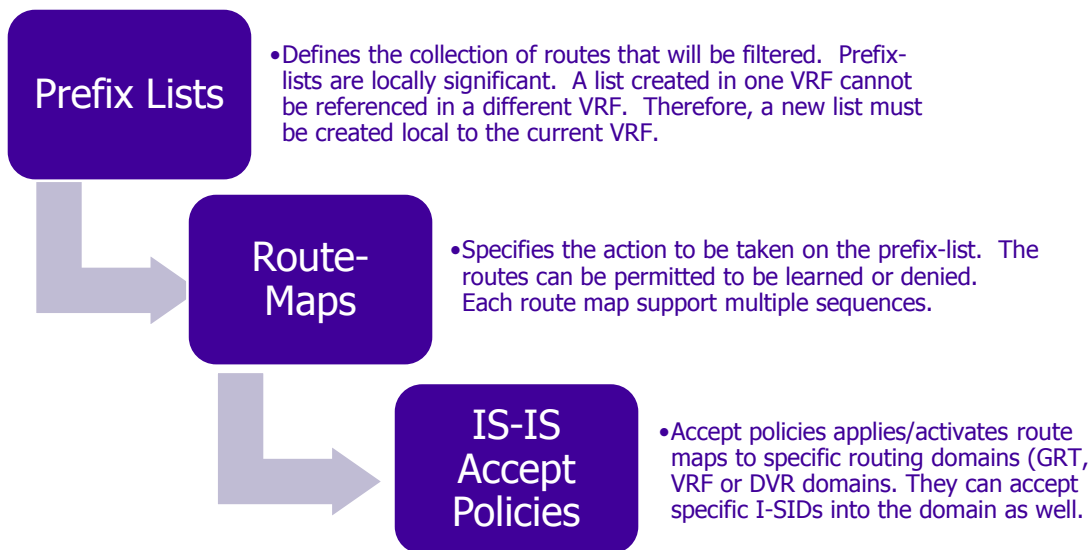
Redistribute directly connected routes into the GRT's IS-IS instance.

Within each VRF instance, redistribute directly connected routes into its IS-IS instance.

Apply redistribution to GRT and each VRF.

Route-Maps and IS-IS Accept Policies

For routes to be advertised or "leaked" between the GRT, VRFs, or DVR domains, prefix-lists, route-maps and IS-IS accept policies are configured.



For example, the DVR domains created in the campuses and server rooms are separate domains, and by default, do not share routing information. For the domains to exchange routing information, route-policies must be configured to share them across the DVR backbone.

GRT Routing Policy:

- The Global Routing Table on BEB-210 has the following requirements:
 - Reachability to networks in VRFs requiring centralized services located in the GRT (DHCP, production servers, etc.).
 - The Wireless Administrator (1050) and Campus User (1051) VLANS, which have DVR enabled, needs to be advertised to the DVR backbone, allowing route information to be shared with other corresponding networks in the DVR backbone (in Campus 1, for example).
- Configure IS-IS Accept policies, to import routes from the specified VRFs:

```
router isis
accept i-sid 1800904 enable
accept i-sid 1800911 enable
exit
```

Imports global I-SIDs for Surveillance and IoT VRF. No route-map needed, as all routes in these VRFs are being accepted.

VRF “IoT” Routing Policy:

- The VRF IoT has the following requirements:
 - Reachability between all IoT VLANs in the campuses and server rooms. This is accomplished when the IoT VLANs in these locations are added to the IoT VRF (L3VSN).
 - Access to the Production Server network and the Network Management subnet (both in the Server Room on the GRT).
 - The Wireless IoT VLAN (1052) which has DVR enabled, needs to be advertised to VRF IoT’s DVR backbone, allowing route information to be shared with other IoT networks in the DVR backbone (in Campus 1, for example).
- Within VRF iot, create prefix-lists identifying the routes above:

```
router vrf iot
ip prefix-list "GRT_mgmt" 172.9.99.0/24 id 1 ge 24 le 24
ip prefix-list "GRT_910" 172.90.1.0/24 id 2 ge 24 le 24
```

- Create route-maps matching/permitting the corresponding prefix-lists:

```
route-map "accept_GRT_mgmt" 1
permit
enable
match network "GRT_mgmt,GRT_910"

route-map "accept_GRT_mgmt" 2
no permit
enable
exit
```

Permit routes matching both the GRT_mgmt and GRT_910 prefix-lists.
Deny all other routes being learned.

- Configure IS-IS Accept policies, importing specific GRT routes matching the route-map:

```
router vrf iot
isis accept i-sid 0 enable
isis accept i-sid 0 route-map "accept_GRT_mgmt"
exit
```

Imports the GRT_mgmt prefix-list from GRT (I-SID 0).

VRF “Surveillance” Routing Policy:

- The VRF Surveillance has the following requirements:
 - Reachability from the Surveillance VLANs in the campuses to the server rooms. This is accomplished when the Surveillance VLANs in these locations are added to the Surveillance VRF (L3VSN).
 - Access to the Network Mgmt subnet (for DHCP) and the Storage subnet (for video recordings).

- Configure prefix-lists, route-maps and accept policies for the “surveillance” VRF:

```

router vrf surveillance
ip prefix-list "GRT_mgmt" 172.9.99.0/24 id 1 ge 24 le 24
ip prefix-list "GRT_stor" 172.90.3.0/24 id 2 ge 24 le 24

route-map "accept_GRT_mgmt" 1
permit
enable
match network "GRT_mgmt,GRT_stor"
route-map "accept_GRT_mgmt" 2
no permit
enable
exit

isis accept i-sid 0 enable
isis accept i-sid 0 route-map "accept_GRT_mgmt"
exit

isis apply accept
isis apply accept vrf iot
isis apply accept vrf surveillance

```

Define the routes to import from the GRT.

Permit routes matching those prefix-lists.

Accept the routes from the GRT defined in the route-map.

Apply the accept policies to the GRT and both VRFs.

Fabric Attach

Fabric Attach uses the IEEE802.1ab *LLDP (Link Layer Discovery Protocol)* extensions to automatically attach network devices to individual services in a Fabric Connect network. These network devices typically do not support SPB, MAC-in-MAC (802.1ah) or Network Services Identifier (NSI)/Individual Service Identifier (I-SID) usage, and therefore cannot easily take advantage of the Fabric infrastructure without manual configuration of VLAN attachments to NSIs or ISIDs in multiple locations. Fabric Attach deals with this issue by facilitating automated network device discovery and the automatic configuration and teardown of NSI/ISID to VLAN associations at the edge of the network.

Upon connection and detection of an FA Client, the FA Server (BEB) will advertise (via LLDP) the management I-SID/VLAN to the FA-Proxy switch.

The FA Proxy on the access switch communicates directly with the FA server on the BEB to request VLAN to I-SID mappings for user traffic.

Enter the following on BEB-210:

```

interface mlt 1
fa
fa enable
no fa message-authentication
fa management i-sid 1020200 c-vid 200
exit

interface mlt 2
fa
fa enable
no fa message-authentication
fa management i-sid 1020200 c-vid 200
exit

```

Under each MLT interface (connecting to the access switches), enable Fabric Attach.

Set the Management I-SID and VLAN that will be advertised to the FA client.

Feature disabled until released on EXOS.

BEB-211 Configuration (Peer)

BEB-211, acting as the RSMLT peer to BEB-210 will follow the same steps for configuration as BEB-210. Once both BEBs are configured, they can be connected to each other and to the core fabric nodes.

IS-IS and VLAN Configuration

- Enter the base IS-IS configuration and loopback interfaces:

```

config terminal
  prompt "BEB-8284-211"
  spbm

interface loopback 1
ip address 1 10.0.0.211/255.255.255.255
ipv6 interface address 8200:0:0:0:0:0:211/128
exit

router isis
  spbm 1
  spbm 1 nick-name 0.02.11
  spbm 1 b-vid 4051-4052 primary 4051
  sys-name "BEB-8284-211"
  system-id 00bb.0000.0211
  ip-source-address 10.0.0.211
  ipv6-source-address 8200:0:0:0:0:0:211
  spbm 1 ip enable
  spbm 1 ipv6 enable
  manual-area 49.0000
  exit

vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan
sys clipId-topology-ip 1
sys force-topology-ip-flag
vlan member remove 1 1/1-1/2,1/41-1/42
interface GigabitEthernet 1/41
  isis
  isis spbm 1
  isis enable
  no shutdown
  exit
interface GigabitEthernet 1/42
  isis
  isis spbm 1
  isis enable
  no shutdown
  exit

```

- Create the VRFs and enable the L3VSN services:

```

ip vrf iot vrfid 1
ip vrf surveillance vrfid 2

router vrf iot
  ipvpn
  i-sid 1800911
  ipvpn enable
  exit
router vrf surveillance
  ipvpn
  i-sid 1800904
  ipvpn enable
  exit

```

- Create VLANs, I-SIDs and IP interfaces for the L3VSNs:
 - The IoT Campus wired (201) and wireless (1052) VLANs are created and added to the IoT VRF.
 - The Surveillance (204) VLAN is created and added to the Surveillance VRF.

```
vlan create 201 type port-mstprstp 0
vlan i-sid 201 1020201
interface Vlan 201
vrf iot
ip address 172.20.20.2 255.255.252.0
exit

vlan create 1052 type port-mstprstp 0
vlan i-sid 1052 1501052
interface Vlan 1052
vrf iot
ip address 172.105.2.5 255.255.255.0
exit

vlan create 204 type port-mstprstp 0
vlan i-sid 204 1020204
interface Vlan 204
vrf surveillance
ip address 172.20.32.2 255.255.252.0
exit
```

- Create the VLANs and interfaces for networks that will use the Global Routing Table:
 - The Device Mgmt (200), Administrator (202,1050) and Campus User (203,1051) VLANs are created and I-SIDs assigned.

```
vlan create 200 type port-mstprstp 0
vlan i-sid 200 1020200
interface Vlan 200
ip address 172.20.10.2 255.255.255.0
exit

vlan create 202 type port-mstprstp 0
vlan i-sid 202 1020202
interface Vlan 202
ip address 172.20.24.2 255.255.252.0
exit

vlan create 203 type port-mstprstp 0
vlan i-sid 203 1020203
interface Vlan 203
ip address 172.20.28.2 255.255.252.0
ipv6 interface enable
ipv6 interface address 8200:203:0:0:0:0:0:0/64
exit

vlan create 1050 type port-mstprstp 0
vlan i-sid 1050 1501050
interface Vlan 1050
ip address 172.105.0.5 255.255.255.0
exit

vlan create 1051 type port-mstprstp 0
vlan i-sid 1051 1501051
interface Vlan 1051
ip address 172.105.1.5 255.255.255.0
exit
```

RSMLT Configuration

- Configure RSMLT to peer the BEB-211 and -210 BEBs. Be sure to specify the -210 values where called for.

```

vlan create 2 type port-mstprstp 0
vlan i-sid 2 2000
interface Vlan 2
ip address 2.1.1.2 255.255.255.0
exit

virtual-ist peer-ip 2.1.1.1 vlan 2

router isis
spbm 1 smlt-virtual-bmac 00:00:82:00:21:10
spbm 1 smlt-peer-system-id 00bb.0000.0210
exit

router isis enable

interface GigabitEthernet 1/1
no spanning-tree mstp
yes
no shutdown
exit

interface GigabitEthernet 1/2
no spanning-tree mstp
yes
no shutdown
exit

mst 1 enable
mst 1 member 1/1
mst 1 encapsulation dot1q

mst 2 enable
mst 2 member 1/2
mst 2 encapsulation dot1q

interface mlt 1
smst
exit

interface mlt 2
smst
exit

```

Once smst parameters are configured, globally enable ISIS.

- Enable RSMLT on the desired VLANs:

```

interface vlan 200
ip smst
ip smst holdup-timer 9999
exit

interface Vlan 201
ip smst
ip smst holdup-timer 9999
exit

interface Vlan 202
ip smst
ip smst holdup-timer 9999
exit

```

```

interface Vlan 203
ip rsm1t
ip rsm1t holdup-timer 9999
exit

interface Vlan 204
ip rsm1t
ip rsm1t holdup-timer 9999
exit

ip rsm1t edge-support

```

DVR Configuration (Controllers only)

Configure the DVR instance and enable DVR on the desired IP interfaces.

```

dvr controller 20

interface Vlan 1050
dvr gw-ipv4 172.105.0.1
dvr enable
exit

interface Vlan 1051
dvr gw-ipv4 172.105.1.1
dvr enable
exit

interface vlan 1052
dvr gw-ipv4 172.105.2.1
dvr enable
exit

```

The DVR gateway IP will be the same address as configured in BEB-210 to allow for inter-campus roaming

Routing Policies - Redistribution

```

router isis
redistribute direct
redistribute direct enable
ipv6 redistribute direct enable
exit

router vrf iot
isis redistribute direct
isis redistribute direct enable
exit

router vrf surveillance
isis redistribute direct
isis redistribute direct enable
exit

isis apply redistribute direct
isis apply redistribute direct vrf iot
isis apply redistribute direct vrf surveillance

```

Route-Maps and IS-IS Accept Policies

GRT Policy:

```

router isis
accept i-sid 1800904 enable
accept i-sid 1800911 enable
exit

```

VRF “IoT” Routing Policy:

```

router vrf iot
ip prefix-list "GRT_mgmt" 172.9.99.0/24 id 1 ge 24 le 24
ip prefix-list "GRT_910" 172.90.1.0/24 id 2 ge 24 le 24

route-map "accept_GRT_mgmt" 1
permit
enable
match network "GRT_mgmt,GRT_910"

route-map "accept_GRT_mgmt" 2
no permit
enable
exit

isis accept i-sid 0 enable
isis accept i-sid 0 route-map "accept_GRT_mgmt"
exit

```

VRF “Surveillance” Routing Policy:

```

router vrf surveillance
ip prefix-list "GRT_mgmt" 172.9.99.0/24 id 1 ge 24 le 24
ip prefix-list "GRT_stor" 172.90.3.0/24 id 2 ge 24 le 24

route-map "accept_GRT_routes" 1
permit
enable

match network "GRT_mgmt,GRT_stor"
route-map "accept_GRT_routes" 2
no permit
enable
exit
exit

router vrf surveillance
isis accept i-sid 0 enable
isis accept i-sid 0 route-map "accept_GRT_routes"
exit

isis apply accept
isis apply accept vrf iot
isis apply accept vrf surveillance

```

Fabric Attach

- The FA management VLAN in Campus 2 is VLAN id 200

```

interface mlt 1
fa
fa enable
no fa message-authentication
fa management i-sid 1020200 c-vid 200
exit

interface mlt 2
fa
fa enable
no fa message-authentication
fa management i-sid 1020200 c-vid 200
exit

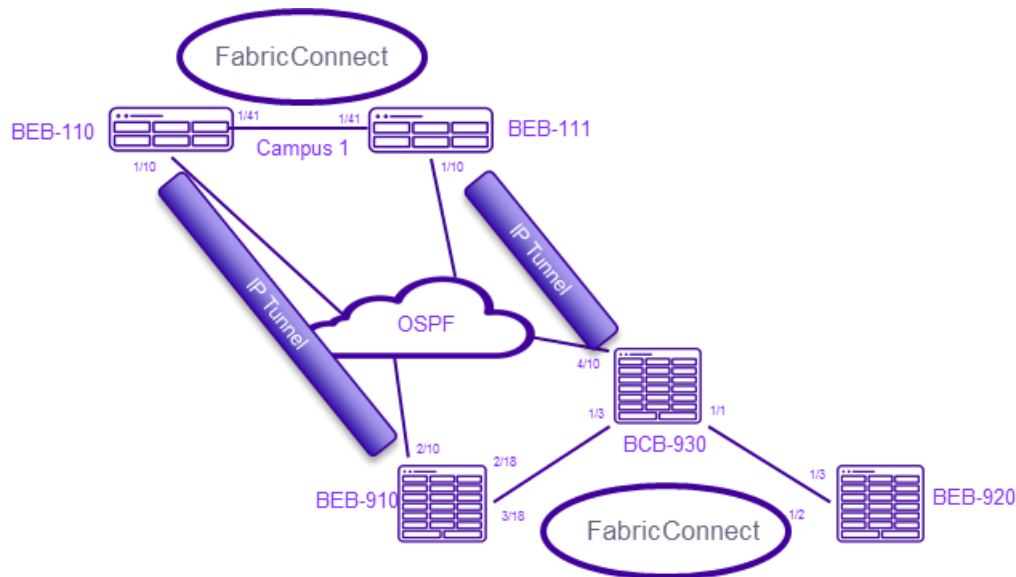
```


Fabric Extend (Fabric Connect over IP) – Campus 1 Configuration

Overview

Fabric Extend allows us to extend the Fabric Connect technology over Layer 2 or Layer 3 core networks. The logical IS-IS interface is the mechanism that enables Fabric Extend to connect SPB fabric nodes. Logical IS-IS interfaces create virtual tunnels and encapsulate SPB traffic by adding a Virtual Extensible LAN (VXLAN) header to SPB packets.

To illustrate this, the Automated Campus utilizes Fabric Extend, using two L3 tunnels, connecting the core fabric nodes (BCB-930 and BEB-910) to the Campus-1 BEBs (-110 and -111) over an intermediate IP network. The intermediate network can consist of any configuration if there is connectivity between the sites. This EVD uses OSPF.



This deployment uses a separate VRF strictly for the tunneling, so the tunnel source IP address must be present on the VRF.

Core Interface (Tunnel) Configuration

BCB-930 Configuration:

- Configure IP interface and OSPF to peer with non-Fabric network:

```
router ospf enable
router ospf
router-id 10.0.0.30
exit
```

Globally enable OSPF, set the loopback as the router id.

```
ip vrf tunnel vrfid 3
router vrf tunnel
ip ospf
ip ospf admin-state
exit
```

Create VRF to configure tunnel in.

```
interface GigabitEthernet 4/10
encapsulation dot1q
```

```

name "OSPF_link_to_Cloud"
no shutdown
vrf tunnel
brouter port 4/10 vlan 2501 subnet 197.1.2.4/255.255.255.0
no spanning-tree mstp
yes
ip ospf enable
yes
exit

```

Within vrf Tunnel, configure IP interface connecting to OSPF network, and enable OSPF.

- Configure the L3 Tunnel to connect to Campus 1, BEB-111:

```

router isis
ip-tunnel-source-address 197.1.2.4 vrf tunnel
exit

logical-intf isis 255 dest-ip 197.1.12.2 name "Tunnel_to_8284-111"
isis
isis spbm 1
isis enable
exit

```

Configure tunnel source IP (same as IP interface in previous step).

Configure tunnel destination IP (IP of BEB-111 in Campus-1), and set the IS-IS instance id to match local instance.

BCB-910 Configuration:

- Configure IP interface and OSPF to peer with non-Fabric network:

```

router ospf enable
router ospf
router-id 10.0.0.10
exit

ip vrf tunnel vrfid 3
router vrf tunnel
ip ospf
exit

interface GigabitEthernet 2/10
encapsulation dot1q
name "OSPF_link_to_Cloud2"
no shutdown
vrf tunnel
brouter port 2/10 vlan 2500 subnet 197.1.1.2/255.255.255.0
no spanning-tree mstp
yes
ip ospf enable
yes
exit

```

Globally enable OSPF, set the loopback as the router id.

Create VRF to configure tunnel in.

Within vrf Tunnel, configure IP interface connecting to OSPF network, and enable

- Configure the L3 Tunnel to connect to Campus 1, BEB-110:

```

router isis
ip-tunnel-source-address 197.1.1.2 vrf tunnel
exit

logical-intf isis 255 dest-ip 197.1.6.2 name "Tunnel_to_8284-110"
isis
isis spbm 1
isis enable
exit

```

Configure tunnel source IP (same as IP interface in previous step).

Configure tunnel destination IP (IP of BEB-110 in Campus-1), and set the IS-IS instance id to match local instance.

BEB-111 Configuration

Campus 1 (VLAN 1xx):

Role/Segment	VLAN	ISID	Subnet	Def Gateway	VRF	VRF ISID
FA Mgmt.VLAN	100	1010100	172.10.10.0/24	RSMLT	GRT	N/A
Wired IoT (routed)	101	1010101	172.10.20.0/22	RSMLT	VRF 1	1800911
Administrator (wired)	102	1010102	172.10.24.0/22	RSMLT	GRT	N/A
Campus User(wired)	103	1010103	172.10.28.0/22	RSMLT	GRT	N/A
Surveillance	104	1010104	172.10.32.0/22	RSMLT	VRF 2	1800904

Common Services:

Role/Segment	VLAN	ISID	Subnet	Def Gateway	VRF	VRF ISID
Administrator(wireless)	1050	1501050	172.105.0.0/24	DVR	GRT	N/A
Campus Users (wireless)	1051	1501051	172.105.1.0/24	DVR	GRT	N/A
IoT Devices (wireless)	1052	1501052	172.105.2.0/24	DVR	VRF 1	1800911
Guest (wireless)	906	1090906	172.90.40.0/24	EWC	Tunnel	N/A
Wired IoT(bridged)	907	1090907	N/A	N/A	L2VSN	N/A

IS-IS Configuration

BEB-111, the tunnel peer to BCB-930 will be configured similarly, except specifying the BCB-930 as its tunnel end-point:

- Configure the base ISIS configuration:

```

config terminal
prompt "BEB-8284-111"
spbm

interface loopback 1
ip address 1 10.0.0.111/255.255.255.255
ipv6 interface address 8200:0:0:0:0:0:111/128
exit

router isis
spbm 1
spbm 1 nick-name 0.01.11
spbm 1 b-vid 4051-4052 primary 4051
sys-name "BEB-8284-111"
system-id 00bb.0000.0111
ip-source-address 10.0.0.111
ipv6-source-address 8200:0:0:0:0:0:111
spbm 1 ip enable
spbm 1 ipv6 enable
manual-area 49.0000
exit

vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan
vlan member remove 1 1/1-1/2,1/10,1/41
sys clipId-topology-ip 1
sys force-topology-ip-flag

interface GigabitEthernet 1/41
encapsulation dot1q
isis
isis spbm 1
isis enable
no spanning-tree mstp
yes
no shutdown
exit

```

Fabric Extend (tunnel) Configuration

- Configure the IP Tunnel to BCB-930:

```

router ospf enable
router ospf
router-id 10.0.0.111
exit

ip vrf tunnel vrfid 3
router vrf tunnel
ip ospf
ip ospf admin-state
exit

interface GigabitEthernet 1/10
name "ospf_vlan_to_cloud"
no shutdown
vrf tunnel
brouter port 1/10 vlan 3501 subnet 197.1.12.2/255.255.255.0

```

```

no spanning-tree mstp
yes
ip ospf enable
yes
exit

router isis
ip-tunnel-source-address 197.1.12.2 vrf tunnel
exit

logical-intf isis 255 dest-ip 197.1.2.4 name "Tunnel_to_Core"
isis
isis spbm 1
isis enable
exit

```

- Once connected, ensure the OSPF neighbor state between the Campus BEBs and Core Fabric nodes to their respective OSPF neighbors is established.

```
CORE-BEB-8284-111:1(config)#show ip ospf neighbor vrf tunnel
```

```

=====
                        OSPF Neighbors - VRF tunnel
=====
INTERFACE          NBRROUTERID    NBRIPADDR      PRIO    STATE    RTXQLEN  PERM  TTL
-----
197.1.12.2         82.60.189.0    197.1.12.3     1       Full     0        Dyn   32
=====
Total ospf neighbors: 1
H = Helping a Restarting neighbor

```

The OSPF state to the intermediate OSPF network router should be "FULL".

- Verify that the tunnel to Campus1 is operational and Fabric Extend is working.

```
BEB-8284-111:1(config)#show isis logical-interface
```

```

=====
                        ISIS Logical Interfaces
=====
IFIDX  NAME          ENCAP  L2_INFO  VIDS (PRIMARY)  TUNNEL  L3_TUNNEL_NEXT_HOP_INFO
TYPE   PORT/MLT      DEST-IP  PORT/MLT  VLAN           VRF
-----
255    Tunnel_to_Core  IP      --        --              197.1.2.4  Port1/10  3501  tunnel
=====
1 out of 1 Total Num of Logical ISIS interfaces

```

If the tunnel is operational, the interface will be listed. Otherwise, it will state "NULL".

VLAN and I-SID Configuration

VLANs and services for Campus 1 are configured in this section based on the VLAN/I-SID scheme illustrated at the beginning of this section.

- Create the VRFs and enable the L3VSN services:

```

ip vrf iot vrfid 1
ip vrf surveillance vrfid 2
router vrf iot
ipvpn
i-sid 1800911
ipvpn enable
exit
router vrf surveillance
ipvpn
i-sid 1800904
ipvpn enable
exit

```

2. Create VLANs, I-SIDs and IP interfaces for the L3VSNs:

- The IoT Campus wired (101) and wireless (1052) VLANs are created and added to the IoT VRF.
- The Surveillance (104) VLAN is created and added to the Surveillance VRF.

```
vlan create 101 type port-mstprstp 0
vlan i-sid 101 1010101
interface Vlan 101
vrf iot
ip address 172.10.20.2 255.255.252.0
exit

vlan create 104 type port-mstprstp 0
vlan i-sid 104 1010104
interface Vlan 104
vrf surveillance
ip address 172.10.32.2 255.255.252.0
exit

vlan create 1052 type port-mstprstp 0
vlan i-sid 1052 1501052
interface Vlan 1052
vrf iot
ip address 172.105.2.3 255.255.255.0
exit
```

3. Create the VLANs and interfaces for networks that will use the Global Routing Table:

- The Device Mgmt (100), Administrator (102,1050) and Campus User (103,1051) VLANs are created and I-SIDs assigned.

```
vlan create 100 type port-mstprstp 0
vlan i-sid 100 1010100
interface Vlan 100
ip address 172.10.10.2 255.255.255.0
exit

vlan create 102 type port-mstprstp 0
vlan i-sid 102 1010102
interface Vlan 102
ip address 172.10.24.2 255.255.252.0
exit

vlan create 103 type port-mstprstp 0
vlan i-sid 103 1010103
interface Vlan 103
ip address 172.10.28.2 255.255.252.0
ipv6 interface enable
ipv6 interface address 8200:103:0:0:0:0:0:2/64
exit

vlan create 1050 type port-mstprstp 0
vlan i-sid 1050 1501050
interface Vlan 1050
ip address 172.105.0.3 255.255.255.0
exit

vlan create 1051 type port-mstprstp 0
vlan i-sid 1051 1501051
interface Vlan 1051
ip address 172.105.1.3 255.255.255.0
exit
```

RSMLT Configuration

- Configure RSMLT to peer the BEB-110 and -111 in Campus1, forming a redundant router gateway for the specified VLANs from the access switches.

```

vlan create 2 type port-mstprstp 0
vlan i-sid 2 2200
interface Vlan 2
ip address 2.2.2.2 255.255.255.0 0
exit

virtual-ist peer-ip 2.2.2.1 vlan 2

router isis
spbm 1 smlt-virtual-bmac 00:bb:00:01:10:11
spbm 1 smlt-peer-system-id 00bb.0000.0110
exit

router isis enable

interface GigabitEthernet 1/1
no spanning-tree mstp
yes
no shutdown
exit

interface GigabitEthernet 1/2
no spanning-tree mstp
yes
no shutdown
exit

mlt 1 enable
mlt 1 member 1/1
mlt 1 encapsulation dot1q

mlt 2 enable
mlt 2 member 1/2
mlt 2 encapsulation dot1q

interface mlt 1
smlt
exit

interface mlt 2
smlt
exit

```

- Enable RSMLT on the desired VLANs:

```

interface vlan 100
ip rsmlt
ip rsmlt holdup-timer 9999
exit

interface Vlan 101
ip rsmlt
ip rsmlt holdup-timer 9999
exit

interface Vlan 102
ip rsmlt
ip rsmlt holdup-timer 9999
exit

```

```

interface Vlan 103
ip rsmult
ip rsmult holdup-timer 9999
exit

interface Vlan 104
ip rsmult
ip rsmult holdup-timer 9999
exit

ip rsmult edge-support

```

DVR Configuration

- Configure the DVR instance and enable DVR on the desired IP interfaces.

```

dvr controller 10

interface Vlan 1050
dvr gw-ipv4 172.105.0.1
dvr enable
exit

interface Vlan 1051
dvr gw-ipv4 172.105.1.1
dvr enable
exit

interface vlan 1052
dvr gw-ipv4 172.105.2.1
dvr enable
exit

```

From Global mode, configure the DVR domain id for Campus 1. BEB-110 and -111 will share this id.

Routing Policies - Redistribution

- The redistribution configuration will be the same as the Campus 2 configuration:

```

router isis
redistribute direct
redistribute direct enable
ipv6 redistribute direct enable

router vrf iot
isis redistribute direct
isis redistribute direct enable
exit

router vrf surveillance
isis redistribute direct
isis redistribute direct enable
exit

isis apply redistribute direct
isis apply redistribute direct vrf iot
isis apply redistribute direct vrf surveillance

```


Route-Maps and IS-IS Accept Policies

The route policy configuration will be the same as the Campus 2 configuration.

- GRT Policy:

```
router isis
accept i-sid 1800904 enable
accept i-sid 1800911 enable
exit
```

- VRF “IoT” Routing Policy:

```
router vrf iot
ip prefix-list "GRT_mgmt" 172.9.99.0/24 id 1 ge 24 le 24
ip prefix-list "GRT_910" 172.90.1.0/24 id 2 ge 24 le 24

route-map "accept_GRT_mgmt" 1
permit
enable
match network "GRT_mgmt,GRT_910"

route-map "accept_GRT_mgmt" 2
no permit
enable
exit

isis accept i-sid 0 enable
isis accept i-sid 0 route-map "accept_GRT_mgmt"
exit
```

- VRF “Surveillance” Routing Policy:

```
router vrf surveillance
ip prefix-list "GRT_mgmt" 172.9.99.0/24 id 1 ge 24 le 24
ip prefix-list "GRT_stor" 172.90.3.0/24 id 2 ge 24 le 24

route-map "accept_GRT_mgmt" 1
permit
enable
match network "GRT_mgmt,GRT_stor"
route-map "accept_GRT_mgmt" 2
no permit
enable
exit
exit

router vrf surveillance
isis accept i-sid 0 enable
isis accept i-sid 0 route-map "accept_GRT_mgmt"
exit

isis apply accept
isis apply accept vrf iot
isis apply accept vrf surveillance
```

Fabric Attach

- The FA management VLAN in Campus 1 is VLAN id 100

```
interface mlt 1
fa
fa enable
no fa message-authentication
fa management i-sid 1010100 c-vid 100
exit

interface mlt 2
fa
fa enable
no fa message-authentication
fa management i-sid 1010100 c-vid 100
exit
```

BEB-110 Configuration

IS-IS Configuration

BEB-110, the tunnel peer to BEB-910 will be configured similarly, except specifying the BEB-910 as its tunnel end-point:

- Configure the base ISIS configuration:

```
config terminal
prompt "BEB-8284-110"
spbm
interface loopback 1
ip address 1 10.0.0.110/255.255.255.255
ipv6 interface address 8200:0:0:0:0:0:110/128
exit

router isis
spbm 1
spbm 1 nick-name 0.01.10
spbm 1 b-vid 4051-4052 primary 4051
sys-name "BEB-8284-110"
system-id 00bb.0000.0110
ip-source-address 10.0.0.110
ipv6-source-address 8200:0:0:0:0:0:110
spbm 1 ip enable
spbm 1 ipv6 enable
manual-area 49.0000
exit

vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan
vlan member remove 1 1/1-1/2,1/10,1/41
sys clipId-topology-ip 1
sys force-topology-ip-flag

interface GigabitEthernet 1/41
encapsulation dot1q
isis
isis spbm 1
isis enable
no spanning-tree mstp
yes
no shutdown
exit
```

Fabric Extend (tunnel) Configuration

- Configure the IP Tunnel to BCB-910:

```

router ospf enable
router ospf
router-id 10.0.0.110
exit

ip vrf tunnel vrfid 3
router vrf tunnel
ip ospf
ip ospf admin-state
exit

interface GigabitEthernet 1/10
name "ospf_vlan_to_cloud"
no shutdown
vrf tunnel
brouter port 1/10 vlan 3500 subnet 197.1.11.2/255.255.255.0
no spanning-tree mstp
yes
ip ospf enable
yes
exit

router isis
ip-tunnel-source-address 197.1.11.2 vrf tunnel
exit

logical-intf isis 255 dest-ip 197.1.1.2 name "Tunnel-8404-910"
isis
isis spbm 1
isis enable
exit

```

- Once connected, ensure the OSPF neighbor state between the Campus BEBs and Core Fabric nodes to their respective OSPF neighbors is established.

```
BEB-8284-110:1(config)#show ip ospf neighbor vrf tunnel
```

```

=====
                        OSPF Neighbors - VRF tunnel
=====
INTERFACE          NBRROUTERID      NBRIPADDR        PRIO    STATE    RTXQLEN  PERM  TTL
-----
197.1.11.2         82.60.189.0     197.1.11.3       1       Full     0        Dyn   35

```

The OSPF state to the intermediate OSPF network router should be "FULL".

- Verify that the tunnel to Campus1 is operational and Fabric Extend is working.

```
BEB-8284-110:1(config)#show isis logical-interface
```

ISIS Logical Interfaces							
IFIDX	NAME	ENCAP	L2_INFO		TUNNEL		
L3_TUNNEL_NEXT_HOP_INFO		TYPE	PORT/MLT	VIDS (PRIMARY)	DEST-IP	PORT/MLT	VLAN
VRF							
255	Tunnel-8404-910	IP	--	--	197.1.1.2	Port1/10	3500

tunnel

If the tunnel is operational, the interface will be listed. Otherwise, it will state "NULL".

VLAN and I-SID Configuration

VLANs and services for Campus 1 are configured in this section based on the VLAN/I-SID scheme illustrated at the beginning of this section.

- Create the VRFs and enable the L3VSN services:

```
ip vrf iot vrfid 1
ip vrf surveillance vrfid 2

router vrf iot
  ipvpn
  i-sid 1800911
  ipvpn enable
  exit
router vrf surveillance
  ipvpn
  i-sid 1800904
  ipvpn enable
  exit
```

- Create VLANs, I-SIDs and IP interfaces for the L3VSNs:

- The IoT Campus wired (101) and wireless (1052) VLANs are created and added to the IoT VRF.
- The Surveillance (104) VLAN is created and added to the Surveillance VRF.

```
vlan create 101 type port-mstprstp 0
vlan i-sid 101 1010101
interface Vlan 101
  vrf iot
  ip address 172.10.20.1 255.255.252.0
  exit

vlan create 104 type port-mstprstp 0
vlan i-sid 104 1010104
interface Vlan 104
  vrf surveillance
  ip address 172.10.32.1 255.255.252.0
  exit

vlan create 1052 type port-mstprstp 0
vlan i-sid 1052 1501052
interface Vlan 1052
  vrf iot
  ip address 172.105.2.2 255.255.255.0
  exit
```

3. Create the VLANs and interfaces for networks that will use the Global Routing Table:

- The Device Mgmt (100), Administrator (102,1050) and Campus User (103,1051) VLANs are created and I-SIDs assigned.

```
vlan create 100 type port-mstprstp 0
vlan i-sid 100 1010100
interface Vlan 100
ip address 172.10.10.1 255.255.255.0
exit

vlan create 102 type port-mstprstp 0
vlan i-sid 102 1010102
interface Vlan 102
ip address 172.10.24.1 255.255.252.0
exit

vlan create 103 type port-mstprstp 0
vlan i-sid 103 1010103
interface Vlan 103
ip address 172.10.28.1 255.255.252.0
ipv6 interface enable
ipv6 interface address 8200:103:0:0:0:0:0:1/64
exit

vlan create 1050 type port-mstprstp 0
vlan i-sid 1050 1501050
interface Vlan 1050
ip address 172.105.0.2 255.255.255.0
exit

vlan create 1051 type port-mstprstp 0
vlan i-sid 1051 1501051
interface Vlan 1051
ip address 172.105.1.2 255.255.255.0
exit
```

RSMLT Configuration

- Configure RSMLT to peer the BEB-110 and -111 in Campus1, forming a redundant router gateway for the specified VLANs from the access switches.

```
vlan create 2 type port-mstprstp 0
vlan i-sid 2 2200
interface Vlan 2
ip address 2.2.2.1 255.255.255.0 0
exit

virtual-ist peer-ip 2.2.2.2 vlan 2

router isis
spbm 1 smlt-virtual-bmac 00:bb:00:01:10:11
spbm 1 smlt-peer-system-id 00bb.0000.0111
exit

router isis enable

interface GigabitEthernet 1/1
no spanning-tree mstp
yes
no shutdown
exit

interface GigabitEthernet 1/2
```

```
no spanning-tree mstp
yes
no shutdown
exit

mlt 1 enable
mlt 1 member 1/1
mlt 1 encapsulation dot1q

mlt 2 enable
mlt 2 member 1/2
mlt 2 encapsulation dot1q

interface mlt 1
smlt
exit

interface mlt 2
smlt
exit
```

- Enable RSMLT on the desired VLANs:

```
interface vlan 100
ip rsmlt
ip rsmlt holdup-timer 9999
exit

interface Vlan 101
ip rsmlt
ip rsmlt holdup-timer 9999
exit

interface Vlan 102
ip rsmlt
ip rsmlt holdup-timer 9999
exit

interface Vlan 103
ip rsmlt
ip rsmlt holdup-timer 9999
exit

interface Vlan 104
ip rsmlt
ip rsmlt holdup-timer 9999
exit

ip rsmlt edge-support
```

DVR Configuration

- Configure the DVR instance and enable DVR on the desired IP interfaces.

```
dvr controller 10

interface Vlan 1050
dvr gw-ipv4 172.105.0.1
dvr enable
exit

interface Vlan 1051
dvr gw-ipv4 172.105.1.1
dvr enable
exit

interface vlan 1052
dvr gw-ipv4 172.105.2.1
dvr enable
exit
```

From Global mode, configure the DVR domain id for Campus 1. BEB-110 and -111 will share this id.

Routing Policies - Redistribution

- The redistribution configuration will be the same as the Campus 2 configuration:

```
router isis
redistribute direct
redistribute direct enable
ipv6 redistribute direct enable

router vrf iot
isis redistribute direct
isis redistribute direct enable
exit

router vrf surveillance
isis redistribute direct
isis redistribute direct enable
exit

isis apply redistribute direct
isis apply redistribute direct vrf iot
isis apply redistribute direct vrf surveillance
```

Route-Maps and IS-IS Accept Policies

GRT Policy:

```
router isis
accept i-sid 1800904 enable
accept i-sid 1800911 enable
exit
```

VRF “IoT” Routing Policy:

```

router vrf iot
ip prefix-list "GRT_mgmt" 172.9.99.0/24 id 1 ge 24 le 24
ip prefix-list "GRT_910" 172.90.1.0/24 id 2 ge 24 le 24

route-map "accept_GRT_mgmt" 1
permit
enable
match network "GRT_mgmt,GRT_910"

route-map "accept_GRT_mgmt" 2
no permit
enable
exit

isis accept i-sid 0 enable
isis accept i-sid 0 route-map "accept_GRT_mgmt"
exit

```

VRF “Surveillance” Routing Policy:

```

router vrf surveillance
ip prefix-list "GRT_mgmt" 172.9.99.0/24 id 1 ge 24 le 24
ip prefix-list "GRT_stor" 172.90.3.0/24 id 2 ge 24 le 24

route-map "accept_GRT_mgmt" 1
permit
enable
match network "GRT_mgmt,GRT_stor"
route-map "accept_GRT_mgmt" 2
no permit
enable
exit
exit

router vrf surveillance
isis accept i-sid 0 enable
isis accept i-sid 0 route-map "accept_GRT_mgmt"
exit

isis apply accept
isis apply accept vrf iot
isis apply accept vrf surveillance

```

Fabric Attach

```

interface mlt 1
fa
fa enable
no fa message-authentication
fa management i-sid 1010100 c-vid 100
exit

interface mlt 2
fa
fa enable
no fa message-authentication
fa management i-sid 1010100 c-vid 100
exit

```


Fabric Connect – Campus 3 Configuration

Overview

This section will illustrate configuring the Campus 3 BEB switches (-310 and -311), and the interconnection to the Fabric Connect core. The access layer in Campus 3 utilizes ERS Access switches.

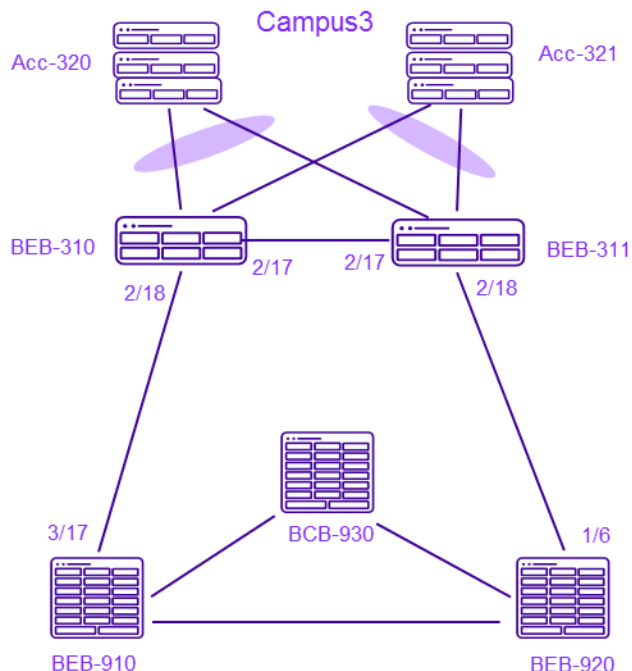
The BEB Fabric nodes are where the access data VLANs are created and assigned to a service. There are no L2/L3 configurations on the BCB switch, which allows for the core to be totally independent of any changes or modifications on the edge of the network.

After the initial SPB configuration, the process consists of the following steps:

- VRF creation for L3VSN services.
- VLAN creation, I-SID mapping, and VRF assignment.
- Enabling global VRF I-SID and VSN.
- Default Gateway protocol configuration (RSMLT and DVR).
- Redistribution/routing policies.

Note

- An L2VSN will be used for the Wired IOT Bridged VLAN (907).
- L3VSNs will be used for the IoT and Surveillance VLANs.
- The remaining VLANs will be routed on the Global Routing Table via IP Shortcuts.



Campus 3 (VLAN 3xx):

Role/Segment	VLAN	ISID	Subnet	Def Gateway	VRF	VRF ISID
FA Mgmt. VLAN	300	1030300	172.30.10.0/24	RSMLT	GRT	N/A
Wired IoT (routed)	301	1030301	172.30.20.0/22	RSMLT	VRF 1	1800911
Administrator (wired)	302	1030302	172.30.24.0/22	RSMLT	GRT	N/A
Campus User(wired)	303	1030303	172.30.28.0/22	RSMLT	GRT	N/A
Surveillance	304	1030304	172.30.32.0/22	RSMLT	VRF 2	1800904

Common Services:

Role/Segment	VLAN	ISID	Subnet	Def Gateway	VRF	VRF ISID
Administrator(wireless)	1050	1501050	172.105.0.0/24	DVR	GRT	N/A
Campus Users (wireless)	1051	1501051	172.105.1.0/24	DVR	GRT	N/A
IoT Devices (wireless)	1052	1501052	172.105.2.0/24	DVR	VRF 1	1800911
Guest (wireless)	906	1090906	172.90.40.0/24	EWC	Tunnel	N/A
Wired IoT(bridged)	907	1090907	N/A	N/A	L2VSN	N/A

Core Interface Configuration

As the base IS-IS configuration is already complete on the core Fabric Connect switches, all that's required on the core switches to connect the campus is to enable IS-IS on the connecting interfaces.

- To connect Campus 3 to the core Fabric Connect nodes:

BEB-910 Configuration:

```
Vlan member remove 1 3/17
interface GigabitEthernet 3/17
encapsulation dot1q
isis
isis spbm 1
isis enable
no shutdown
exit
```

BCB-920 Configuration:

```
Vlan member remove 1 1/6
interface GigabitEthernet 1/6
encapsulation dot1q
isis
isis spbm 1
isis enable
no shutdown
exit
```

BEB-310 Configuration

Note

An L2 VSN will be used for VLAN 907. The L2 VSN in the Automated Campus is created dynamically based on Fabric Attach requests from the FA client, therefore no manual configuration is necessary on the BEBs. When an end-user authenticates and is assigned to this VLAN/ISID, VLAN 907 will dynamically be added to the access and uplink ports.

As FA is not used in the server room, L2VSN configuration is required on those switches.

IS-IS and VLAN Configuration

1. Enter the base IS-IS configuration (from previous section) and loopback interfaces:

```
config terminal
prompt "BEB-8404-310"
spbm
interface loopback 1
ip address 1 10.0.0.210/255.255.255.255
ipv6 interface address 8200:0:0:0:0:0:210/128
exit

router isis
spbm 1
spbm 1 nick-name 0.03.10
spbm 1 b-vid 4051-4052 primary 4051
sys-name "BEB-8284-310"
system-id 00bb.0000.0310
manual-area 49.0000
ip-source-address 10.0.3.10
ipv6-source-address 8200:0:0:0:0:0:310
spbm 1 ip enable
spbm 1 ipv6 enable
exit
vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan
vlan member remove 1 1/1-1/2,1/41-1/42
sys clipId-topology-ip 1
sys force-topology-ip-flag

interface GigabitEthernet 2/17
isis
isis spbm 1
isis enable
no shutdown
exit
interface GigabitEthernet 2/18
isis
isis spbm 1
isis enable
no shutdown
exit
```

As both IPv4/v6 are requirements for the Campus User VLAN, enable IPv6 and set an IPv6 loopback on fabric nodes routing IPv6 subnets.

Set advertised IP addresses and globally enable IP Shortcut functionality.

2. Create the VRFs and enable the L3VSN services:

```
ip vrf iot vrfid 1
ip vrf surveillance vrfid 2

router vrf iot
ipvpn
i-sid 1800911
ipvpn enable
exit

router vrf surveillance
ipvpn
i-sid 1800904
ipvpn enable
exit
```

Provide a name and VRF id.

Assign the VRF I-SID to the L3VSN, and enable the service.

3. Create VLANs, I-SIDs and IP interfaces for the L3VSNs:

- The IoT Campus wired (301) and wireless (1052) VLANs are created and added to the IoT VRF.
- The Surveillance (304) VLAN is created and added to the Surveillance VRF.

```
vlan create 301 type port-mstprstp 0
vlan i-sid 301 1030301
interface Vlan 301
vrf iot
ip address 172.30.20.1 255.255.252.0
exit

vlan create 1052 type port-mstprstp 0
vlan i-sid 1052 1501052
interface Vlan 1052
vrf iot
ip address 172.105.2.6 255.255.255.0
exit

vlan create 304 type port-mstprstp 0
vlan i-sid 304 1030304
interface Vlan 304
vrf surveillance
ip address 172.30.32.1 255.255.252.0
exit
```

Create VLAN, map VLAN to associated I-SID

Assign VLAN to VRF for L3VSN service

Configure IP interface.

4. Create the VLANs and interfaces for networks that will use the Global Routing Table:

- The Device Mgmt (300), Administrator (302,1050) and Campus User (303,1051) VLANs are created and I-SIDs assigned.

```

vlan create 300 type port-mstprstp 0
vlan i-sid 300 1030300
interface Vlan 300
ip address 172.30.10.1 255.255.255.0
exit

vlan create 302 type port-mstprstp 0
vlan i-sid 302 1030302
interface Vlan 302
ip address 172.30.24.1 255.255.252.0
exit

vlan create 303 type port-mstprstp 0
vlan i-sid 303 1030303
interface Vlan 303
ip address 172.30.28.1 255.255.252.0
ipv6 interface enable
ipv6 interface address 8200:303:0:0:0:0:1/64
exit

vlan create 1050 type port-mstprstp 0
vlan i-sid 1050 1501050
interface Vlan 1050
ip address 172.105.0.6 255.255.255.0
exit

vlan create 1051 type port-mstprstp 0
vlan i-sid 1051 1501051
interface Vlan 1051
ip address 172.105.1.6 255.255.255.0
exit

```

Callout 1: Create VLAN, map VLAN to associated I-SID

Callout 2: Configure IPv6 interfaces on VLAN 303, as this VLAN requires dual-stack support.

Callout 3: Configure IP interfaces on the VLANs.

- Verification of VLAN I-SIDs:

```

BEB-8404-310:1(config)#show vlan i-sid

=====
Vlan I-SID
=====
VLAN_ID  I-SID
-----
1
300      1030300
301      1030301
302      1030302
303      1030303
304      1030304
1050     1501050
1051     1501051
1052     1501052
4051
4052

```

RSMLT Configuration

- Configure RSMLT on BEB-310 to peer to BEB-311, forming a redundant router gateway for the specified VLANs from the access switches.

```

vlan create 3 type port-mstprstp 0
vlan i-sid 3 3300
interface Vlan 3
ip address 3.3.3.1 255.255.255.0
exit

virtual-ist peer-ip 3.3.3.2 vlan 3

router isis
spbm 1 smlt-virtual-bmac 00:bb:00:03:10:11
spbm 1 smlt-peer-system-id 00bb.0000.0311
exit

router isis enable

interface GigabitEthernet 2/1
no spanning-tree mstp
no shutdown
exit

interface GigabitEthernet 2/2
no spanning-tree mstp
no shutdown
exit

m1t 1 enable
m1t 1 member 2/1
m1t 1 encapsulation dot1q

m1t 2 enable
m1t 2 member 2/2
m1t 2 encapsulation dot1q

interface m1t 1
smlt
exit

interface m1t 2
smlt
exit

```

Configure VLAN/IP/I-SID used for vIST control communication between the MLT peers. This is locally significant for the MLT only.

Configure BEB-311's IP, designated as the vIST IP address.

Configure shared MLT virtual MAC (same on both peers) and the MLT peer system id address of BEB-311.

Once smlt parameters are configured, globally enable ISIS.

Disable spanning tree on the gig interfaces to be used for the MLT.

Configure the MLT instances, and assign the corresponding ports to each.

Under each MLT interface, configure Split Multi-Link Trunking (SMLT) to allow the LAG to be distributed across both BEBs to the access switch.

- Enable RSMLT on the desired VLANs:

```

interface vlan 300
ip rsmlt
ip rsmlt holdup-timer 9999
exit

interface Vlan 301
ip rsmlt
ip rsmlt holdup-timer 9999
exit

interface Vlan 302
ip rsmlt
ip rsmlt holdup-timer 9999
exit

```

Enable RSMLT on associated VLANs, indicating these VLANs will function as an RSMLT gateway.

Configure RSMLT holdup-timer to "9999" (infinity). This allows the redundant switch to forward the other switch's traffic indefinitely if its unreachable.

```
interface Vlan 303
ip rsmlt
ip rsmlt holdup-timer 9999
exit
```

```
interface Vlan 304
ip rsmlt
ip rsmlt holdup-timer 9999
exit
```

```
ip rsmlt edge-support
```

When enabling Edge-Support, each RSMLT peer will learn the other's IP and MAC address information, allowing one to resume the routing duties for the other in case of an outage.

- Once the peer switch is also configured on the corresponding VLANs, they will communicate over the vIST to discover the peer's information:

```
BEB-8404-310:1#show ip rsmlt local
```

```
=====
                          Ip Rsmlt Local Info - GlobalRouter
=====
```

VID	IP	MAC	ADMIN	OPER	HDTMR	HUTMR
300	172.30.10.1	64:6a:52:ce:0d:00	Enable	Up	60	infinity
302	172.30.24.1	64:6a:52:ce:0d:02	Enable	Up	60	infinity
303	172.30.28.1	64:6a:52:ce:0d:03	Enable	Up	60	infinity

```
VID  SMLT ID
-----
300      1, 2
302
303      1, 2
```

VID	IPv6	MAC	ADMIN	OPER	HDTMR	HUTMR
303	8200:303:0:0:0:0:0:0/64 8200:303:0:0:0:0:0:1/64 fe80:0:0:0:666a:52ff:fece:d03/128	64:6a:52:ce:0d:03	Enable	Up	60	infinity

```
VID  SMLT ID
-----
303      1, 2
```

```
BEB- BEB-8404-310:1#show ip rsmlt peer
```

```
=====
                          Ip Rsmlt Peer Info - GlobalRouter
=====
```

VID	IP	MAC	ADMIN	OPER	HDTMR	HUTMR
300	172.30.10.2	64:6a:52:c5:39:01	Enable	Up	60	infinity
302	172.30.24.2	64:6a:52:c5:39:03	Enable	Up	60	infinity
303	172.30.28.2	64:6a:52:c5:39:04	Enable	Up	60	infinity

```
VID  HDT REMAIN  HUT REMAIN  SMLT ID
-----
300  60           infinity    1, 2
```

```

302 60 infinity
303 60 infinity 1, 2

VID IPv6 MAC ADMIN OPER HDTMR HUTMR
-----
303 8200:303:0:0:0:0:0/64 Enable Up 60 infinity
8200:303:0:0:0:0:2/64
fe80:0:0:0:666a:52ff:fec5:3904/128

VID HDT REMAIN HUT REMAIN SMLT ID
-----
303 60 infinity 1, 2

```

DVR Configuration (Controllers only)

DVR is configured in all campuses for the wireless networks (IoT, Administrator and Campus User), specifying the BEBs as Controllers. Although the Server Rooms will have a full Controller-Leaf configuration, no Leaf configuration is required for the Campus DVR deployment.

Configuring DVR in the campuses for wireless networks extends those VLANs and subnets across the campuses, allowing for seamless roaming.

- Configure the DVR instance and enable DVR on the desired IP interfaces.

```

dvr controller 30

interface Vlan 1050
dvr gw-ipv4 172.105.0.1
dvr enable
exit

interface Vlan 1051
dvr gw-ipv4 172.105.1.1
dvr enable
exit

interface vlan 1052
dvr gw-ipv4 172.105.2.1
dvr enable
exit

```

From Global mode, configure the DVR domain id. BEB-310 and -311 will share this id. The BEBs in other Campuses will have different domain id's.

Enable DVR for each Access VLAN, specifying the shared Default GW IP to be used,

- Verification:

```
BEB- BEB-8404-310:1#show dvr interfaces
```

```

=====
DVR Interfaces
=====
SPBMC IGMP Admin
Interface Mask L3ISID VRFID L2ISID VLAN GW IPv4 State
State Version
-----
172.105.0.6 255.255.255.0 0 0 1501050 1050 172.105.0.1 enable
disable 2
172.105.1.6 255.255.255.0 0 0 1501051 1051 172.105.1.1 enable
disable 2
172.105.2.6 255.255.255.0 1800911 1 1501052 1052 172.105.2.1 enable
disable 2

```

```
3 out of 3 Total Num of DVR Interfaces displayed
```


Routing Policies - Overview

One of the benefits of Virtual Service Networks is the security and traffic isolation that occurs between them. However, network environments still require some controlled access between subnets, VRFs and DVR domains. Route Maps and IS-IS accept policies allow routes to be advertised across these boundaries.

The following are the current route policies applied on BEBs in the Automated Campus EVD.

Note

Given the security and traffic isolation inherent in Fabric Connect, routing policy and redistribution are vital concepts in allowing inter-domain communication and may require further research and assistance than the overview in this document.

The GRT and VRF instances that are created become separate routing domains and therefore have separate, isolated routing tables. DVR domains (which are created within one or both) also act as a separate routing domain (i.e. a domain within a domain).

Routing Policies - Redistribution

Fabric Connect uses one global IS-IS instance for reachability information. When vln interfaces are created on fabric nodes within the same domain (GRT or VRF) in different parts of the network, those directly connected routes need to be redistributed into IS-IS for reachability WITHIN that routing domain.

```

router isis
redistribute direct
redistribute direct enable
ipv6 redistribute direct enable
exit

router vrf iot
isis redistribute direct
isis redistribute direct enable
exit

router vrf surveillance
isis redistribute direct
isis redistribute direct enable
exit

isis apply redistribute direct
isis apply redistribute direct vrf iot
isis apply redistribute direct vrf surveillance
  
```

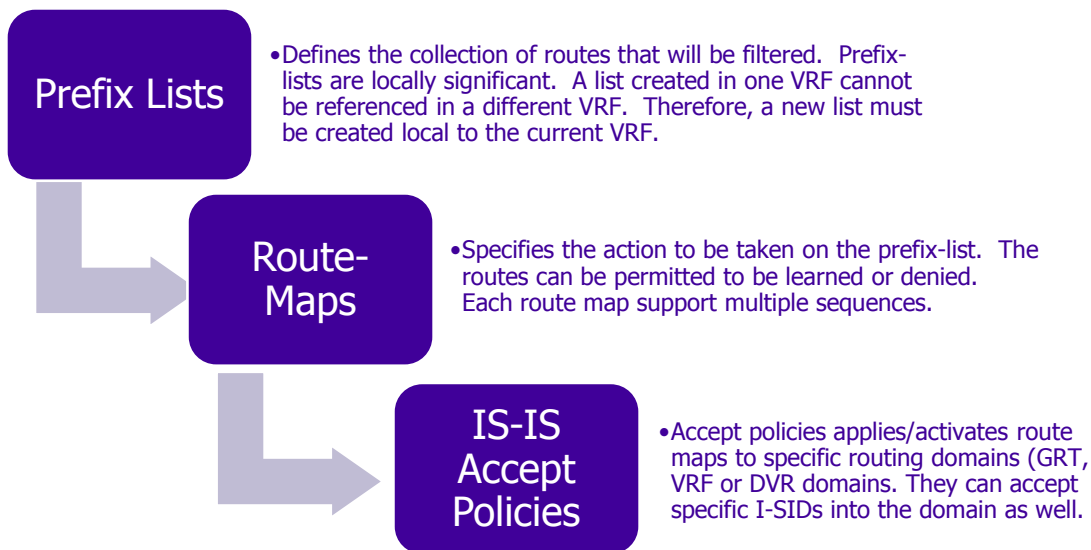
Redistribute directly connected routes into the GRT's IS-IS instance.

Within each VRF instance, redistribute directly connected routes into its IS-IS instance.

Apply redistribution to GRT and each VRF.

Route-Maps and IS-IS Accept Policies

For routes to be advertised or "leaked" between the GRT, VRFs, or DVR domains, prefix-lists, route-maps and IS-IS accept policies are configured.



For example, the DVR domains created in the campuses and server rooms are separate domains, and by default, do not share routing information. For the domains to exchange routing information, route-policies must be configured to share them across the DVR backbone.

GRT Routing Policy:

- The Global Routing Table on BEB-310 has the following requirements:
 - Reachability to networks in VRFs requiring centralized services located in the GRT (DHCP, production servers, etc.).
 - The Wireless Administrator (1050) and Campus User (1051) VLANS, which have DVR enabled, needs to be advertised to the DVR backbone, allowing route information to be shared with other corresponding networks in the DVR backbone (in Campus 1, for example).
- 9Configure IS-IS Accept policies, to import routes from the specified VRFs:

```
router isis
accept i-sid 1800904 enable
accept i-sid 1800911 enable
exit
```

Imports global I-SIDs for Surveillance and IoT VRF. No route-map needed, as all routes in these VRFs are being accepted.

VRF “IoT” Routing Policy:

- The VRF IoT has the following requirements:
 - Reachability between all IoT VLANs in the campuses and server rooms. This is accomplished when the IoT VLANs in these locations are added to the IoT VRF (L3VSN).
 - Access to the Production Server network and the Network Management subnet (both in the Server Room on the GRT).
 - The Wireless IoT VLAN (1052) which has DVR enabled, needs to be advertised to VRF IoT’s DVR backbone, allowing route information to be shared with other IoT networks in the DVR backbone (in Campus 1, for example).
- Within VRF iot, create prefix-lists identifying the routes above:

```
router vrf iot
ip prefix-list "GRT_mgmt" 172.9.99.0/24 id 1 ge 24 le 24
ip prefix-list "GRT_910" 172.90.1.0/24 id 2 ge 24 le 24
```

- Create route-maps matching/permitting the corresponding prefix-lists:

```
route-map "accept_GRT_mgmt" 1
permit
enable
match network "GRT_mgmt,GRT_910"

route-map "accept_GRT_mgmt" 2
no permit
enable
exit
```

Permit routes matching both the GRT_mgmt and GRT_910 prefix-lists.
Deny all other routes being learned.

- Configure IS-IS Accept policies, importing specific GRT routes matching the route-map:

```
router vrf iot
isis accept i-sid 0 enable
isis accept i-sid 0 route-map "accept_GRT_mgmt"
exit
```

Imports the GRT_mgmt prefix-list from GRT (I-SID 0).

VRF “Surveillance” Routing Policy:

- The VRF Surveillance has the following requirements:
 - Reachability from the Surveillance VLANs in the campuses to the server rooms. This is accomplished when the Surveillance VLANs in these locations are added to the Surveillance VRF (L3VSN).
 - Access to the Network Mgmt subnet (for DHCP) and the Storage subnet (for video recordings).

- Configure prefix-lists, route-maps and accept policies for the “surveillance” VRF:

```

router vrf surveillance
ip prefix-list "GRT_mgmt" 172.9.99.0/24 id 1 ge 24 le 24
ip prefix-list "GRT_stor" 172.90.3.0/24 id 2 ge 24 le 24

route-map "accept_GRT_mgmt" 1
permit
enable
match network "GRT_mgmt,GRT_stor"
route-map "accept_GRT_mgmt" 2
no permit
enable
exit

isis accept i-sid 0 enable
isis accept i-sid 0 route-map "accept_GRT_mgmt"
exit

isis apply accept
isis apply accept vrf iot
isis apply accept vrf surveillance

```

Define the routes to import from the GRT.

Permit routes matching those prefix-lists.

Accept the routes from the GRT defined in the route-map.

Apply the accept policies to the GRT and both VRFs.

Fabric Attach

Fabric Attach uses the IEEE802.1ab *LLDP (Link Layer Discovery Protocol)* extensions to automatically attach network devices to individual services in a Fabric Connect network. These network devices typically do not support SPB, MAC-in-MAC (802.1ah) or Network Services Identifier (NSI)/Individual Service Identifier (I-SID) usage, and therefore cannot easily take advantage of the Fabric infrastructure without manual configuration of VLAN attachments to NSIs or ISIDs in multiple locations. Fabric Attach deals with this issue by facilitating automated network device discovery and the automatic configuration and teardown of NSI/ISID to VLAN associations at the edge of the network.

Upon connection and detection of an FA Client, the FA Server (BEB) will advertise (via LLDP) the management I-SID/VLAN to the FA-Proxy switch.

The FA Proxy on the access switch communicates directly with the FA server on the BEB to request VLAN to I-SID mappings for user traffic.

Enter the following on BEB-310:

```

interface mlt 1
fa
fa enable
no fa message-authentication
fa management i-sid 1030300 c-vid 300
exit

interface mlt 2
fa
fa enable
no fa message-authentication
fa management i-sid 1030300 c-vid 300
exit

```

Under each MLT interface (connecting to the access switches), enable Fabric Attach.

Set the Management I-SID and VLAN that will be advertised to the FA client.

Feature disabled until released on EXOS.

BEB-311 Configuration (Peer)

BEB-311, acting as the RSMLT peer to BEB-310 will follow the same steps for configuration as BEB-310. Once both BEBs are configured, they can be connected to each other and to the core fabric nodes.

IS-IS and VLAN Configuration

- Enter the base IS-IS configuration and loopback interfaces:

```

config terminal
  prompt "BEB-8404-311"
  spbm

interface loopback 1
ip address 1 10.0.3.11/255.255.255.255
ipv6 interface address 8200:0:0:0:0:0:0:311/128
exit

router isis
  spbm 1
  spbm 1 nick-name 0.03.11
  spbm 1 b-vid 4051-4052 primary 4051
  sys-name "BEB-8284-311"
  system-id 00bb.0000.0311
  ip-source-address 10.0.3.11
  ipv6-source-address 8200:0:0:0:0:0:0:311
  spbm 1 ip enable
  spbm 1 ipv6 enable
  manual-area 49.0000
  exit

vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan
sys clipId-topology-ip 1
sys force-topology-ip-flag
vlan member remove 1 1/1-1/2,2/1-2/18,3/1-3/24
interface GigabitEthernet 2/17
  encapsulation dot1q
  isis
  isis spbm 1
  isis enable
  no shutdown
  exit
interface GigabitEthernet 2/18
  encapsulation dot1q
  isis
  isis spbm 1
  isis enable
  no shutdown
  exit

```

- Create the VRFs and enable the L3VSN services:

```

ip vrf iot vrfid 1
ip vrf surveillance vrfid 2

router vrf iot
  ipvpn
  i-sid 1800911
  ipvpn enable
  exit
router vrf surveillance
  ipvpn
  i-sid 1800904

```

```

ipvpn enable
exit

```

- Create VLANs, I-SIDs and IP interfaces for the L3VSNs:
 - The IoT Campus wired (301) and wireless (1052) VLANs are created and added to the IoT VRF.
 - The Surveillance (304) VLAN is created and added to the Surveillance VRF.

```

vlan create 301 type port-mstprstp 0
vlan i-sid 301 1030301
interface Vlan 301
vrf iot
ip address 172.30.20.2 255.255.252.0
exit

vlan create 1052 type port-mstprstp 0
vlan i-sid 1052 1501052
interface Vlan 1052
vrf iot
ip address 172.105.2.5 255.255.255.0
exit

vlan create 304 type port-mstprstp 0
vlan i-sid 304 1030304
interface Vlan 304
vrf surveillance
ip address 172.30.32.2 255.255.252.0
exit

```

- Create the VLANs and interfaces for networks that will use the Global Routing Table:
 - The Device Mgmt (300), Administrator (302,1050) and Campus User (303,1051) VLANs are created and I-SIDs assigned.

```

vlan create 300 type port-mstprstp 0
vlan i-sid 300 1030300
interface Vlan 300
ip address 172.30.10.2 255.255.255.0
exit

vlan create 302 type port-mstprstp 0
vlan i-sid 302 1030302
interface Vlan 302
ip address 172.30.24.2 255.255.252.0
exit

vlan create 303 type port-mstprstp 0
vlan i-sid 303 1030303
interface Vlan 303
ip address 172.30.28.2 255.255.252.0
ipv6 interface enable
ipv6 interface address 8200:303:0:0:0:0:0:2/64
exit

vlan create 1050 type port-mstprstp 0
vlan i-sid 1050 1501050
interface Vlan 1050
ip address 172.105.0.5 255.255.255.0
exit

vlan create 1051 type port-mstprstp 0
vlan i-sid 1051 1501051

```

```
interface Vlan 1051
ip address 172.105.1.5 255.255.255.0
exit
```

RSMLT Configuration

- Configure RSMLT to peer the BEB-311 and -310 BEBs. Be sure to specify the -310 values where called for.

```
vlan create 3 type port-mstprstp 0
vlan i-sid 3 3300
interface Vlan 3
ip address 3.3.3.2 255.255.255.0
exit

virtual-ist peer-ip 3.3.3.1 vlan 3

router isis
spbm 1 smlt-virtual-bmac 00:bb:00:03:10:11
spbm 1 smlt-peer-system-id 00bb.0000.0310
exit
```

```
router isis enable
```

Once smlt parameters are configured, globally enable ISIS.

```
interface GigabitEthernet 2/1
no spanning-tree mstp
yes
no shutdown
exit
```

```
interface GigabitEthernet 2/2
no spanning-tree mstp
yes
no shutdown
exit
```

```
mlt 1 enable
mlt 1 member 2/1
mlt 1 encapsulation dot1q
```

```
mlt 2 enable
mlt 2 member 2/2
mlt 2 encapsulation dot1q
```

```
interface mlt 1
smilt
exit
```

```
interface mlt 2
smilt
exit
```

- Enable RSMLT on the desired VLANs:

```
interface vlan 300
ip rsmlt
ip rsmlt holdup-timer 9999
exit
```

```
interface Vlan 301
ip rsmlt
ip rsmlt holdup-timer 9999
exit
```

```

interface Vlan 302
ip rsm1t
ip rsm1t holdup-timer 9999
exit

interface Vlan 303
ip rsm1t
ip rsm1t holdup-timer 9999
exit

interface Vlan 304
ip rsm1t
ip rsm1t holdup-timer 9999
exit

ip rsm1t edge-support

```

DVR Configuration (Controllers only)

- Configure the DVR instance and enable DVR on the desired IP interfaces.

```

dvr controller 30

interface Vlan 1050
dvr gw-ipv4 172.105.0.1
dvr enable
exit

interface Vlan 1051
dvr gw-ipv4 172.105.1.1
dvr enable
exit

interface vlan 1052
dvr gw-ipv4 172.105.2.1
dvr enable
exit

```

The DVR gateway IP will be the same address as configured in BEB-310 to allow for inter-campus roaming

Routing Policies - Redistribution

```

router isis
redistribute direct
redistribute direct enable
ipv6 redistribute direct enable
exit

router vrf iot
isis redistribute direct
isis redistribute direct enable
exit

router vrf surveillance
isis redistribute direct
isis redistribute direct enable
exit

isis apply redistribute direct
isis apply redistribute direct vrf iot
isis apply redistribute direct vrf surveillance

```


Route-Maps and IS-IS Accept Policies

- GRT Policy:

```
router isis
accept i-sid 1800904 enable
accept i-sid 1800911 enable
exit
```

- VRF “IoT” Routing Policy:

```
router vrf iot
ip prefix-list "GRT_mgmt" 172.9.99.0/24 id 1 ge 24 le 24
ip prefix-list "GRT_910" 172.90.1.0/24 id 2 ge 24 le 24

route-map "accept_GRT_mgmt" 1
permit
enable
match network "GRT_mgmt,GRT_910"

route-map "accept_GRT_mgmt" 2
no permit
enable
exit

isis accept i-sid 0 enable
isis accept i-sid 0 route-map "accept_GRT_mgmt"
exit
```

- VRF “Surveillance” Routing Policy:

```
router vrf surveillance
ip prefix-list "GRT_mgmt" 172.9.99.0/24 id 1 ge 24 le 24
ip prefix-list "GRT_stor" 172.90.3.0/24 id 2 ge 24 le 24

route-map "accept_GRT_routes" 1
permit
enable

match network "GRT_mgmt,GRT_stor"
route-map "accept_GRT_routes" 2
no permit
enable
exit
exit

router vrf surveillance
isis accept i-sid 0 enable
isis accept i-sid 0 route-map "accept_GRT_routes"
exit

isis apply accept
isis apply accept vrf iot
isis apply accept vrf surveillance
```

Fabric Attach

```
interface mlt 1
fa
fa enable
no fa message-authentication
fa management i-sid 1030300 c-vid 300
exit

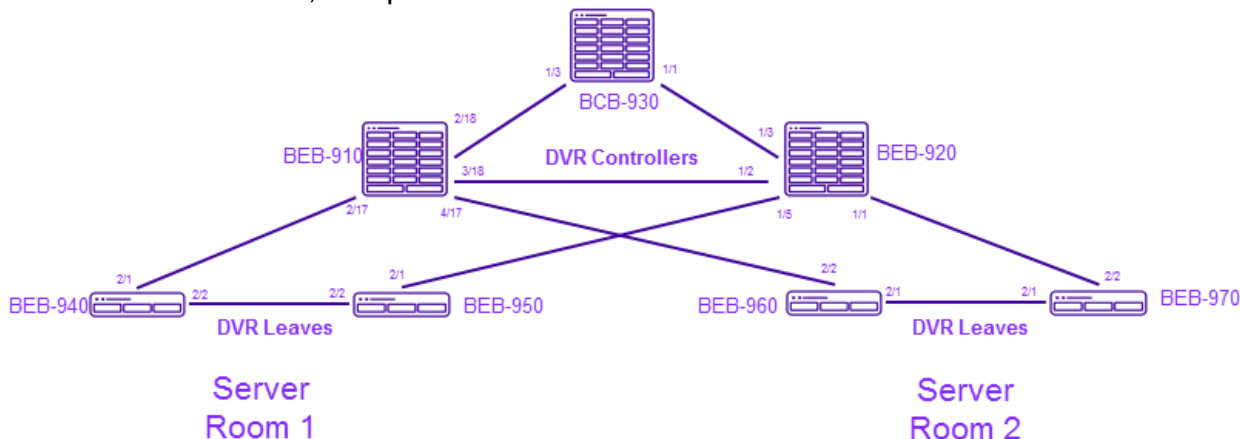
interface mlt 2
fa
fa enable
no fa message-authentication
fa management i-sid 1030300 c-vid 300
exit
```

Fabric Connect - Server Room Configuration

Overview

The two server rooms will be the home for the Extreme network management assets, including XMC, ExtremeControl, Extreme Analytics, Extreme Wireless controllers, DHCP/Radius servers, and other centralized server assets.

The server rooms are each front-ended by a pair of VSP-7200 switches, configured as DVR Leaves. The core switches (BEB-910 and BEB-920) will be configured as the DVR controllers for this domain. Although not all are members of L3VSNs, all VLANs in the server rooms will be DVR-enabled to allow seamless migration between server rooms, if required.



Server Room (VLAN 9xx):

Role/Segment	VLAN	ISID	Subnet	Def Gateway	VRF	VRF ISID
Production Servers	900	1090900	172.90.1.0/24	DVR	GRT	N/A
Test Servers	901	1090901	172.90.2.0/24	DVR	GRT	N/A
Storage Servers	902	1090902	172.90.3.0/24	DVR	GRT	N/A
Storage Test	903	1090903	172.90.4.0/24	DVR	GRT	N/A
Network Mgmt.	999	1090999	172.9.99.0/24	DVR	GRT	N/A
Network Mgmt. (EWC)	998	1090998	172.9.98.0/24	DVR	GRT	N/A
Wired IoT (routed)	911	1090911	172.90.20.0/22	DVR	VRF 1	1800911
Surveillance	904	1090904	172.90.14.0/22	DVR	VRF 2	1800904
Wired IoT (bridged)	907	1090907	N/A	N/A	L2VSN	N/A

Common Services:

Role/Segment	VLAN	ISID	Subnet	Def Gateway	VRF	VRF ISID
Guest (wireless)	906	1090906	172.90.40.0/24	EWC	Tunnel	N/A
Wired IoT(bridged)	907	1090907	N/A	N/A	L2VSN	N/A

BEB-910 Configuration (DVR Controller)

IS-IS Configuration to Server Rooms

As the initial IS-IS configuration was already done during core configuration, only the interfaces connecting to the server rooms are required.

```
interface GigabitEthernet 2/17
encapsulation dot1q
no shutdown
isis
isis spbm 1
isis enable
no spanning-tree mstp
yes
exit

interface GigabitEthernet 4/17
encapsulation dot1q
no shutdown
isis
isis spbm 1
isis enable
no spanning-tree mstp
yes
exit
```

Configure the interfaces connecting to the leaves.

VRF and VSN Creation

- On BEB-910, create the VRFs and configure the L3VSN services.

```
ip vrf iot vrfid 1
ip vrf surveillance vrfid 2

router vrf iot
ipvpn
i-sid 1800911
ipvpn enable
exit

router vrf surveillance
ipvpn
i-sid 1800904
ipvpn enable
exit
```

Create the VRFs and the corresponding L3VSN service. Assign the global I-SID, and enable the VPN for each.

The VRF I-SIDs correspond with the VSNs in the campus BEBs, creating an isolated virtual service for those VRFs.

VLAN Configuration

- Configure the Server VLANs hosted in the server rooms, residing on the GRT:

```
vlan create 900 type port-mstprstp 0
vlan i-sid 900 1090900
interface Vlan 900
ip address 172.90.1.2 255.255.255.0
exit

vlan create 901 type port-mstprstp 0
vlan i-sid 901 1090901
interface Vlan 901
ip address 172.90.2.2 255.255.255.0
exit

vlan create 902 type port-mstprstp 0
vlan i-sid 902 1090902
interface Vlan 902
ip address 172.90.3.2 255.255.255.0
exit

vlan create 903 type port-mstprstp 0
vlan i-sid 903 1090903
interface Vlan 903
ip address 172.90.4.2 255.255.255.0
exit
```

Create required VLANs for server room applications (Production, Prod Test, Storage, Storage Test). Map to corresponding I-SID.

- Configure the IoT, Surveillance, Guest and Network Management VLANs:

```
vlan create 904 type port-mstprstp 0
vlan i-sid 904 1090904
interface Vlan 904
vrf surveillance
ip address 172.90.14.2 255.255.252.0
exit

vlan create 906 type port-mstprstp 0
vlan i-sid 906 1090906
interface Vlan 906
ip address 172.90.40.2 255.255.255.0
exit

vlan create 911 type port-mstprstp 0
vlan i-sid 911 1090911
interface Vlan 911
vrf iot
ip address 172.90.20.2 255.255.252.0
exit

vlan create 998 type port-mstprstp 0
vlan i-sid 998 1090998
interface Vlan 998
ip address 172.9.98.2 255.255.255.0
exit

vlan create 999 type port-mstprstp 0
vlan i-sid 999 1090999
interface Vlan 999
ip address 172.9.99.2 255.255.255.0
exit
```

Surveillance VLAN/IP interface, assigned to the VRF.

Guest VLAN/interface for traffic emerging from the wireless tunnel between AP and the EWC.

IoT Server VLAN/interface, assigned to the VRF.

Extreme Wireless Controller VLAN/interface

Network Mgmt VLAN (XMC, ExtremeControl, DHCP/Radius servers)

DVR Configuration

- Configure the DVR instance, and enable DVR on the desired IP interfaces, specifying the IP that will act as default gateway for that VLAN. As VLAN 907 is an L2VSN, no default gateway is configured.

```
dvr controller 90
```

```
interface Vlan 900
dvr gw-ipv4 172.90.1.1
dvr enable
exit
```

```
interface Vlan 901
dvr gw-ipv4 172.90.2.1
dvr enable
exit
```

```
interface Vlan 902
dvr gw-ipv4 172.90.3.1
dvr enable
exit
```

```
interface Vlan 903
dvr gw-ipv4 172.90.4.1
dvr enable
exit
```

```
interface Vlan 904
dvr gw-ipv4 172.90.14.1
dvr enable
exit
```

```
interface Vlan 906
dvr gw-ipv4 172.90.40.1
dvr enable
exit
```

```
interface Vlan 911
dvr gw-ipv4 172.90.20.1
dvr enable
exit
```

```
interface Vlan 998
dvr gw-ipv4 172.9.98.1
dvr enable
exit
```

```
interface Vlan 999
dvr gw-ipv4 172.9.99.1
dvr enable
exit
```

From Global mode, configure the DVR domain id for the Server Room. BEB-910 and -920 will share this id.

Specify the IP interface that will be each subnet's default gateway.

All VLANs in the server rooms (with the exception of 907) will have DVR enabled.

Redistribution

- Redistribute directly connected networks and static routes for GRT and all VRFs present on the controller into their respective IS-IS instances and apply.

```

router isis
redistribute direct
redistribute direct enable
ipv6 redistribute direct enable
exit

router vrf iot
isis redistribute direct
isis redistribute direct enable
exit

router vrf surveillance
isis redistribute direct
isis redistribute direct enable
exit
isis apply redistribute direct
isis apply redistribute direct vrf iot
isis apply redistribute direct vrf surveillance

```

Redistribute direct routes into GRT ISIS Domain.

Redistribute direct routes from each VRF into each VRF ISIS Domain.

Route Maps and Accept Policies

- Configure routing policy for the GRT VLANs:

```

router isis
accept i-sid 1800911 enable
exit

```

Accepting routes from VRF IoT, which includes Server Room2 as well as the Campus IoT VRFs.

BEB-920 Configuration (DVR Controller)

As BEB-920 is a paired controller with -910, the configuration will be, except for the IP interface configuration, almost identical.

IS-IS Configuration to Server Rooms

As the initial IS-IS configuration was already done during core configuration, only the interfaces connecting to the server rooms are required.

```

Vlan member remove 1 1/1,1/5

interface GigabitEthernet 1/1
encapsulation dot1q
no shutdown
isis
isis spbm 1
isis enable
no spanning-tree mstp
yes
exit
interface GigabitEthernet 1/5
encapsulation dot1q
no shutdown
isis
isis spbm 1
isis enable
no spanning-tree mstp
yes
exit

```

VRF and VSN Creation

- On BEB-920, create the VRFs and configure the L3VSN services.

```
ip vrf iot vrfid 1
ip vrf surveillance vrfid 2

router vrf iot
  ipvpn
  i-sid 1800911
  ipvpn enable
  exit

router vrf surveillance
  ipvpn
  i-sid 1800904
  ipvpn enable
  exit
```

VLAN Configuration

- Configure the Server VLANs hosted in the server rooms.

```
vlan create 900 type port-mstprstp 0
vlan i-sid 900 1090900
interface Vlan 900
ip address 172.90.1.3 255.255.255.0
exit

vlan create 901 type port-mstprstp 0
vlan i-sid 901 1090901
interface Vlan 901
ip address 172.90.2.3 255.255.255.0
exit

vlan create 902 type port-mstprstp 0
vlan i-sid 902 1090902
interface Vlan 902
ip address 172.90.3.3 255.255.255.0
exit

vlan create 903 type port-mstprstp 0
vlan i-sid 903 1090903
interface Vlan 903
ip address 172.90.4.3 255.255.255.0
exit
```

Create required VLANs for server room applications (Production, Prod Test, Storage, Storage Test). Map to corresponding I-SID.

- Configure the IoT, Surveillance, Guest and Network Management VLANs:

```
vlan create 904 type port-mstprstp 0
vlan i-sid 904 1090904
interface Vlan 904
vrf surveillance
ip address 172.90.14.3 255.255.252.0
exit

vlan create 906 type port-mstprstp 0
vlan i-sid 906 1090906
interface Vlan 906
ip address 172.90.40.3 255.255.255.0
exit

vlan create 911 type port-mstprstp 0
vlan i-sid 911 1090911
```

The same VLAN and I-SID values are assigned as on BEB-910, with a different IP interface configured.


```

interface Vlan 911
vrf iot
ip address 172.90.20.3 255.255.252.0
exit

vlan create 998 type port-mstprstp 0
vlan i-sid 998 1090998
interface Vlan 998
ip address 172.9.98.3 255.255.255.0
exit

vlan create 999 type port-mstprstp 0
vlan i-sid 999 1090999
interface Vlan 999
ip address 172.9.99.3 255.255.255.0
exit

```

- Enable IPv6 Shortcut functionality at the global level.

DVR Configuration

- Configure the DVR instance, and enable DVR on the desired IP interfaces, specifying the IP that will act as default gateway for that VLAN. As VLAN 907 is an L2VSN, no default gateway is configured.

```

dvr controller 90

interface Vlan 900
dvr gw-ipv4 172.90.1.1
dvr enable
exit

interface Vlan 901
dvr gw-ipv4 172.90.2.1
dvr enable
exit

interface Vlan 902
dvr gw-ipv4 172.90.3.1
dvr enable
exit

interface Vlan 903
dvr gw-ipv4 172.90.4.1
dvr enable
exit

interface Vlan 904
dvr gw-ipv4 172.90.14.1
dvr enable
exit

interface Vlan 906
dvr gw-ipv4 172.90.40.1
dvr enable
exit

interface Vlan 911
dvr gw-ipv4 172.90.20.1
dvr enable
exit

interface Vlan 998
dvr gw-ipv4 172.9.98.1
dvr enable

```

From Global mode, configure the DVR domain id for the Server Room. BEB-910 and -920 will share this id.

Specify the IP interface that will be each subnet's default gateway

All VLANs in the server rooms (with the exception of 907) will have DVR enabled.

```

exit

interface Vlan 999
dvr gw-ipv4 172.9.99.1
dvr enable
exit

```

Redistribution

- Redistribute directly connected networks and static routes for GRT and all VRFs present on the controller into their respective IS-IS instances and apply.

```

router isis
redistribute direct
redistribute direct enable
ipv6 redistribute direct enable
exit

router vrf iot
isis redistribute direct
isis redistribute direct enable
exit

router vrf surveillance
isis redistribute direct
isis redistribute direct enable
exit

isis apply redistribute direct
isis apply redistribute direct vrf iot
isis apply redistribute direct vrf surveillance

```

Redistribute direct routes into GRT ISIS Domain.

Redistribute direct routes from each VRF into each VRF ISIS Domain.

Route Maps and Accept Policies

- Configure routing policy for the GRT VLANs:

```

router isis
accept i-sid 1800911 enable
exit

```

Accepting routes from VRF IoT, which includes Server Room2 as well as the Campus IoT VRFs.

BEB-960 (DVR Leaf)

Each server room will have 2 Leaf nodes clustered together in an SMLT for Extreme Management, the Extreme Wireless Controllers, and other appliance redundancy. The following section illustrates the steps to configure BEB-960. The same steps will apply to all the Leaf nodes.

Attaching hosts to the Leaf requires a specific interface setting option:

- Switched UNI (Flex) – a combination of VLAN ID and a Port maps to a L2 VSN. With this UNI type, VLAN IDs can be re-used on other ports and therefore mapped to different VSNs.
- Transparent Port UNI – a physical port maps to a L2 VSN. All traffic through that port, 802.1Q tagged or untagged, ingress and egress is mapped to the VSN.

For the purposes of the EVD, all host-attached interfaces will be set to Flex-UNI.

IS-IS Configuration

- Enable the DVR-leaf-mode flag.

Warning

Setting this flag will prompt the user to save the configuration and reboot the system. Much of the system's current configuration will be cleared, so it's highly recommended to follow this step first.

```
boot config flags dvr-leaf-mode
y
save config
reset
```

- After reset, configure the switch for IS-IS.

```
config terminal
prompt "BEB-7254-960"
spbm
```

```
router isis
spbm 1
spbm 1 nick-name 0.09.60
spbm 1 b-vid 4051-4052 primary 4051
sys-name "BEB-7254-960"
inband-mgmt-ip 10.0.9.60
system-id 00bb.0000.0960
manual-area 49.0000
exit
```

In DVR Leaf mode, setting the management IP address only requires the **inband-mgmt-ip** command.

```
vlan members remove 1 1/1-1/48,2/1-2/6 portmember
vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan
```

Remove network ports from default VLAN before configuring.

```
interface GigabitEthernet 2/1
encapsulation dot1q
no shutdown
isis
isis spbm 1
isis enable
no spanning-tree mstp
yes
exit
```

```
interface GigabitEthernet 2/2
encapsulation dot1q
no shutdown
isis
isis spbm 1
isis enable
no spanning-tree mstp
yes
exit
```

```
sys force-topology-ip-flag
```

MLT, DVR and Interface Configuration

- Configure SMLT between the Leaf pairs for dual-attached hosts.
- DVR Leaves in this EVD are configured as clusters (via a vIST), with one cluster of two Leaf nodes in each server room. Both server rooms are configured in the same DVR domain.

```

router isis
spbm 1 smlt-virtual-bmac 00:bb:00:00:60:70
spbm 1 smlt-peer-system-id 00bb.0000.0970
exit

dvr leaf 90
dvr leaf virtual-ist 90.90.90.1 255.255.255.0 peer-ip 90.90.90.2 cluster-id 90

router isis enable

mlt 1 enable
mlt 1 member 1/3
mlt 1 encapsulation dot1q

mlt 2 enable
mlt 2 member 1/5
mlt 2 encapsulation dot1q

mlt 3 enable
mlt 3 member 1/25
mlt 3 encapsulation dot1q

```

Set shared SMLT gateway MAC and SMLT peer id.

Set the DVR domain id and vIST IP interface, and specify the SMLT peer leaf IP (BEB-970).

Bind BEB-960's MLT instances to physical interfaces.

- Configure Flex-UNI mode on host-connected ports.

```

interface mlt 1
smlt
flex-uni enable
exit
interface mlt 2
smlt
flex-uni enable
exit
interface mlt 3
smlt
flex-uni enable
exit

interface GigabitEthernet 1/13
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/20
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/22
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

```

Enable SMLT feature on MLT interfaces.

Enable Flex-UNI mode on MLT interfaces (connecting to dual-attached hosts) and other interfaces (connecting to single-connection servers).

```

interface GigabitEthernet 1/24
default-vlan-id 0
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

```

VLAN/I-SID Configuration

- Configure VLAN/I-SID to physical or logical port where server(s) are connected.

```

i-sid 1090900 elan
untagged-traffic port 1/13,1/22
exit

```

I-SID mapping for untagged single stations

```

i-sid 1090901 elan
c-vid 901 port 1/35
exit

```

```

i-sid 1090902 elan
c-vid 902 port 1/36
exit

```

```

i-sid 1090903 elan
c-vid 903 port 1/37
exit

```

```

i-sid 1090904 elan
c-vid 904 port 1/33
exit

```

```

i-sid 1090906 elan
c-vid 906 mlt 2
exit

```

I-SID mapping for tagged traffic.

```

i-sid 1090911 elan
c-vid 911 port 1/13,1/33
exit

```

```

i-sid 1090998 elan
untagged-traffic mlt 2
exit

```

I-SID mapping for untagged dual-attached stations.

```

i-sid 1090999 elan
untagged-traffic mlt 1
untagged-traffic mlt 3
exit

```

- Confirm I-SID mappings.

```
7254-960:1(config)#show i-sid
```

Isid Info					
ISID ID	ISID TYPE	VLANID	PORT INTERFACES	MLT INTERFACES	ORIGIN
1090900	ELAN	2	u:1/22	-	CONFIG
1090901	ELAN	3	c901:1/40	-	CONFIG
1090902	ELAN	4	c902:1/41	-	CONFIG
1090903	ELAN	5	c903:1/42	-	CONFIG
1090904	ELAN	10	c904:1/33	-	CONFIG
1090906	ELAN	6	-	c906:2	CONFIG
1090911	ELAN	9	c911:1/13,1/33	-	CONFIG
1090998	ELAN	7	-	u:2	CONFIG
1090999	ELAN	8	-	u:1,3	CONFIG
16677305	CVLAN	4002	-	-	CONFIG
16777001	ELAN	N/A	-	-	CONFIG

VLAN ID on Leaf nodes is only logical value, not actual C-VID.

Indicates the physical or MLT interface bound to each I-SID

BEB-970 (DVR Leaf)

The Leaf cluster configuration will be, other than IP configuration, identical.

IS-IS Configuration

- Enable the DVR-leaf-mode flag.

Warning

Setting this flag will prompt the user to save the configuration and reboot the system. Much of the system's current configuration will be cleared, so its highly recommended to follow this step first.

```
boot config flags dvr-leaf-mode
```

- Configure the switch for IS-IS.

```
config terminal
prompt "BEB-7254-970"
spbm

router isis
spbm 1
spbm 1 nick-name 0.09.70
spbm 1 b-vid 4051-4052 primary 4051
sys-name "BEB-7254-970"
inband-mgmt-ip 10.0.9.70
system-id 00bb.0000.0970
manual-area 49.0000
exit

vlan members remove 1 1/1-1/48,2/1-2/6 portmember
vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan

interface GigabitEthernet 2/1
```

In DVR Leaf mode, setting the management IP address only requires the inband-mgmt-ip command.

```

encapsulation dot1q
default-vlan-id 0
no shutdown
isis
isis spbm 1
isis enable
no spanning-tree mstp
yes
exit

interface GigabitEthernet 2/2
encapsulation dot1q
default-vlan-id 0
no shutdown
isis
isis spbm 1
isis enable
no spanning-tree mstp
yes
exit

sys force-topology-ip-flag

```

MLT, DVR and Interface Configuration

- Configure SMLT between the Leaf pairs for dual-attached hosts.
- DVR Leaves in this EVD are configured as clusters (via a vIST), with one cluster of two Leaf nodes in each server room. Both server rooms are configured in the same DVR domain.

```

router isis
spbm 1 smlt-virtual-bmac 00:bb:00:00:60:70
spbm 1 smlt-peer-system-id 00bb.0000.0960
exit

dvr leaf 90
dvr leaf virtual-ist 90.90.90.2 255.255.255.0 peer-ip 90.90.90.1 cluster-id 90

router isis enable

mlt 1 enable
mlt 1 member 1/3
mlt 1 encapsulation dot1q

mlt 2 enable
mlt 2 member 1/5
mlt 2 encapsulation dot1q

mlt 3 enable
mlt 3 member 1/25
mlt 3 encapsulation dot1q

```

Set shared SMLT gateway MAC and SMLT peer id.

Bind BEB-970's MLT instances to physical interfaces.

- Configure Flex-UNI mode on host-connected ports.

```

interface mlt 1
smlt
flex-uni enable
exit
interface mlt 2
smlt
flex-uni enable
exit
interface mlt 3
smlt

```

```

flex-uni enable
exit

interface GigabitEthernet 1/13
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/20
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/22
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/35
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/36
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/37
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/40
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

```

VLAN/I-SID Configuration

- Configure VLAN/I-SID to physical or logical port where server(s) are connected.

```

i-sid 1090900 elan
untagged-traffic port 1/13,1/22
exit

i-sid 1090901 elan
c-vid 901 port 1/35
exit

i-sid 1090902 elan

```



```

c-vid 902 port 1/36
exit

i-sid 1090903 elan
c-vid 903 port 1/37
exit

i-sid 1090904 elan
c-vid 904 port 1/40
exit

i-sid 1090906 elan
c-vid 906 mlt 2
exit

i-sid 1090907 elan
untagged-traffic port 1/20,1/40
exit

i-sid 1090911 elan
c-vid 911 port 1/13
exit

i-sid 1090998 elan
untagged-traffic mlt 2
exit

i-sid 1090999 elan
untagged-traffic mlt 1
untagged-traffic mlt 3
exit

```

- Confirm I-SID mappings.

```
BEB-7254-970:1(config)#show i-sid
```

```

=====
                        Isid Info
=====
ISID      ISID      VLANID    PORT          MLT           ORIGIN
ID        TYPE                               INTERFACES    INTERFACES
-----
1090900   ELAN      2          u:1/13,1/22   -             CONFIG
1090901   ELAN      3          c901:1/35     -             CONFIG
1090902   ELAN      4          c902:1/36     -             CONFIG
1090903   ELAN      5          c903:1/37     -             CONFIG
1090904   ELAN      10         c904:1/40     -             CONFIG
1090906   ELAN      6          -             c906:2       CONFIG
1090907   ELAN      N/A        u:1/20,1/40   -             CONFIG
1090911   ELAN      9          c911:1/13     -             CONFIG
1090998   ELAN      7          -             u:2          CONFIG
1090999   ELAN      8          -             u:1,3        CONFIG
16677305  CVLAN     4002       -             -             CONFIG
16777001  ELAN      N/A        -             -             CONFIG
c: customer vid    u: untagged-traffic

```

BEB-940 (DVR Leaf)

The Leaf nodes in Server Room 2 will also be clustered together and follow the same configuration steps.

IS-IS Configuration

- Set switch to DVR Leaf mode:

```
config terminal
boot config flags dvr-leaf-mode
save config
reset
```

- Configure the switch for IS-IS.

```
config terminal
prompt "BEB-7254-940"
spbm

router isis
spbm 1
spbm 1 nick-name 0.09.40
spbm 1 b-vid 4051-4052 primary 4051
sys-name "BEB-7254-940"
inband-mgmt-ip 10.0.9.40
system-id 00bb.0000.0940
manual-area 49.0000
exit

vlan members remove 1 1/1-1/48,2/1-2/6 portmember
vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan

interface GigabitEthernet 2/1
encapsulation dot1q
no shutdown
isis
isis spbm 1
isis enable
no spanning-tree mstp
yes
exit

interface GigabitEthernet 2/2
encapsulation dot1q
no shutdown
isis
isis spbm 1
isis enable
no spanning-tree mstp
yes
exit

sys force-topology-ip-flag
```

MLT, DVR and Interface Configuration

- Configure SMLT between the Leaf pairs for dual-attached hosts.

```

router isis
spbm 1 smlt-virtual-bmac 00:bb:00:00:11:50
spbm 1 smlt-peer-system-id 00bb.0000.0950
exit

dvr leaf 90
dvr leaf virtual-ist 91.91.91.1 255.255.255.0 peer-ip 91.91.91.2 cluster-id 91

router isis enable

mlt 1 enable
mlt 1 member 1/5
mlt 1 encapsulation dot1q

mlt 2 enable
mlt 2 member 1/25
mlt 2 encapsulation dot1q

```

- Configure Flex-UNI mode on host-connected ports.

```

interface mlt 1
smlt
flex-uni enable
exit
interface mlt 2
smlt
flex-uni enable
exit

interface GigabitEthernet 1/13
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/20
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/22
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/35
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/36
flex-uni enable
no shutdown
no spanning-tree mstp
yes

```

```
exit

interface GigabitEthernet 1/37
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit
```

VLAN/I-SID Configuration

- Configure VLAN/I-SID to physical or logical port where server(s) are connected.

```
i-sid 1090900 elan
untagged-traffic port 1/13
exit

i-sid 1090901 elan
c-vid 901 port 1/35
exit

i-sid 1090902 elan
c-vid 902 port 1/36
exit

i-sid 1090903 elan
c-vid 903 port 1/37
exit

i-sid 1090904 elan
c-vid 904 port 1/20
exit

i-sid 1090906 elan
c-vid 906 mlt 1
exit

i-sid 1090907 elan
untagged-traffic port 1/20
exit

i-sid 1090998 elan
untagged-traffic mlt 1
exit

i-sid 1090999 elan
untagged-traffic mlt 2
exit
```

- Confirm I-SID mappings:

```
BEB-7254-940:1(config)#show i-sid
```

```
=====
                        Isid Info
=====
ISID      ISID      PORT      MLT      ORIGIN
ID        TYPE      VLANID    INTERFACES  INTERFACES
-----
1090900   ELAN      10        u:1/13      -          CONFIG
1090901   ELAN      11        c901:1/35   -          CONFIG
1090902   ELAN      12        c902:1/36   -          CONFIG
1090903   ELAN      13        c903:1/37   -          CONFIG
1090904   ELAN      18        c904:1/20   -          CONFIG
1090906   ELAN      14        -           c906:1     CONFIG
1090907   ELAN      N/A       c907:1/20   -          CONFIG
1090911   CVLAN     17        -           -          CONFIG
1090998   ELAN      15        -           u:1        CONFIG
1090999   ELAN      16        -           u:2        CONFIG
16677306  CVLAN     4002     -           -          CONFIG
16777001  ELAN      N/A       -           -          CONFIG
```

```
c: customer vid    u: untagged-traffic
```

BEB-950 (DVR Leaf)

The Leaf cluster configuration will be, other than IP configuration, identical.

IS-IS Configuration

- Set switch to DVR Leaf mode:

```
config terminal
boot config flags dvr-leaf-mode
save config
reset
```

- Configure the switch for IS-IS.

```
config terminal
prompt "BEB-7254-950"
spbm

router isis
spbm 1
spbm 1 nick-name 0.09.50
spbm 1 b-vid 4051-4052 primary 4051
sys-name "BEB-7254-950"
inband-mgmt-ip 10.0.9.50
system-id 00bb.0000.0950
manual-area 49.0000
exit

vlan members remove 1 1/1-1/48,2/1-2/6 portmember
vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan

interface GigabitEthernet 2/1
encapsulation dot1q
no shutdown
isis
isis spbm 1
isis enable
no spanning-tree mstp
yes
exit

interface GigabitEthernet 2/2
encapsulation dot1q
no shutdown
isis
isis spbm 1
isis enable
no spanning-tree mstp
yes
exit

sys force-topology-ip-flag
```

In DVR Leaf mode, setting the management IP address only requires the inband-mgmt-ip command.

MLT, DVR and Interface Configuration

- Configure SMLT between the Leaf pairs for dual-attached hosts.

```

router isis
spbm 1 smlt-virtual-bmac 00:00:00:00:11:50
spbm 1 smlt-peer-system-id 00bb.0000.0940
exit

dvr leaf 90
dvr leaf virtual-ist 91.91.91.2 255.255.255.0 peer-ip 91.91.91.1 cluster-id 91

router isis enable

mlt 1 enable
mlt 1 member 1/5
mlt 1 encapsulation dot1q

mlt 2 enable
mlt 2 member 1/25
mlt 2 encapsulation dot1q

```

- Configure Flex-UNI mode on host-connected ports.

```

interface mlt 1
smlt
flex-uni enable
exit
interface mlt 2
smlt
flex-uni enable
exit

interface GigabitEthernet 1/13
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/20
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/22
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/35
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/36
flex-uni enable
no shutdown
no spanning-tree mstp

```

```
yes
exit

interface GigabitEthernet 1/37
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit

interface GigabitEthernet 1/40
flex-uni enable
no shutdown
no spanning-tree mstp
yes
exit
```

VLAN/I-SID Configuration

- Configure VLAN/I-SID to physical or logical port where server(s) are connected.

```
i-sid i-sid 1090900 elan
c-vid 900 port 1/22
exit

i-sid 1090901 elan
c-vid 901 port 1/35
exit

i-sid 1090902 elan
c-vid 902 port 1/36
exit

i-sid 1090903 elan
c-vid 903 port 1/37
exit

i-sid 1090904 elan
c-vid 904 port 1/13,1/20
exit

i-sid 1090906 elan
c-vid 906 mlt 1
exit

i-sid 1090907 elan
c-vid 907 port 1/13
exit

i-sid 1090998 elan
untagged-traffic mlt 1
exit

i-sid 1090999 elan
untagged-traffic mlt 2
exit
```


- Confirm I-SID mappings.

```
BEB-7254-950:1(config)#show i-sid
```

```
=====
                                Isid Info
=====
```

ISID ID	ISID TYPE	VLANID	PORT INTERFACES	MLT INTERFACES	ORIGIN
1090900	ELAN	10	c900:1/22	-	CONFIG
1090901	ELAN	11	c901:1/35	-	CONFIG
1090902	ELAN	12	c902:1/36	-	CONFIG
1090903	ELAN	13	c903:1/37	-	CONFIG
1090904	ELAN	18	c904:1/13,1/20	-	CONFIG
1090906	ELAN	14	-	c906:1	CONFIG
1090907	ELAN	N/A	c907:1/13 u:1/20	-	CONFIG
1090911	CVLAN	17	-	-	CONFIG
1090998	ELAN	15	-	u:1	CONFIG
1090999	ELAN	16	-	u:2	CONFIG
16677306	CVLAN	4002	-	-	CONFIG
16777001	ELAN	N/A	-	-	CONFIG

```
c: customer vid    u: untagged-traffic
```

- Confirm DVR Domain members. BEB-910 and -920 should show as controllers for the four leaves:

```
BEB-7254-950:1(config)#show dvr members
```

```
=====
                                DVR Members (Domain ID: 90)
=====
```

System Name	Nick-Name	Nodal MAC	Role
BEB-8404-910	0.09.10	00:bb:00:00:09:10	Controller
BEB-8404-920	0.09.20	00:bb:00:00:09:20	Controller
BEB-7254-940	0.09.40	00:bb:00:00:09:40	Leaf
BEB-7254-950	0.09.50	00:bb:00:00:09:50	Leaf
BEB-7254-960	0.09.60	00:bb:00:00:09:60	Leaf
BEB-7254-970	0.09.70	00:bb:00:00:09:70	Leaf

```
6 out of 6 Total Num of DVR Members displayed
```

- Connect the Extreme Management Assets and network servers to their corresponding ports in the server rooms.

Route Table Verification

With the Fabric Connect network configured, the following are illustrations of the resulting route tables.

- BEB-210 Global Routing Table:

```

BEB- BEB-8284-210:1(config)#show ip route
=====
                        IP Route - GlobalRouter
=====
DST                MASK                NEXT                NH                COST                INTER                PROT AGE TYPE PRF
-----
2.1.1.1.0          255.255.255.0      2.1.1.1            -                 1                   2                   LOC  0  DB  0
10.0.0.10          255.255.255.255   BEB-8404-910       GlobalRouter       30                  4051                ISIS 0  IBS  7
10.0.0.20          255.255.255.255   BEB-8404-920       GlobalRouter       20                  4051                ISIS 0  IBS  7
10.0.0.110        255.255.255.255   BEB-8284-110       GlobalRouter       20030               4051                ISIS 0  IBS  7
10.0.0.111        255.255.255.255   BEB-8284-111       GlobalRouter       20040               4051                ISIS 0  IBS  7
10.0.0.210        255.255.255.255   10.0.0.210         -                 1                   0                   LOC  0  DB  0
10.0.0.211        255.255.255.255   BEB-8284-211       GlobalRouter       10                  4051                ISIS 0  IBS  7
10.0.3.10          255.255.255.255   BEB-8404-310       GlobalRouter       30                  4051                ISIS 0  IBS  7
10.0.3.11          255.255.255.255   BEB-8404-311       GlobalRouter       30                  4051                ISIS 0  IBS  7
10.0.9.40          255.255.255.255   BEB-7254-940       GlobalRouter       40                  4051                ISIS 0  IBS  7
10.0.9.50          255.255.255.255   BEB-7254-950       GlobalRouter       30                  4051                ISIS 0  IBS  7
10.0.9.60          255.255.255.255   BEB-7254-960       GlobalRouter       40                  4051                ISIS 0  IBS  7
10.0.9.70          255.255.255.255   BEB-7254-970       GlobalRouter       30                  4051                ISIS 0  IBS  7
172.9.98.0         255.255.255.0     BEB-8404-920       GlobalRouter       20                  4051                ISIS 0  IBS  7
172.9.99.0         255.255.255.0     BEB-8404-920       GlobalRouter       20                  4051                ISIS 0  IBS  7
172.10.10.0        255.255.255.0     BEB-8284-110       GlobalRouter       30                  4051                ISIS 0  IBS  7
172.10.20.0        255.255.252.0     BEB-8284-110       iot                20030               4051                ISIS 0  IBS  7
172.10.24.0        255.255.252.0     BEB-8284-110       GlobalRouter       20030               4051                ISIS 0  IBSV 200
172.10.28.0        255.255.252.0     BEB-8284-110       surveillance        20030               4051                ISIS 0  IBSV 200
172.10.32.0        255.255.252.0     BEB-8284-110       surveillance        20030               4051                ISIS 0  IBSV 200
172.20.10.0        255.255.255.0     172.20.10.1        -                 1                   200                LOC  0  DB  0
172.20.20.0        255.255.252.0     172.20.20.1        iot                1                   4051                ISIS 0  IBSV 200
172.20.24.0        255.255.252.0     172.20.24.1        -                 1                   202                LOC  0  DB  0
172.20.28.0        255.255.252.0     172.20.28.1        -                 1                   203                LOC  0  DB  0
172.20.32.0        255.255.252.0     172.20.32.1        surveillance        1                   4051                ISIS 0  IBSV 200
172.30.10.0        255.255.255.0     BEB-8404-311       GlobalRouter       30                  4051                ISIS 0  IBS  7
172.30.20.0        255.255.252.0     BEB-8404-311       iot                30                  4051                ISIS 0  IBSV 200
172.30.24.0        255.255.252.0     BEB-8404-311       GlobalRouter       30                  4051                ISIS 0  IBS  7
172.30.28.0        255.255.252.0     BEB-8404-311       GlobalRouter       30                  4051                ISIS 0  IBS  7
172.30.32.0        255.255.252.0     BEB-8404-311       surveillance        30                  4051                ISIS 0  IBSV 200

172.90.1.0         255.255.255.0     BEB-8404-920       GlobalRouter       20                  4051                ISIS 0  IBS  7
172.90.2.0         255.255.255.0     BEB-8404-920       GlobalRouter       20                  4051                ISIS 0  IBS  7
172.90.3.0         255.255.255.0     BEB-8404-920       GlobalRouter       20                  4051                ISIS 0  IBS  7
172.90.4.0         255.255.255.0     BEB-8404-920       GlobalRouter       20                  4051                ISIS 0  IBS  7
172.90.5.0         255.255.255.0     BEB-8404-920       GlobalRouter       20                  4051                ISIS 0  IBS  7
172.90.12.0        255.255.252.0     BEB-8404-920       surveillance        20                  4051                ISIS 0  IBSV 200
172.90.20.0        255.255.252.0     BEB-8404-920       iot                20                  4051                ISIS 0  IBSV 200
172.90.40.0        255.255.255.0     BEB-8404-920       GlobalRouter       20                  4051                ISIS 0  IBS  7
172.105.0.0        255.255.255.0     172.105.0.4        -                 1                   1050               LOC  0  DB  0
172.105.1.0        255.255.255.0     172.105.1.4        -                 1                   1051               LOC  0  DB  0
172.105.2.0        255.255.255.0     172.105.2.4        iot                1                   4051                ISIS 0  IBSV 200

51 out of 51 Total Num of Route Entries, 51 Total Num of Dest Networks displayed.
=====
TYPE Legend:
I=Indirect Route, D=Direct Route, A=Alternative Route, B=Best Route, E=Ecmp Route,
U=Unresolved Route, N=Not in HW, F=Replaced by FTN, V=IPVPN Route, S=SPBM Route
PROTOCOL Legend:
v=Inter-VRF route redistributed
    
```

Redistributed routes within the GRT from Server Rooms and Campus 1 and 3.

Routes received via Route-maps from VRF IOT and Surveillance.

• BEB-210 VRF IOT:

```

BEB-8284-210:1(config)#show ip route vrf iot
=====
IP Route - VRF iot
=====
DST          MASK          NEXT          NH          COST    INTER
VRF/ISID    FACE        PROT AGE  TYPE  PRF
-----
172.9.99.0   255.255.255.0  BEB-8404-910  GlobalRouter  20     4051    ISIS 0   IBSV 200
172.10.20.0  255.255.252.0  BEB-8284-111  iot          20010  4051    ISIS 0   IBSV 7
172.20.20.0  255.255.252.0  172.20.20.1  -            1      201     LOC 0   DB 0
172.30.20.0  255.255.252.0  BEB-8404-310  iot          30     4051    ISIS 0   IBSV 7
172.90.1.0   255.255.255.0  BEB-8404-910  GlobalRouter  20     4051    ISIS 0   IBSV 200
172.90.20.0  255.255.252.0  BEB-8404-910  iot          20     4051    ISIS 0   IBSV 7
172.105.2.0  255.255.255.0  172.105.2.4  -            1      1052    LOC 0   DB 0

14 out of 14 Total Num of Route Entries, 14 Total Num of Dest Networks displayed.
=====
TYPE Legend:
I=Indirect Route, D=Direct Route, A=Alternative Route, B=Best Route, U=Unresolved Route, N=Not in HW, F=Replaced by FTN, V=IPVPN Route, S=
PROTOCOL Legend:
v=Inter-VRF route redistributed
    
```

As a result of redistribution within the VRF, BEB-210 has route information on Campus1, 3 and Server Room IOT subnets.

As a result of route-map policies, VRF IOT on BEB-210 has route information for the Network Mgmt and Production Servers subnet in the GRT.

• BEB-210 VRF Surveillance:

```

BEB-8284-210:1(config)#show ip route vrf surveillance
=====
IP Route - VRF surveillance
=====
DST          MASK          NEXT          NH          COST    INTER
VRF/ISID    FACE        PROT AGE  TYPE  PRF
-----
172.9.99.0   255.255.255.0  BEB-8404-910  GlobalRouter  20     4051    ISIS 0   IBSV 200
172.10.32.0  255.255.252.0  BEB-8284-111  surveillance  20010  4051    ISIS 0   IBSV 7
172.20.32.0  255.255.252.0  172.20.32.1  -            1      204     LOC 0   DB 0
172.30.32.0  255.255.252.0  BEB-8404-310  surveillance  30     4051    ISIS 0   IBSV 7
172.90.3.0   255.255.255.0  BEB-8404-910  GlobalRouter  20     4051    ISIS 0   IBSV 200
172.90.12.0  255.255.252.0  BEB-8404-910  surveillance  20     4051    ISIS 0   IBSV 7

6 out of 6 Total Num of Route Entries, 6 Total Num of Dest Networks displayed.
=====
TYPE Legend:
I=Indirect Route, D=Direct Route, A=Alternative Route, B=Best Route, U=Unresolved Route, N=Not in HW, F=Replaced by FTN, V=IPVPN Route, S=
PROTOCOL Legend:
v=Inter-VRF route redistributed
    
```

Redistribution within the VRF, BEB-210 has route information on Campus1, 3 and Server Room Surveillance subnets.

As a result of route-map policies, BEB-210 has route information for the Network Mgmt network and the Storage subnet in the Server Room GRT.

• BEB-960 DVR Leaf Table:

```

BEB-7254-960:1(config)#show dvr database
=====
DVR DATABASE
=====
DEST          MASK          NEXT          VRFID  L3VSN  L2VSN  OUTGOING  SPB  PR
HOP          ISID      ISID      INTERFACE COST COST
-----
0.0.0.0       0.0.0.0       BEB-8404-920  0       0       0       2/1       10  1
1 day(s), 02:12:30
0.0.0.0       0.0.0.0       BEB-8404-910  0       0       0       2         10  1
1 day(s), 02:12:30
0.0.0.0       0.0.0.0       BEB-8404-920  2       1800904 0       2         10  1
1 day(s), 02:12:30
0.0.0.0       0.0.0.0       BEB-8404-910  2       1800904 0       2/1       10  1
1 day(s), 02:12:30
    
```

If unknown packet that's member of the GRT(0) or this VRF, its sent to DVR controller.

0.0.0.0	0.0.0.0	BEB-8404-920	1	1800911	0	2/1	10	1
1 day(s), 02:12:30								
0.0.0.0	0.0.0.0	BEB-8404-910	1	1800911	0	2/1	10	1
1 day(s), 02:12:30								
172.9.98.0	255.255.255.0	BEB-8404-920	0	0	1090998	2/1	10	1
1 day(s), 02:12:30								
172.9.98.0	255.255.255.0	BEB-8404-910	0				10	1
1 day(s), 02:12:30								
172.9.98.2	255.255.255.255	BEB-8404-910	0				10	1
1 day(s), 02:12:30								
172.9.98.3	255.255.255.255	BEB-8404-920	0	0	1090998	2/1	10	1
1 day(s), 02:12:30								
172.9.98.106	255.255.255.255	BEB-7254-970	0	0	1090998	MLT-2	10	1
1 day(s), 01:51:49								
172.9.98.106	255.255.255.255	BEB-7254-960	0	0	1090998	MLT-2	10	1
1 day(s), 01:51:49								
172.9.98.107	255.255.255.255	BEB-7254-950	0	0	1090998	2/1	10	1
0 day(s), 04:07:42								
172.9.98.107	255.255.255.255	BEB-7254-940	0	0	1090998	2/1	10	1
0 day(s), 04:07:42								
172.9.99.0	255.255.255.0	BEB-8404-920	9			2/1	10	1
1 day(s), 02:12:30								
172.9.99.0	255.255.255.0	BEB-8404-910	9			2/1	10	1
1 day(s), 02:12:30								

Known hosts connected to Leaf nodes, connected to specified port/MLT.

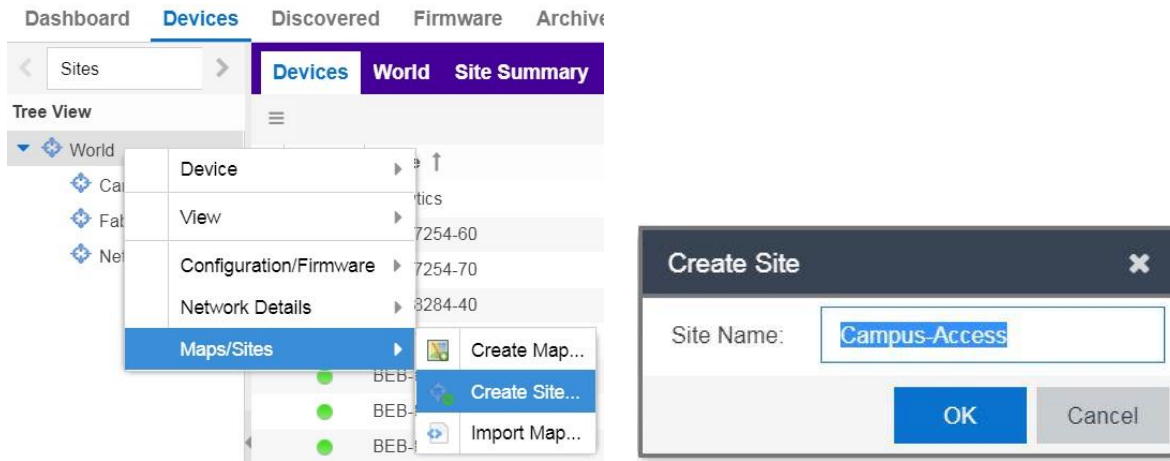
Known hosts learned from other Leaf nodes across DVR domain.

Extreme Management Center Configuration

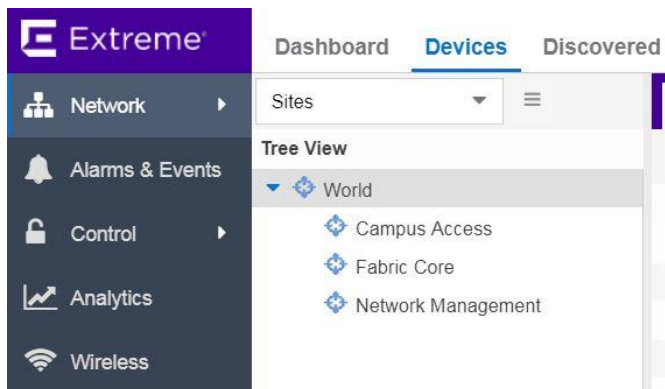
Site Configuration

Extreme Management Center provides the possibility to break a larger network into smaller, more manageable pieces by grouping switches and appliances under Sites. This logical separation, which can be done based on physical location or purpose, can help users understand more complex networks by allowing them to concentrate on smaller segments.

- To create a site, go to the **Devices** tab, right click on **World site**, go to **Maps/Sites** and select **Create Site**. Enter a site name and click **OK**.

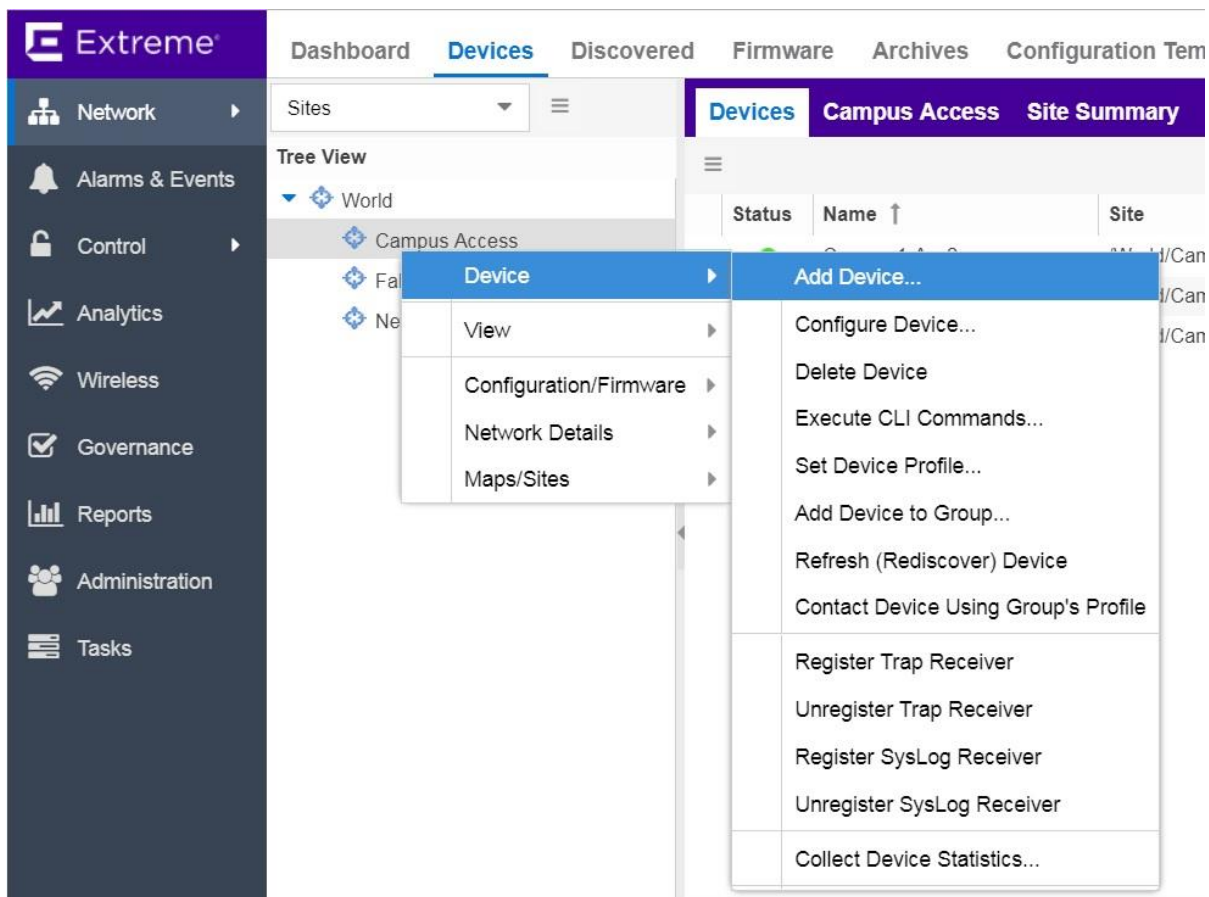


- Three sites were created in the Automated Campus to group devices based on their function.



Adding a Device to the Site Configuration

To add a device to a site, right-click on the site name and select **Add Device**.

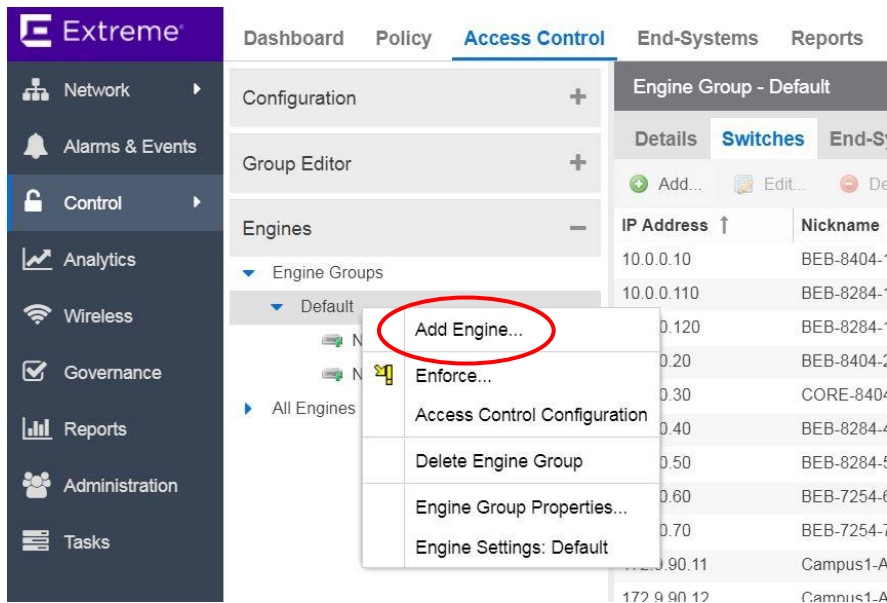


- The **Campus Access** site contains all the access switches deployed at the Campus edge:

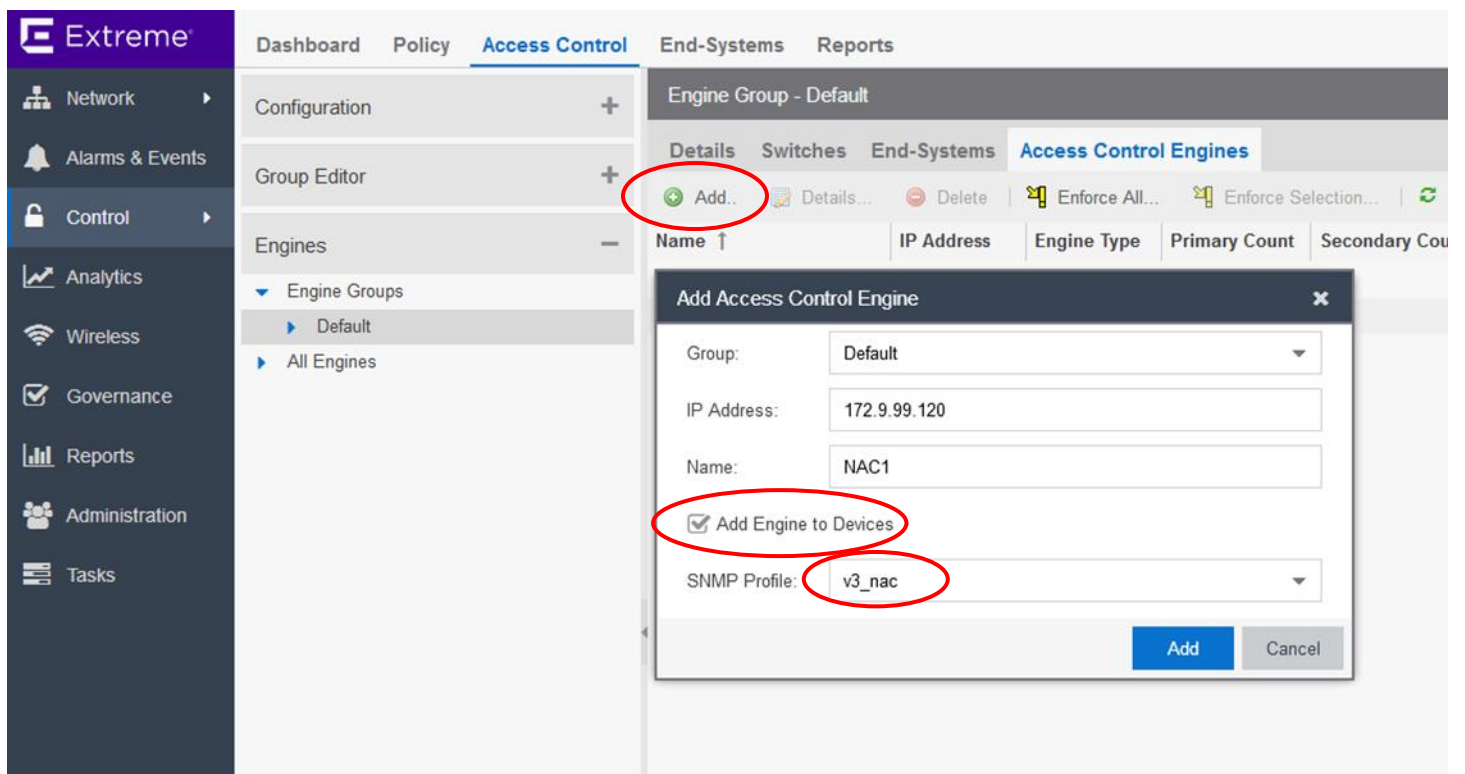


Adding an ExtremeControl Appliance to Extreme Management Center

- To add a new ExtremeControl engine to Extreme Management Center, go to **Control** → **Access Control** → **Engines** → **Engine Groups** → **Default**, right-click on **Default**, and click **Add Engine**.



- Enter the IP address of the engine. The Engine will also automatically be added to Devices with the **Add Engine to Devices** check box. Select the desired SNMP profile:



- Highlight the Engine, click Engine Settings:

Engine - NAC1/172.9.99.120

Details End-Systems Switches

Status: OK

Engine

IP Address: 172.9.99.120
Type: Virtual Access Control Engine
Version: 8.1.4.40
Serial Number: 564d698a30d5630d-dd0e...

Management

Configuration...
Engine Settings...

License

Update... Status:

Certificates

Manage...

Interface Summary

Edit...
Static Routes...

Bypass Configuration

Engine Settings - Default

Credentials Network Settings Auditing

Switch Configuration

Specify the shared secret to use when switches communicate with Access Control Engines.

Shared Secret:

RADIUS Timeout: 10

RADIUS Timeout Retry Count: 3

Use Primary RADIUS Server for Redundancy in a Single Engine Configuration. (Basic AAA Configuration only.)

SNMP Timeout: 3

Admin Web Page Credentials

Changes to the credentials will be propagated to the Access Control Engines on Enforce.

Username: admin

Save Cancel

Enter the "shared secret" for communication with this Engine through radius protocol.

Adding Fabric Switches to Extreme Management Center

The VSP switches comprising the Fabric Connect network can be added to Extreme Management Center for SNMP management, polling and to manage secure access. To add a device to Extreme Management Center, go to **Network** → **Devices** → **Devices**. Then, right-click (under either the Devices list or within the corresponding Site created in Tree View), selecting **Add Device**. This step uses the same SNMPv3 profile used previously.

Extreme

Dashboard Devices Discovered Firmware Archives Configuration Templates

Network

Alarms & Events

Control

Analytics

Wireless

Governance

Reports

Administration

Tasks

Sites

Tree View

- World
 - Campus Access
 - Fabric Core
 - Network Management

Devices Fabric Core Site Summary FlexRe

Status	Name ↑	Site
●	BEB-7254-940	/World/Fabric Core

Device

- View
- Configuration/Firmware
- Network Details
- Maps/Sites

Add Device...

- Configure Device...
- Delete Device
- Execute CLI Commands...
- Set Device Profile...
- Add Device to Group...
- Refresh (Rediscover) Device
- Contact Device Using Group's Profile
- Register Trap Receiver

- Enter the parameters for the switch, and click OK:

1. Enter the IP address of the VSP switch.
2. Select the desired SNMP profile.
3. Optional: Provide a nickname for how the device will be displayed.

Note

Refer to the [Design Considerations](#) for procedures on configuring an SNMPv3 profile in XMC.

- Repeat this process for the other VSP switches in the network. Check their status in the Devices view:

Status	Name ↑	Site	IP Address	Device Type	Family	Firmware
●	BEB-7254-940	/World/Fabric Core	10.0.9.40	VSP-7254XSQ	VSP Series	7.1.0.0
●	BEB-7254-950	/World/Fabric Core	10.0.9.50	VSP-7254XSQ	VSP Series	7.1.0.0
●	BEB-7254-960	/World/Fabric Core	10.0.9.60	VSP-7254XSQ	VSP Series	7.1.0.0
●	BEB-7254-970	/World/Fabric Core	10.0.9.70	VSP-7254XSQ	VSP Series	7.1.0.0
●	BEB-8284-110	/World/Fabric Core	10.0.0.110	VSP-8284XSQ	VSP Series	7.1.0.0
●	BEB-8284-111	/World/Fabric Core	10.0.0.111	VSP-8284XSQ	VSP Series	7.1.0.0
●	BEB-8284-210	/World/Fabric Core	10.0.0.210	VSP-8284XSQ	VSP Series	7.1.0.0
●	BEB-8284-211	/World/Fabric Core	10.0.0.211	VSP-8284XSQ	VSP Series	7.1.0.0
●	BEB-8404-10	/World/Fabric Core	10.0.0.10	VSP-8404	VSP Series	7.1.0.0
●	BEB-8404-20	/World/Fabric Core	10.0.0.20	VSP-8404	VSP Series	7.1.0.0
●	CORE-8404-30	/World/Fabric Core	10.0.0.30	VSP-8404C	VSP Series	7.1.0.0
●	INTERNET_GW	/World/Fabric Core	10.0.0.180	VSP-4850GTS-PWR+	VSP Series	7.1.0.0

Adding Wireless Controllers to Extreme Management Center

Like all network devices, the wireless controllers can be managed from Extreme Management Center. This step is necessary for the access control configuration. To add a device to Extreme Management Center, go to **Network** → **Devices** → **Devices**. Then, right-click (under either the Devices list or within the corresponding Site created in Tree View), selecting **Add Device**. This step uses the same SNMPv3 profile used previously.

The screenshot shows the Extreme Networks management console. The 'Devices' page is active for the 'Network Management' site. A table lists devices with columns for Status, Name, and Site. Two devices are visible: 'Analytics' and 'EWC1a'. A context menu is open over the 'EWC1a' device, showing options such as 'View', 'Configuration/Firmware', 'Network Details', 'Maps/Sites', and 'Add Device...'. The 'Add Device...' option is highlighted.

- The wireless controllers are added under the **Network Management** site.

The screenshot shows the Extreme Networks management console. The 'Devices' page is active for the 'Network Management' site. A table lists devices with columns for Status, Name, Site, IP Address, Device Type, Family, and Firmware. Three devices are visible: 'Analytics', 'EWC1a', and 'EWC1b'.

Status	Name ↑	Site	IP Address	Device Type	Family	Firmware
●	Analytics	/World/Network Managem...	172.9.99.122	Virtual Application An...	Extreme An...	8.1.3.65
●	EWC1a	/World/Network Managem...	172.9.98.106	V2110	Wireless Co...	10.41.07.0014
●	EWC1b	/World/Network Managem...	172.9.98.107	V2110	Wireless Co...	10.41.07.0014

- Ensure that the XMC and the Wireless Controllers are using the same Shared Secret to ensure a secured connection for communication. This shared secret is a default value in XMC under **Administration**→**Options**→**Wireless Manager**:

The screenshot shows the Extreme Networks management console. The 'Options' page is active for the 'Wireless Manager' section. The 'Shared Secret' option is selected, and the default shared secret is displayed as '10dmcj#ru57!wid'.

- Log into the EWC and navigate to **Controller**→**Network**→**Secure Connections**. Enter the XMC IP address, and the same shared secret found in the XMC. Then click Add/Update:

Administration

Logs

Network

L2 Ports
Network Time
Routing Protocols
Secure Connections
SNMP
Topologies
Utilities

Shared Secret for Remote Connections

Enable Weak Ciphers

Peer IP Address	Shared Secret
172.9.99.119	10dmcj,#ru57!wid

Enter XMC IP and matching shared secret.

172.9.99.119 10dmcj,#ru57!wid

Add / Update

Save

Hide Shared Secrets Remove Selected Peer

- To discover a controller, navigate to **Wireless** → **Network** → **Wireless Network** → **Controllers** → and select **Discover All Controllers** from the drop-down list.

Extreme

Dashboard Network Controllers Acce

Wireless Network

Controller ↑

Mobility Zones 172.9.98.106

Virtual Networks 172.9.98.107

Controllers

172.9.98.106

172.9.98.107

AP Groups

Manage Controllers

Discover All Controllers

Discover Controller

Refresh

Extreme Policy and Extreme Control Configuration

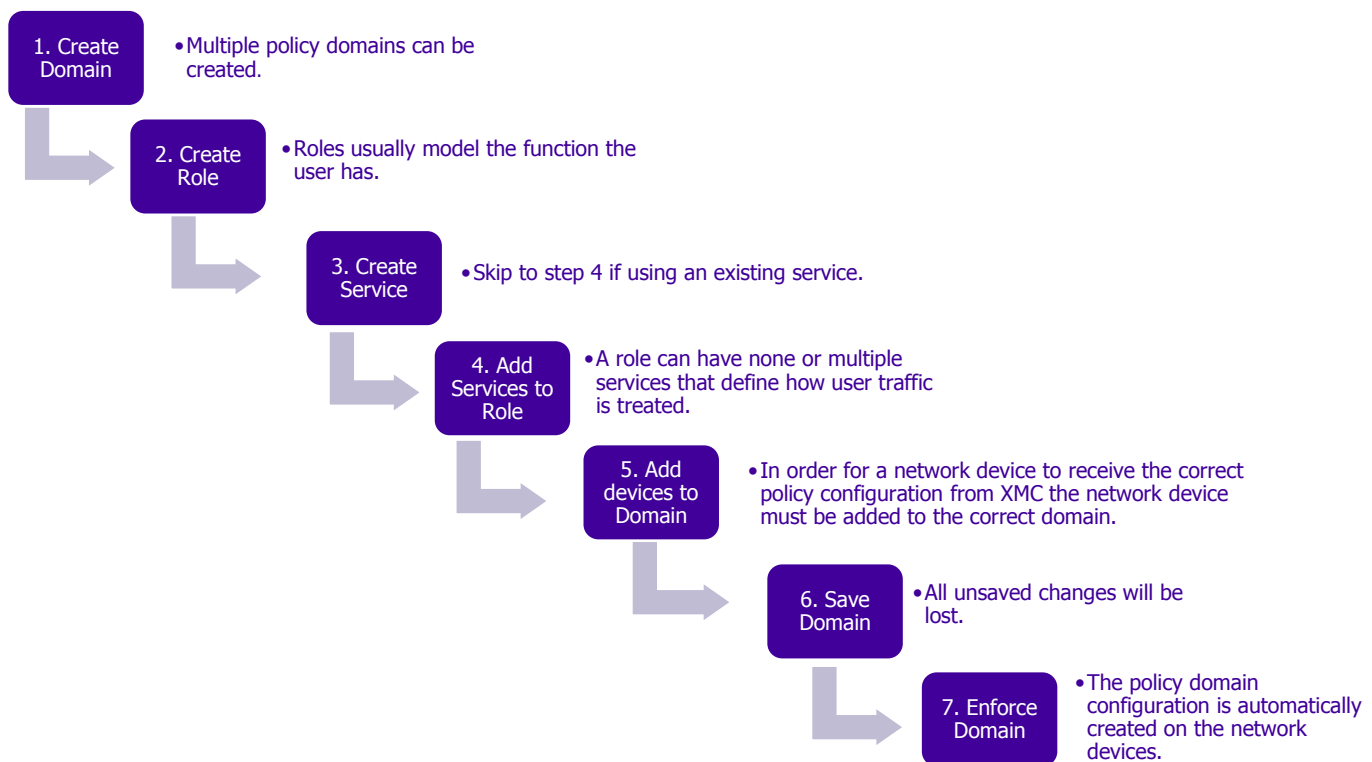
Extreme Policy

Policy provides for the configuration of role-based profiles on Summit access switches for securing and provisioning network resources based upon the role the user or device plays within the enterprise. By first defining the user or device role, network resources can be granularly tailored to a specific user, system, service, or port-based context by configuring and assigning rules to the policy role. A policy role can be configured for any combination of Class of Service, VLAN/NSI assignment, or default behavior based upon L2, L3, and L4 packet fields. Hybrid authentication allows either policy or dynamic VLAN assignment, or both, to be applied through RADIUS (Remote Authentication Dial In User Service) authorization.

Warning

Make note of the service rule limitations for each platform in the policy domain. If there is a set (or sets) of service rules common to multiple roles, this quickly multiplies the total number of rules configured. One way to avoid this is to create multiple policy domains.

The configuration flow can be reduced to the steps below:



This section assumes that SNMPv3 has been configured. To configure SNMPv3 on the switches, wireless controllers, and Extreme Management appliances, refer to the [Simple Network Management Protocol \(SNMPv3\)](#) section in **Design Considerations**.

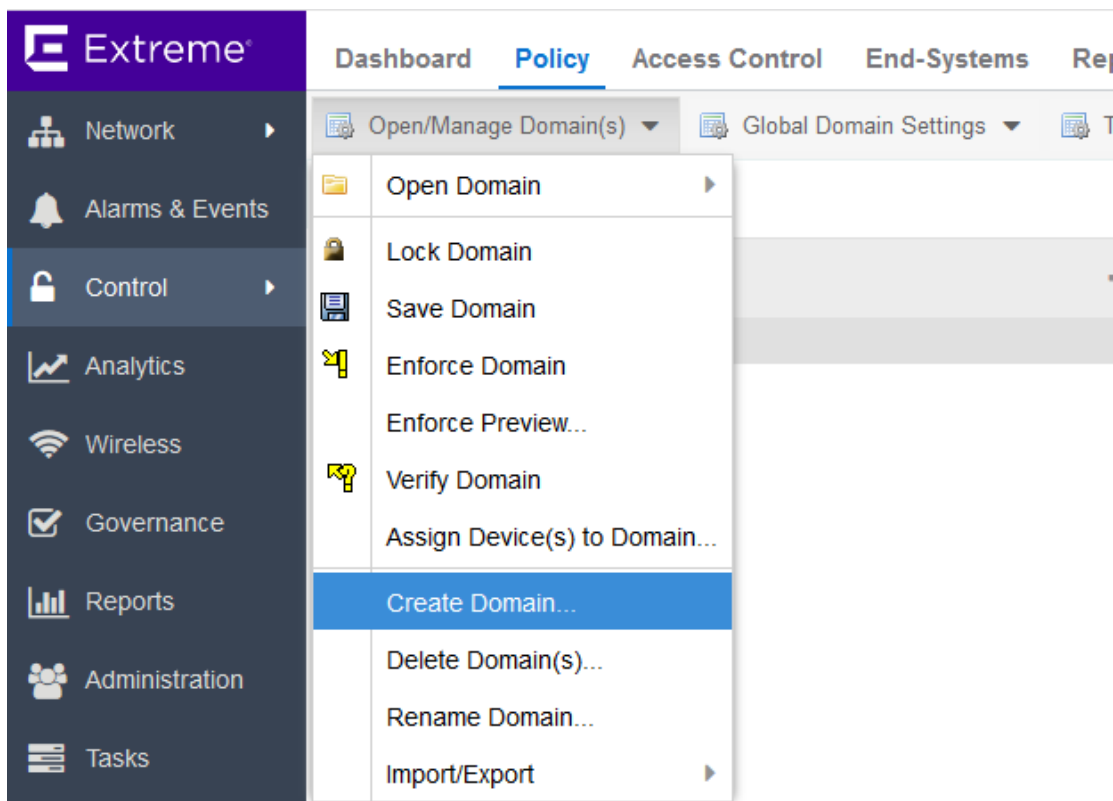
Policy Domain Configuration

The Automated Campus Validated Design contains three main domains created with Extreme Management Center, each containing a subset of associated roles and sets of rules for each role. These three domains work to organize the network in an efficient manner, allowing specific policies and rules to apply only across desired domains. The domains are:

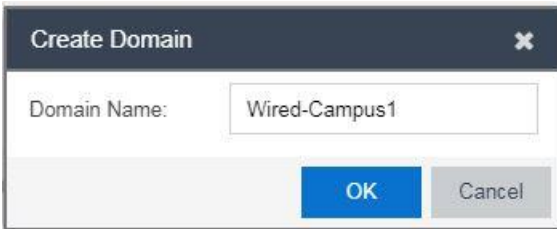
- **Wired-Campus1** (Acc120, Acc121)
- **Wired-Campus2** (Acc220, Acc221)
- **Wireless-Campus** (Wireless controllers in the server rooms, which push policies to the APs in the campuses)

The “**Wired-Campus**” domains enforce the roles and services assigned to the wired users accessing the campus Summit access switches, with each campus its own domain. The “**Wireless-Campus**” domain contains the roles and services enforced on the wireless controllers for the APs on the network.

- To create new domains, go to **Control** → **Policy** → **Open/Manage Domain(s)**. Select **Create Domain** from the drop-down list and name the new domain:



- Create the three required domains for this validated design: **Wired-Campus1**, **Wired-Campus2** and **Wireless-Campus**.



- Click **OK** to complete domain configuration.

Role Configuration – Wired-Campus1 Domain

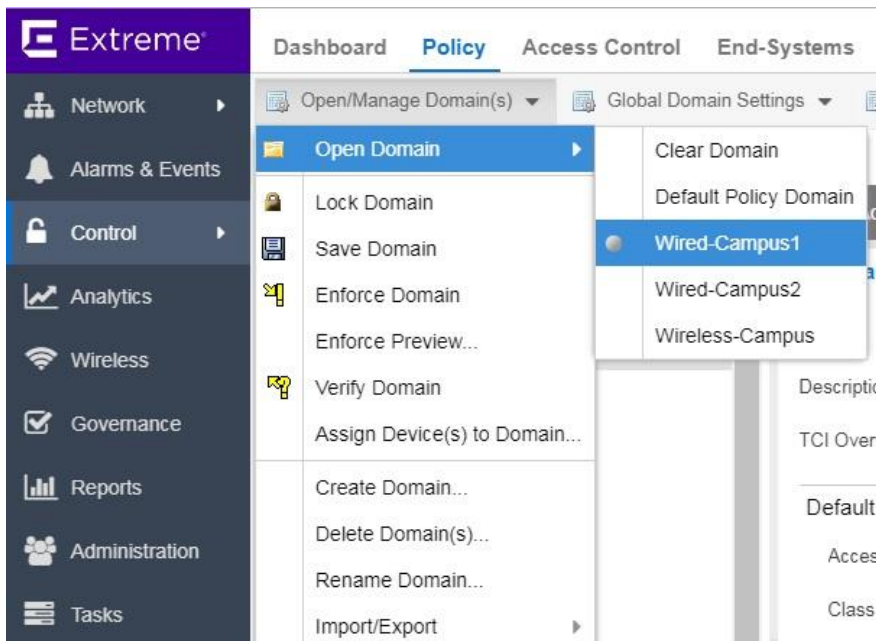
Eight unique policy roles are configured for wired campus traffic.

A role has two components that define how user traffic is treated: The Default Actions and the Services. Only the Access Control, Class of Service, and AP Aware actions are configured in the roles defined for this solution. The configuration steps for the Administrator role are presented in this section. All roles are configured in the same manner.

Note

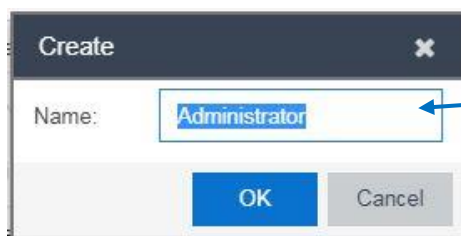
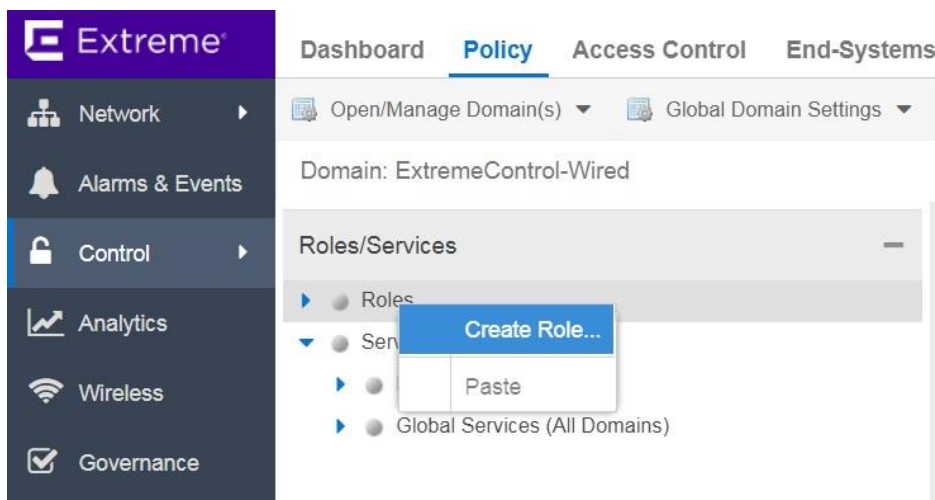
The roles illustrated in this section are examples only. Policy roles are created specifically for the needs of each network and can vary greatly.

To configure the policy roles, open the **Wired-Campus1** policy domain:



1. Administrator (VLAN 102/ NSI: 1010102)

- The Administrator role is intended for administrative users who have no limitations of services or network use. The Administrator role is important for allowing IT Administrators complete access to the network so that they can conduct the required analysis, development, and troubleshooting processes that belong to their role in the enterprise. There are no rules for this role. In addition, Class of Service (CoS) is untouched to provide administrators an unbiased network experience. If this were set to a high value, the administrator's monitoring tools may not reflect network latency accurately. If the administrators require a higher priority to ensure network access, then we recommend creating an additional Administrator role for that purpose.
- This role is used by all wired administrator users/assets across both campuses, and, other than the VLAN/Service ID mapping, is identical to the Administrator role used in the **Wired-Campus2** and **Wireless-Campus** policy domains.
- To create a new role, go to **Control** → **Policy** → **Roles/Services**, and right-click on **Roles**:



Name the role and click Ok to complete role creation.

- To configure the default actions for the Administrator role, go to **Control → Policy → Roles/Services** and select **Role**. If the options are not displayed, click **Show All**.

Role: Administrator

General VLAN Egress Mappings Port Default Usage

Name: Administrator

Description:

TCI Overwrite: Disabled

Default Actions

Access Control: Contain to VLAN

VLAN: 102[102]

Service ID: 1010102

Class of Service: None

The **Contain to VLAN** access control action is selected for the Administrator role. For this access control type, the VLAN must be specified.

Set the corresponding Service ID value for this VLAN (1010102).

- If the VLAN doesn't exist, click **New VLAN** in the drop-down, and enter VLAN name and ID:

Create VLAN

Name: 102

VID: 102 Next Available VID

OK Cancel

- To add services to the Administrator role, click **Add/Remove** and select from the existing default services. Click OK.

Role: Administrator

General VLAN Egress Mappings Port Default Usage

Name: Administrator

Description: Edit...

TCI Overwrite: Disabled

Default Actions

Access Control: Contain to VLAN

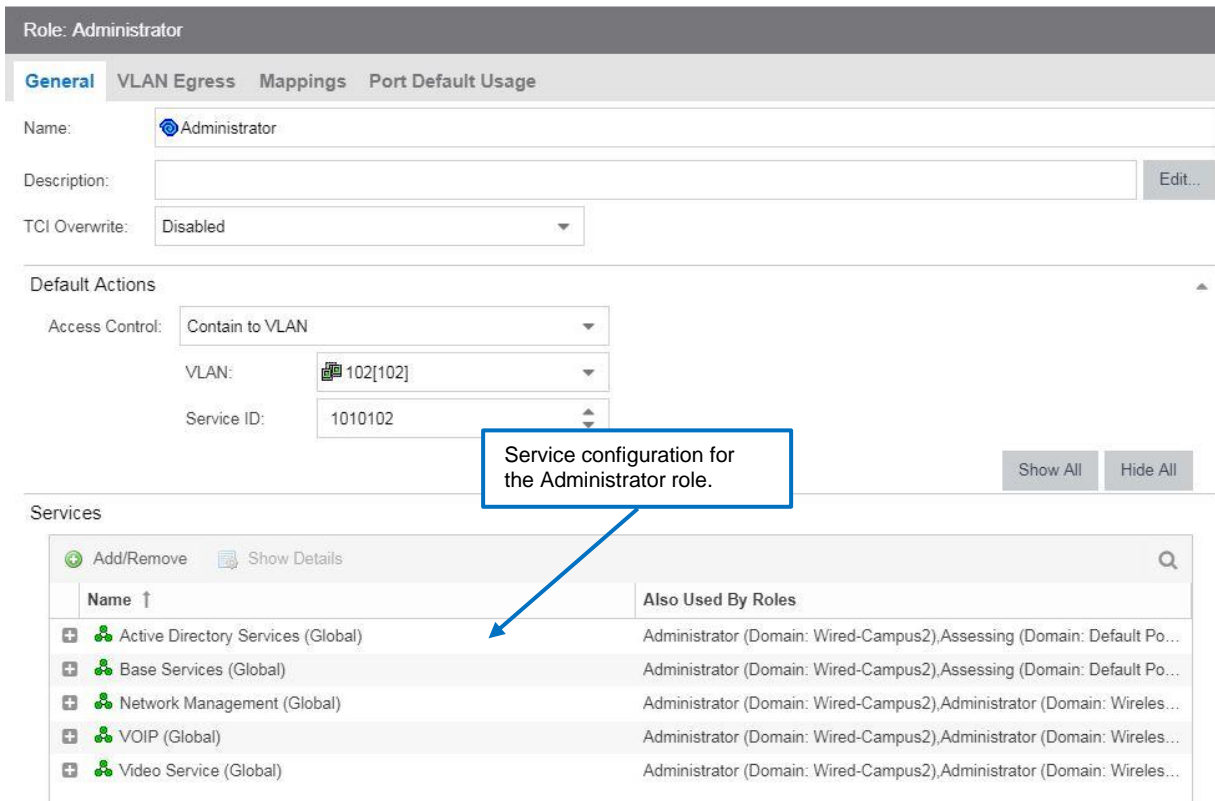
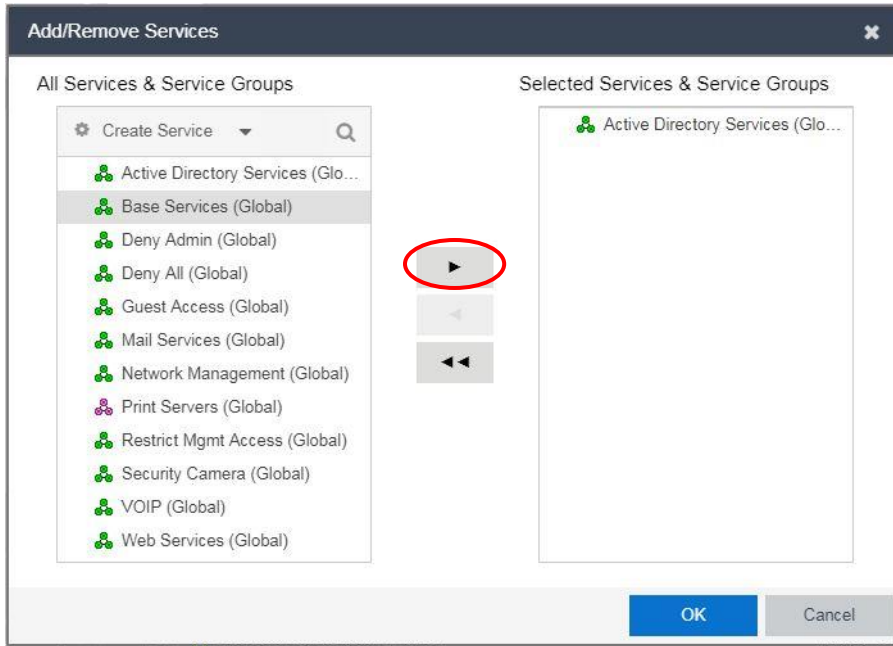
VLAN: 102[102]

Service ID: 1010102

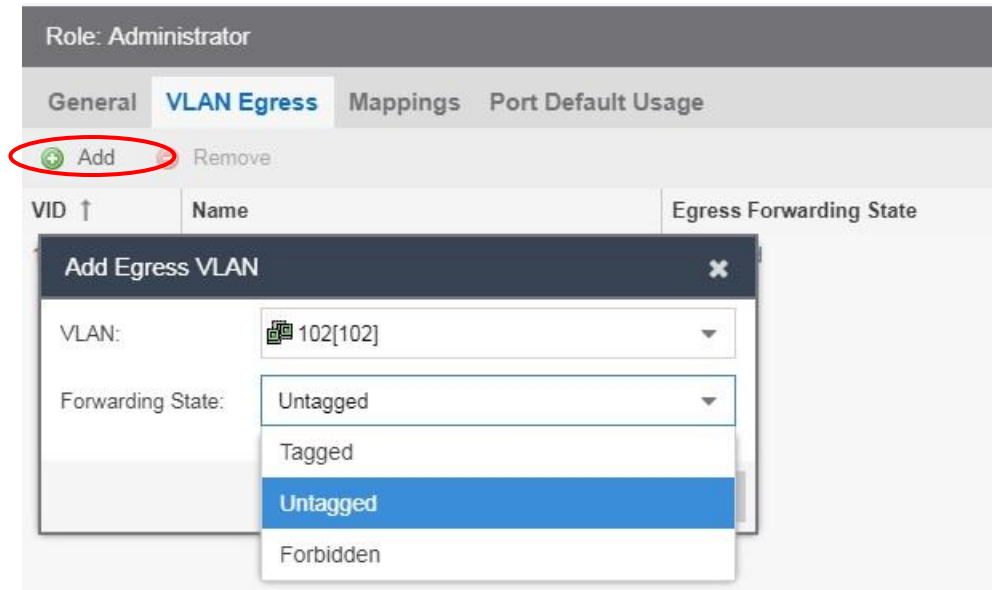
Show All Hide All

Services

Add/Remove Show Details



- The Egress VLAN must also be configured for the roles that have access control set to Contain to VLAN and for roles applied to devices that have other users connected behind them, like an AP or a VoIP phone. To configure the Egress VLAN entries, go to the VLAN Egress tab and click **Add**. Select the desired VLAN and the forwarding state for the port from the drop-down lists.



2. Access Point Role (VLAN 100/ NSI: 1010100)

- This role is applied to any port where Extreme Access Points are detected. The **AP Aware** feature allows all other MACs ingressing this port to be passed through without authentication (as the APs themselves will serve this function). This is specifically useful when bridging wireless client traffic at the AP. Although the Access Point role does not contain any associated services, it does use the Class of Service setting of High Priority. This CoS value is the highest available in the network. For Fabric Attach wireless topologies, the AP switch port is used to forward user traffic into the network. The VLANs associated with the traffic can be assigned dynamically using the VLAN Egress functionality of the role.

Note

This role is used by wired domains only and does not exist on the Wireless-Campus domain.

Role: Access Point

General | VLAN Egress | Mappings | Port Default Usage

Name:

Description: Edit...

TCl Overwrite:

Default Actions

Access Control:

VLAN:

Service ID:

Class of Service:

AP Aware:

Show All Hide All

Services

Add/Remove Show Details Q

Name ↑	Also Used By Roles

Set the VLAN id to be used for IP and FA management (100).
Set the corresponding NSI value (1010100).

Set the CoS value to High Priority for AP-EWC mgmt. traffic.

Enable AP-Aware feature.

Traffic for the AP is sent untagged on egress.

Role: Access Point

General | **VLAN Egress** | Mappings | Port Default Usage

Add Remove

VID ↑	Name	Egress Forwarding State
100	100	Untagged

3. Deny Access

- The Deny Access Role is used in ExtremeControl to assign to an end-system that has been denied access through MAC Registration. The definition of the Deny Access role may vary depending on the customer environment.

Role: Deny Access

General | VLAN Egress | Mappings | Port Default Usage

Name: Deny Access

Description: The Deny Access Role is used in Extreme Management Access Control as a role to be assigned to an end-system that has been denied access.

TCI Overwrite: Disabled

Default Actions

Access Control: **Deny Traffic**

VLAN: Disabled

Service ID: N/A

Services

Name ↑	Also Used By Roles
--------	--------------------

4. IoT Campus Role (VLAN 101/ NSI: 1010101)

- The IoT Device role represents a dedicated VLAN for IoT computing devices requiring communication with other IoT devices and systems within the campus or with other campuses.

Role: IoT Campus

General | VLAN Egress | Mappings | Port Default Usage

Name: IoT Campus

Description:

TCI Overwrite: Disabled

Default Actions

Access Control: Contain to VLAN

VLAN: **101[101]**

Service ID: 1010101

Services

Name ↑	Also Used By Roles
<input type="checkbox"/> Active Directory Services (Global)	Administrator,Administrator (Domain: Wired-Campus2),Assessing (Doma...
<input type="checkbox"/> Base Services (Global)	Administrator,Administrator (Domain: Wired-Campus2),Assessing (Doma...
<input type="checkbox"/> Deny Admin (Global)	Campus User,Campus User (Domain: Wired-Campus2),Campus User (D...
<input type="checkbox"/> Mail Services (Global)	Campus User,Campus User (Domain: Wired-Campus2),Campus User (D...
<input type="checkbox"/> Restrict Mgmt Access (Global)	Campus User,Campus User (Domain: Wired-Campus2),Campus User (D...
<input type="checkbox"/> Web Services (Global)	Campus User,Campus User (Domain: Wired-Campus2),IoT Campus (Do...

Set the corresponding NSI value for this VLAN (1010101)

Role: IoT Campus		
General VLAN Egress Mappings Port Default Usage		
➕ Add ➖ Remove		
VID ↑	Name	Egress Forwarding State
101	101	Untagged

5. Surveillance Role (VLAN 104/ NSI: 1010104)

- The Surveillance role in this design is to represent dedicated applications using multicast, such as security cameras. A Class of Service profile will be created for this role.

Role: Surveillance

General | **VLAN Egress** | Mappings | Port Default Usage

Default Actions

Access Control: Contain to VLAN

VLAN: 104[104]

Service ID: 1010104

Class of Service: None

System Log: New...

Audit Trap: None

Disable Port: Scavenger (Priority: 0)

AP Aware: Best Effort (Priority: 1)

HTTP Redirect: Bulk Data (Priority: 2)

Traffic Mirror: Critical Data (Priority: 3)

Services: Network Control (Priority: 4)

Network Management (Priority: 5)

RTP/Voice/Video (Priority: 6)

Hide Disabled | Hide All

Set the VLAN and corresponding NSI value.

Under Class of Service, choose **New**.

- Give the CoS service a name, and click OK, which will assign it to this Role:

Create ✕

Name:

- In the CoS drop-down menu, choose the gear icon next to the CoS profile created:

Role: Surveillance

General | VLAN Egress | Mappings | Port Default Usage

Default Actions

Access Control: Permit Traffic

VLAN: Disabled

Service ID: N/A

Class of Service: Surveillance Video (Priority: 7)

System Log: Best Effort (Priority: 1)

Audit Trap: Bulk Data (Priority: 2)

Disable Port: Critical Data (Priority: 3)

AP Aware: High Priority (Priority: 7)

HTTP Redirect: Network Control (Priority: 4)

Traffic Mirror: Network Management (Priority: 5)

Services: Scavenger (Priority: 0)

Surveillance Video (Priority: 7)

- Select the dot1p priority and DSCP values for this profile:

Class of Service

Name: Surveillance Video

Description:

Transmit Queue: Q9-LLQ (11Q) / Q9 (16Q) / Q7 (8Q) / Q3 (4Q)

DSCP/ToS: None

802.1p Priority: Priority 5

Drop Precedence: None

Click the box next to DSCP/ToS.

Set the priority to 5.

- Set the desired DSCP value (in this EVD, the DSCP will be AF42, DSCP 36):

DSCP/ToS Configuration

Differentiated Services Code Point (DSCP)

Well-Known Value: AF11 Assured Forwarding PHB Class 1 Low Drop Precedence [001010 / 0x0a / 10]

Raw Binary Value: AF33 Assured Forwarding PHB Class 3 High Drop Precedence [011110 / 0x1e / 30]

Type of Service (ToS)

Precedence: 0

Delay Sensitive

High Throughput

High Reliability

Explicit Congestion Notification

ToS Hex Value

Value: 0x:

Mask: 0x:

OK Cancel

AF11	Assured Forwarding PHB Class 1	Low Drop Precedence	[001010 / 0x0a / 10]
AF33	Assured Forwarding PHB Class 3	High Drop Precedence	[011110 / 0x1e / 30]
AF41	Assured Forwarding PHB Class 4	Low Drop Precedence	[100010 / 0x22 / 34]
AF42	Assured Forwarding PHB Class 4	Medium Drop Precedence	[100100 / 0x24 / 36]
AF43	Assured Forwarding PHB Class 4	High Drop Precedence	[100110 / 0x26 / 38]
CS1	Class-Selector PHB 1	Precedence 1 / Scavenger	[001000 / 0x08 / 8]
CS2	Class-Selector PHB 2	Precedence 2 / OAM	[010000 / 0x10 / 16]
CS3	Class-Selector PHB 3	Precedence 3 / Signaling	[011000 / 0x18 / 24]
CS4	Class-Selector PHB 4	Precedence 4 / Realtime	[100000 / 0x20 / 32]
CS5	Class-Selector PHB 5	Precedence 5 / Broadcast Video	[101000 / 0x28 / 40]

- Navigate back to the Surveillance role, and add any services desired:

Role: Surveillance

General | VLAN Egress | Mappings | Port Default Usage

Name:

Description: Edit...

TCI Overwrite:

Default Actions

Access Control:

VLAN:

Service ID:

Class of Service:

Show All Hide All

Services

Add/Remove Show Details Q

Name ↑	Also Used By Roles
<input type="checkbox"/> Base Services (Global)	Administrator, Administrator (Domain: Wired-Campus2), Assessing (Domain: Defa...
<input type="checkbox"/> Deny Admin (Global)	Campus User, Campus User (Domain: Wired-Campus2), IoT Campus, IoT Campu...
<input type="checkbox"/> Security Camera (Global)	Surveillance (Domain: Wired-Campus2)

- Set the VLAN Egress for this role.

Role: Surveillance

General **VLAN Egress** Mappings Port Default Usage

+ Add - Remove

VID ↑	Name	Egress Forwarding State
104	104	Untagged

Set the VLAN Egress for this role.

6. Campus User Role (VLAN 101/ NSI: 1010101)

- The Campus User role in this EVD represent any user traffic that is not Administrator or is lower priority.

Role: Campus User

General **VLAN Egress** Mappings Port Default Usage

Name:

Description:

TCI Overwrite:

Default Actions

Access Control:

VLAN:

Service ID:

Show All Hide All

Services

Name ↑	Also Used By Roles
Active Directory Services (Global)	Administrator,Administrator (Domain: Wired-Campus2),Assessing (Do...
Base Services (Global)	Administrator,Administrator (Domain: Wired-Campus2),Assessing (Do...
Deny Admin (Global)	Campus User (Domain: Wired-Campus2),Campus User (Domain: Wirel...
Mail Services (Global)	Campus User (Domain: Wired-Campus2),Campus User (Domain: Wirel...
Restrict Mgmt Access (Global)	Campus User (Domain: Wired-Campus2),Campus User (Domain: Wirel...
VOIP (Global)	Administrator,Administrator (Domain: Wired-Campus2),Administrator (...)
Video Service (Global)	Administrator,Administrator (Domain: Wired-Campus2),Administrator (...)
Web Services (Global)	Campus User (Domain: Wired-Campus2),IoT_Campus.IoT_Campus (D...

Set the VLAN and corresponding NSI value.

Role: Campus User

General **VLAN Egress** Mappings Port Default Usage

+ Add - Remove

VID ↑	Name	Egress Forwarding State
103	103	Untagged

7. Printer Role (VLAN 101/ NSI: 1010101)

- The Printer Role is simply used to define a subset of services that should be applied to any related printer devices on the network.

Role: Printer

General | VLAN Egress | Mappings | Port Default Usage

Name:

Description:

TCI Overwrite:

Default Actions

Access Control:

VLAN:

Service ID:

Services

Name ↑	Also Used By Roles
Base Services (Global)	Administrator, Administrator (Domain: Wired-Campus2), Campus User, Campus User (Domain: Wir...
Print Servers (Global)	Printer (Domain: Wired-Campus2), Printer (Domain: Wireless-Campus)

Printers are contained to the Campus User VLAN and assigned the same NSI.

Services defined for this role.

- The “Print Servers” service is predefined under Services. Under Network Resources, Print Servers can be selected and edited, specifying the MAC or IP addresses of the servers in the network to be included in this service and applied to this role.

Roles/Services

- Global Services (All Domains)
 - Service Groups
 - Services
 - Print Servers
 - Active Directory Services
 - Base Services

Class of Service +

VLANs +

Network Resources +

Devices/Port Groups +

Enforce Auto Collapse Panel

Rule: Print Servers

Service Name:

Description:

TCI Overwrite:

Traffic Description

Type:

Network Resource Type:

Network Resources:

Actions

Access Control:

Class of Service:

System Log:

Clicking the “gear” in the drop-down next to this option allows for specifying server MAC/IP addresses to include.

Role: Printer

General **VLAN Egress** Mappings Port Default Usage

VID ↑	Name	Egress Forwarding State
103	103	Untagged

Printer traffic is sent as untagged on egress.

8. Wired IoT Bridged Role (Legacy IoT - VLAN 907/ NSI: 1090907)

- This role is applied to devices that may not support newer authentication methods, network addressing, etc, and require a Layer 2 connection across the fabric to its corresponding server. When a client authenticates to this role, the access switch (FA client) will request this VLAN/NSI value and is created dynamically on the FA Server as an L2VSN.

Role: Wired IoT Bridged

General **VLAN Egress** Mappings Port Default Usage

Name:

Description:

TCI Overwrite:

Default Actions

Access Control:

VLAN:

Service ID:

VLAN and NSI value

Services

Name ↑	Also Used By Roles
Base Services (Global)	Administrator, Administrator (Domain: Wired-Campus2), Campus User, Campus User (Domain: Wir...
Deny Admin (Global)	Administrator, Campus User, Campus User (Domain: Wired-Campus2), IoT Campus, IoT Campus (...)

Role: Wired IoT Bridged

General **VLAN Egress** Mappings Port Default Usage

VID ↑	Name	Egress Forwarding State
907	907	Untagged

9. The final list of Policy Roles for Wired-Campus1:

Domain: Wired-Campus1

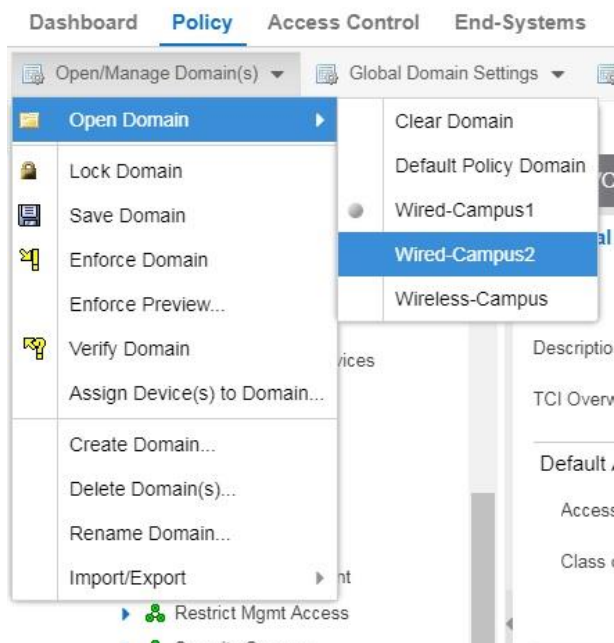
Role / Service / Rule ↑	Summary
Access Point	[100 [100] (SVC ID:1010100)/High Priority/AP Aware] [Egress: (Untag:100)]
Administrator	[102 [102] (SVC ID:1010102)] [Egress: (Untag:102)]
Campus User	[103 [103] (SVC ID:1010103)] [Egress: (Untag:103)]
Deny Access	[Deny Traffic]
IoT Campus	[101 [101] (SVC ID:1010101)] [Egress: (Untag:101)]
Printer	[103 [103] (SVC ID:1010103)] [Egress: (Untag:103)]
Surveillance	[104 [104] (SVC ID:1010104)/RTP/Voice/Video] [Egress: (Untag:104)]
Wired IoT Bridged	[907 [907] (SVC ID:1090907)] [Egress: (Untag:907)]

10. Save the policy domain and enforce to the access switches in this domain.

Role Configuration – Wired-Campus2 Domain

Although the role names between the wired campuses are the same, the actual VLAN and NSI values are different and will be applied based on the policy domain the access switch is a member of.

Create the same roles as was in Wired-Campus1, editing the roles that require different network parameters. To configure the roles, open the **Wired-Campus2** policy domain:



1. Administrator Role

The Administrator role in Campus 2 uses VLAN 202/ NSI: 1020202.

Role: Administrator

General | VLAN Egress | Mappings | Port Default Usage

Name:

Description: Edit...

TCI Overwrite:

Default Actions

Access Control:

VLAN:

Service ID:

Show All Hide All

Services

Add/Remove Show Details		
Name ↑		Also Used By Roles
<input type="checkbox"/> Active Directory Services (Global)		Administrator (Domain: Wired-Campus1),Assessing (Domain: Default Po...
<input type="checkbox"/> Base Services (Global)		Administrator (Domain: Wired-Campus1),Assessing (Domain: Default Po...
<input type="checkbox"/> Network Management (Global)		Administrator (Domain: Wired-Campus1),Administrator (Domain: Wireles...
<input type="checkbox"/> VOIP (Global)		Administrator (Domain: Wired-Campus1),Administrator (Domain: Wireles...
<input type="checkbox"/> Video Service (Global)		Administrator (Domain: Wired-Campus1),Administrator (Domain: Wireles...

Role: Administrator

General | **VLAN Egress** | Mappings | Port Default Usage

Add Remove

VID ↑	Name	Egress Forwarding State
202	202	Untagged

2. Access Point Role (VLAN: 200 / NSI: 1020200)

Role: Access Point

General | VLAN Egress | Mappings | Port Default Usage

Name:

Description: [Edit...](#)

TCI Overwrite:

Default Actions

Access Control:

VLAN:

Service ID:

Class of Service:

AP Aware:

[Show All](#) [Hide All](#)

3. Deny Access Role

The Deny Access Role is identical between the policy domains.

Role: Deny Access

General | VLAN Egress | Mappings | Port Default Usage

Name:

Description: [Edit...](#)

TCI Overwrite:

Default Actions

Access Control:

VLAN:

Service ID:

[Show All](#) [Hide All](#)

Services

[Add/Remove](#) [Show Details](#)

Name ↑	Also Used By Roles

4. IoT Campus Role (VLAN: 201 / NSI: 1020201)

Role: IoT Campus

General | VLAN Egress | Mappings | Port Default Usage

Name:

Description: [Edit...](#)

TCI Overwrite:

Default Actions ▲

Access Control:

VLAN:

Service ID:

[Show All](#) [Hide All](#)

Services

Add/Remove Show Details		Q
Name ↑	Also Used By Roles	
+ Active Directory Services (Global)	Administrator, Administrator (Domain: Wired-Campus1), Assessing (Doma...	
+ Base Services (Global)	Administrator, Administrator (Domain: Wired-Campus1), Assessing (Doma...	
+ Deny Admin (Global)	Campus User, Campus User (Domain: Wired-Campus1), Campus User (D...	
+ Mail Services (Global)	Campus User, Campus User (Domain: Wired-Campus1), Campus User (D...	
+ Restrict Mgmt Access (Global)	Campus User, Campus User (Domain: Wired-Campus1), Campus User (D...	
+ Web Services (Global)	Campus User, Campus User (Domain: Wired-Campus1), IoT Campus (Do...	

Role: IoT Campus

General | **VLAN Egress** | Mappings | Port Default Usage

[+](#) Add [-](#) Remove

VID ↑	Name	Egress Forwarding State
201	201	Untagged

5. Surveillance Role (VLAN: 204 / NSI: 1020204)

- The Surveillance role in Campus 2 will be configured in the same manner as Campus 1, with the creation of a Class of Service for this role.

Role: Surveillance

General VLAN Egress Mappings Port Default Usage

Name: Surveillance

Description:

TCI Overwrite: Disabled

Default Actions

Access Control: Contain to VLAN

VLAN: 204[204]

Service ID: 1020204

Class of Service: None

System Log: New...

Audit Trap: None

Disable Port: Scavenger (Priority: 0)

AP Aware: Best Effort (Priority: 1)

HTTP Redirect: Bulk Data (Priority: 2)

Traffic Mirror: Critical Data (Priority: 3)

Services: Network Control (Priority: 4)

Network Management (Priority: 5)

RTP/Voice/Video (Priority: 6)

Hide Disabled

Set the VLAN and corresponding NSI value.

Under Class of Service, choose **New**.

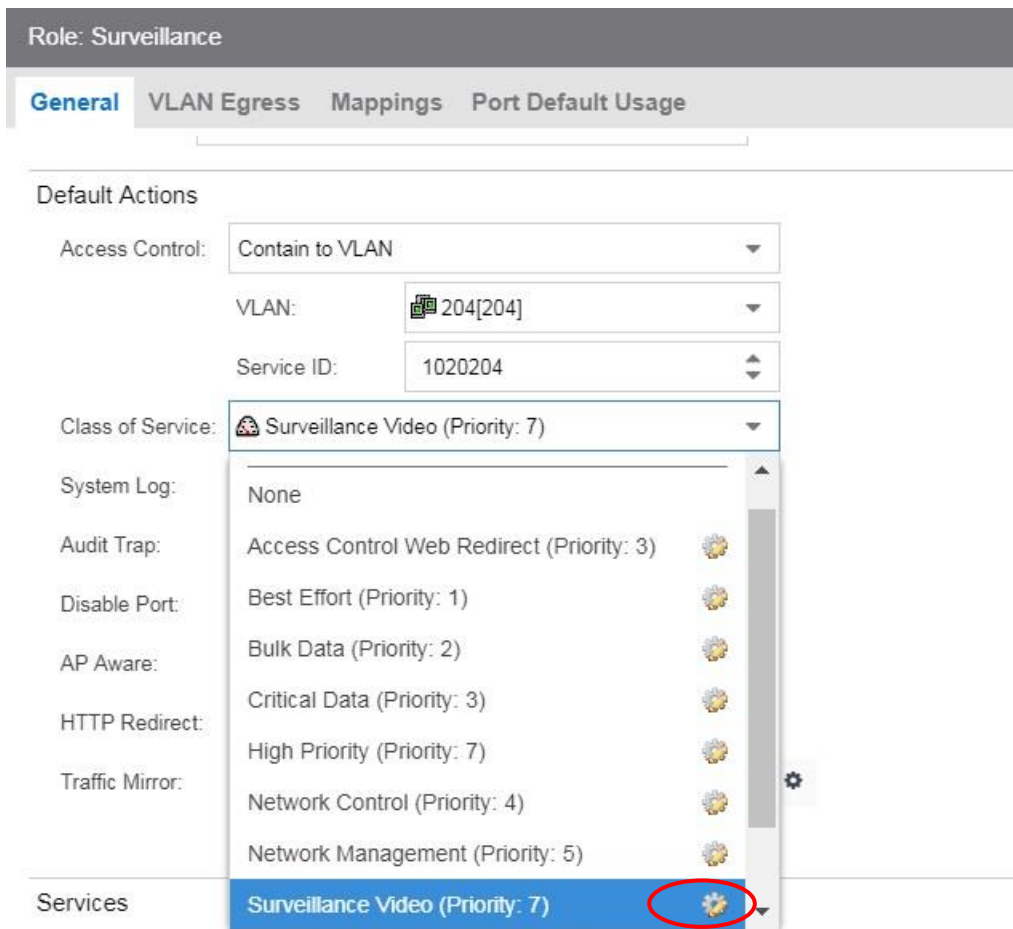
- Give the CoS service a name, and click OK, which will assign it to this Role:

Create

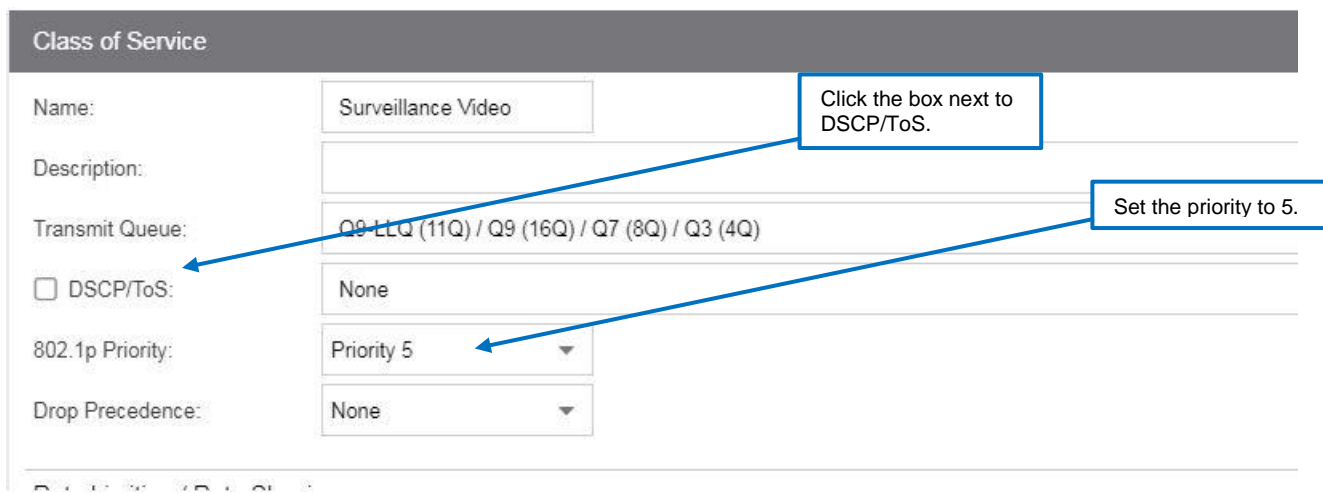
Name: Surveillance Video

OK Cancel

- In the CoS drop-down menu, choose the gear icon next to the CoS profile created:



- Select the dot1p priority and DSCP values for this profile:



- Set the desired DSCP value (in this EVD, the DSCP will be AF42, DSCP 36):

DSCP/ToS Configuration

Differentiated Services Code Point (DSCP)

Well-Known Value: AF11 Assured Forwarding PHB Class 1 Low Drop Precedence [001010 / 0x0a / 10]

Raw Binary Value: AF33 Assured Forwarding PHB Class 3 High Drop Precedence [011110 / 0x1e / 30]

Type of Service (ToS): AF41 Assured Forwarding PHB Class 4 Low Drop Precedence [100010 / 0x22 / 34]

AF42 Assured Forwarding PHB Class 4 Medium Drop Precedence [100100 / 0x24 / 36]

AF43 Assured Forwarding PHB Class 4 High Drop Precedence [100110 / 0x26 / 38]

Precedence: 0

Delay Sensitive

High Throughput

High Reliability

Explicit Congestion Notification

ToS Hex Value

Value: 0x:

Mask: 0x:

- Navigate back to the Surveillance role, and add any services desired:

Role: Surveillance

General | VLAN Egress | Mappings | Port Default Usage

Name:

Description:

TCl Overwrite:

Default Actions

Access Control:

VLAN:

Service ID:

Class of Service:

Services

Name ↑	Also Used By Roles
<input type="checkbox"/> Base Services (Global)	Administrator, Administrator (Domain: Wired-Campus1), Assessing (Domain: Defa...
<input type="checkbox"/> Deny Admin (Global)	Campus User, Campus User (Domain: Wired-Campus1), IoT Campus, IoT Campu...
<input type="checkbox"/> Security Camera (Global)	Surveillance (Domain: Wired-Campus1)

Service configuration for the Surveillance role.

- Set the VLAN Egress for this role.

Role: Surveillance

General **VLAN Egress** Mappings Port Default Usage

+ Add - Remove

VID ↑	Name	Egress Forwarding State
204	204	Untagged

Set the VLAN Egress for this role.

6. Campus User Role (VLAN: 203 / NSI: 1020203)

Role: Campus User

General **VLAN Egress** Mappings Port Default Usage

Name:

Description:

TCI Overwrite:

Default Actions

Access Control:

VLAN:

Service ID:

Services

Name ↑	Also Used By Roles
+ Active Directory Services (Global)	Administrator,Administrator (Domain: Wired-Campus1),Assessing (Do...
+ Base Services (Global)	Administrator,Administrator (Domain: Wired-Campus1),Assessing (Do...
+ Deny Admin (Global)	Campus User (Domain: Wired-Campus1),Campus User (Domain: Wirel...
+ Mail Services (Global)	Campus User (Domain: Wired-Campus1),Campus User (Domain: Wirel...
+ Restrict Mgmt Access (Global)	Campus User (Domain: Wired-Campus1),Campus User (Domain: Wirel...
+ VOIP (Global)	Administrator,Administrator (Domain: Wired-Campus1),Administrator (...)
+ Video Service (Global)	Administrator,Administrator (Domain: Wired-Campus1),Administrator (...)
+ Web Services (Global)	Campus User (Domain: Wired-Campus1),IoT Campus.IoT Campus (D...

Role: Campus User

General **VLAN Egress** Mappings Port Default Usage

+ Add - Remove

VID ↑	Name	Egress Forwarding State
203	203	Untagged

7. Printer Role (VLAN: 203 / NSI: 1020203)

Role: Printer

General | VLAN Egress | Mappings | Port Default Usage

Name:

Description: Edit...

TCI Overwrite:

Default Actions

Access Control:

VLAN:

Service ID:

Show All Hide All

Services

+ Add/Remove Show Details Q

Name ↑	Also Used By Roles
+ Base Services (Global)	Administrator, Administrator (Domain: Wired-Campus1), Campus User, Campus User (Domain: Wir...
+ Print Servers (Global)	Printer (Domain: Wired-Campus1), Printer (Domain: Wireless-Campus)

Role: Printer

General | **VLAN Egress** | Mappings | Port Default Usage

+ Add - Remove

VID ↑	Name	Egress Forwarding State
203	203	Untagged

8. Wired IoT Bridged Role (VLAN: 907 / NSI: 1090907)

This role is applied to devices that may not support newer authentication methods, network addressing, etc, and require a Layer 2 connection across the fabric to its corresponding server. When a client authenticates to this role, the access switch (FA client) will request this VLAN/NSI value and is created dynamically on the FA Server as an L2VSN.

Role: Wired IoT Bridged

General
VLAN Egress
Mappings
Port Default Usage

Name:

Description: Edit...

TCI Overwrite:

Default Actions

Access Control:

VLAN:

Service ID:

Show All Hide All

Services

Add/Remove
Show Details
Q

Name ↑	Also Used By Roles
Base Services (Global)	Administrator, Administrator (Domain: Wired-Campus1), Campus User, Campus User (Domain: Wir...
Deny Admin (Global)	Administrator (Domain: Wired-Campus1), Campus User, Campus User (Domain: Wired-Campus1)...

Role: Wired IoT Bridged

General
VLAN Egress
Mappings
Port Default Usage

+ Add
 - Remove

VID ↑	Name	Egress Forwarding State
907	907	Untagged

9. The final list of Policy roles for Wired-Campus2:

Domain: Wired-Campus2

Roles/Services

- Roles
- Access Point
- Administrator
- Campus User
- Deny Access
- IoT Campus
- Printer
- Surveillance
- Wired IoT Bridged
- Service Repository

Show Editable Columns Collapse All

Role / Service / Rule ↑	Summary
Access Point	[200 [200] (SVC ID:1020200)/High Priority/AP Aware] [Egress: (Tag:200)]
Administrator	[202 [202] (SVC ID:1020202)] [Egress: (Untag:202)]
Campus User	[203 [203] (SVC ID:1020203)] [Egress: (Untag:203)]
Deny Access	[Deny Traffic]
IoT Campus	[201 [201] (SVC ID:1020201)] [Egress: (Untag:201)]
Printer	[203 [203] (SVC ID:1020203)] [Egress: (Untag:203)]
Surveillance	[204 [204] (SVC ID:1020204)/RTP/Voice/Video] [Egress: (Untag:204)]
Wired IoT Bridged	[907 [907] (SVC ID:1090907)] [Egress: (Untag:907)]

10. Save the Policy Domain and enforce to the access switches in this domain.

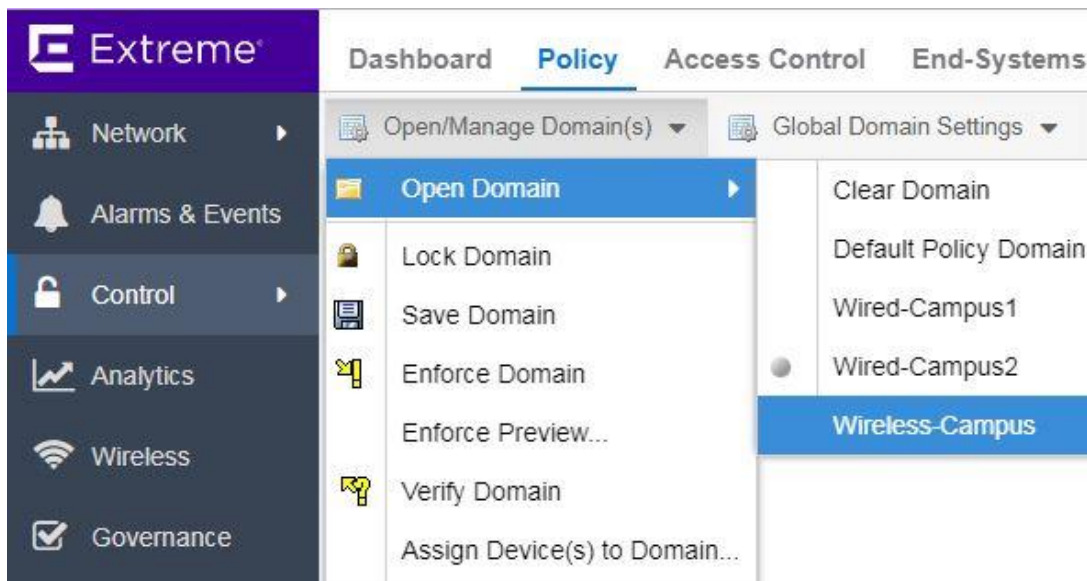
Role Configuration – Wireless Domains

As the two wireless controllers in this EVD are redundant, there will be one wireless domain covering both campuses. Therefore, roles for both campuses will be created in this domain. The roles and services created on the wireless domain are enforced on the wireless controllers, and subsequently pushed to the Access Points.

Many of the roles defined in the Wireless-Campus policy domain are identical in purpose and configuration to their wired version, however wireless networks are kept on a different vlan from the wired. This is done to better allocate the number of supported rules per platform, as well as protecting the wireless network from unnecessary broadcast/multicast traffic.

To allow for wireless roaming between the campuses, the wireless networks have been configured as part of the Fabric Connect DVR domain spanning both campuses, so the same wireless VLAN and subnet is used in both locations.

The roles configured for wireless networks are configured in the same way as for wired networks. To configure the roles, open the Wireless-Campus policy domain:



1. Administrator Role (VLAN: 1050 / NSI: 1501050)

- The wireless Administrator role serves the same function as the wired Admin role.

Role: Administrator

General | VLAN Egress | Mappings | Port Default Usage

Name:

Description: Edit...

TCI Overwrite:

Default Actions

Access Control:

VLAN:

Service ID:

Show All Hide All

Services

+ Add/Remove + Show Details 🔍

Name ↑	Also Used By Roles
+ Active Directory Services (Global)	Administrator (Domain: Wired-Campus1), Administrator (Domain: Wired-Campus2), Asse...
+ Base Services (Global)	Administrator (Domain: Wired-Campus1), Administrator (Domain: Wired-Campus2), Cam...
+ Network Management (Global)	Administrator (Domain: Wired-Campus2)
+ VOIP (Global)	Administrator (Domain: Wired-Campus1), Administrator (Domain: Wired-Campus2), Cam...
+ Video Service (Global)	Administrator (Domain: Wired-Campus1), Campus User (Domain: Wired-Campus1), Cam...

2. Deny Access Role (Deny Access)

- The Deny Access role is used in Wireless-Campus as a role to be assigned to an end-system that has been denied access through failed authentication. The definition of the Deny Access role may vary depending on the customer environment.

Role: Deny Access

General | VLAN Egress | Mappings | Port Default Usage

Name:

Description: Edit...

TCI Overwrite:

Default Actions

Access Control:

VLAN:

Service ID:

Show All Hide All

Services

+ Add/Remove + Show Details 🔍

Name ↑	Also Used By Roles
--------	--------------------

3. Guest Access Role (Guest-Access)

- The Guest Access role is intended for guests or other unknown users connecting to the enterprise network infrastructure. The Guest Access role will be used to enforce the high security of IT assets and the limited availability of IT resources as determined by the business policy. No VLAN/NSI value is required for Guest, as this traffic will be tunneled directly back to the EWC, based on the topology mode.

Role: Guest-Access

General | VLAN Egress | Mappings | Port Default Usage

Name:

Description:

TCI Overwrite:

Default Actions

Access Control:

VLAN:

Service ID:

Show All Hide All

Services

Add/Remove Show Details

Name ↑	Also Used By Roles
Base Services	Campus User, Deny Access, IoT Campus, Printer, Unregistered
Guest Access (Global)	

All traffic except for traffic allowed by the service configuration is dropped.

4. IoT Campus (VLAN: 1052 / NSI: 1501052)

- The IoT Device role represents a dedicated wireless VLAN for IoT computing devices requiring communication with other IoT devices and systems within the campus or with other campuses. The VLANs associated with the traffic can be assigned dynamically using the VLAN Egress functionality of the role.

Role: IoT Campus

General | VLAN Egress | Mappings | Port Default Usage

Name: IoT Campus

Description: Edit...

TCI Overwrite: Disabled

Default Actions

Access Control: Contain to VLAN

VLAN: 1052[1052]

Service ID: 1501052

Show All Hide All

Services

Add/Remove Show Details

Name ↑	Also Used By Roles
+ Active Directory Services	Campus User,Deny Access,Unregistered
+ Base Services	Campus User,Deny Access,Guest-Access,Printer,Unregistered
+ Deny Admin	Campus User
+ Mail Services	Campus User
+ Web Services	Campus User

5. Campus User (VLAN id: 1051 / NSI: 1501051):

- The wireless Campus User role serves the same function as the wired Campus role.

Role: Campus User

General | VLAN Egress | Mappings | Port Default Usage

Name: Campus User

Description: Edit...

TCI Overwrite: Disabled

Default Actions

Access Control: Contain to VLAN

VLAN: 1051[1051]

Service ID: 1501051

Show All Hide All

Services

Add/Remove Show Details

Name ↑	Also Used By Roles
+ Active Directory Services (Global)	Administrator,Administrator (Domain: Wired-Campus1),Administrator (Domain: Wir...
+ Base Services (Global)	Administrator,Administrator (Domain: Wired-Campus1),Administrator (Domain: Wir...
+ Deny Admin (Global)	Administrator (Domain: Wired-Campus1),Campus User (Domain: Wired-Campus1)...
+ Mail Services (Global)	Administrator (Domain: Wired-Campus2),Campus User (Domain: Wired-Campus1)...
+ Web Services (Global)	Administrator (Domain: Wired-Campus2),Campus User (Domain: Wired-Campus1)...

6. Unregistered Role

- The Unregistered Role is used in the Wireless-Campus policy domain for end-systems that have joined the Guest wireless network and have yet to pass through authentication or guest registration. The definition of the Unregistered role may vary depending on the customer environment.

Role: Unregistered

General | VLAN Egress | Mappings | Port Default Usage

Name: Unregistered

Description: The Unregistered Role is used in Extreme Management Access Control as a role to be assigned to an end...

TCI Overwrite: Disabled

Default Actions

Access Control: Deny Traffic | VLAN: Disabled

Services

Name ↑	Also Used By Roles
Base Services (Global)	AdminCampus,Deny Access,Failsafe,Guest-Access,IoT Campus,NonAdmin-C1,N...
Redirect Web Services	Deny Access,Quarantine

All traffic except for traffic allowed by the service configuration is dropped.

Redirect function is enabled for this role and it will be used for captive portal guest access.

7. The final list for policy roles from the Wireless-Campus domain:

Domain: Wireless-Campus

Roles/Services

Roles

- Administrator
- Campus User
- Deny Access
- Guest-Access
- IoT Campus
- Unregistered

Service Repository

Role / Service / Rule ↑	Summary
Administrator	[1050 [1050] (SVC ID:1501050)]
Campus User	[1051 [1051] (SVC ID:1501051)]
Deny Access	[Deny Traffic]
Guest-Access	[Deny Traffic]
IoT Campus	[1052 [1052] (SVC ID:1501052)]
Unregistered	[Deny Traffic]

Services Configurations

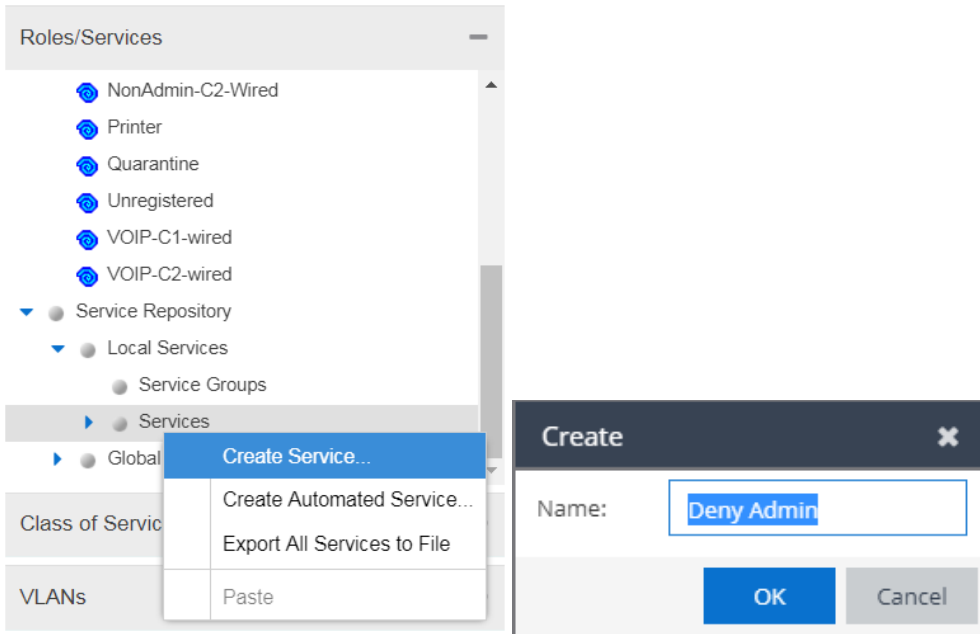
Extreme Management Center provides a set of default services that cover a wide range of protocols and applications. Custom services can be added to match specific requirements, and rules can be added to the existing services. Creating a global role means it is visible and it can be used by all policy domains.

The following non-default services were added for Campus 1. Detailed configuration steps are added for the Deny Admin service. All services are configured in the same manner.

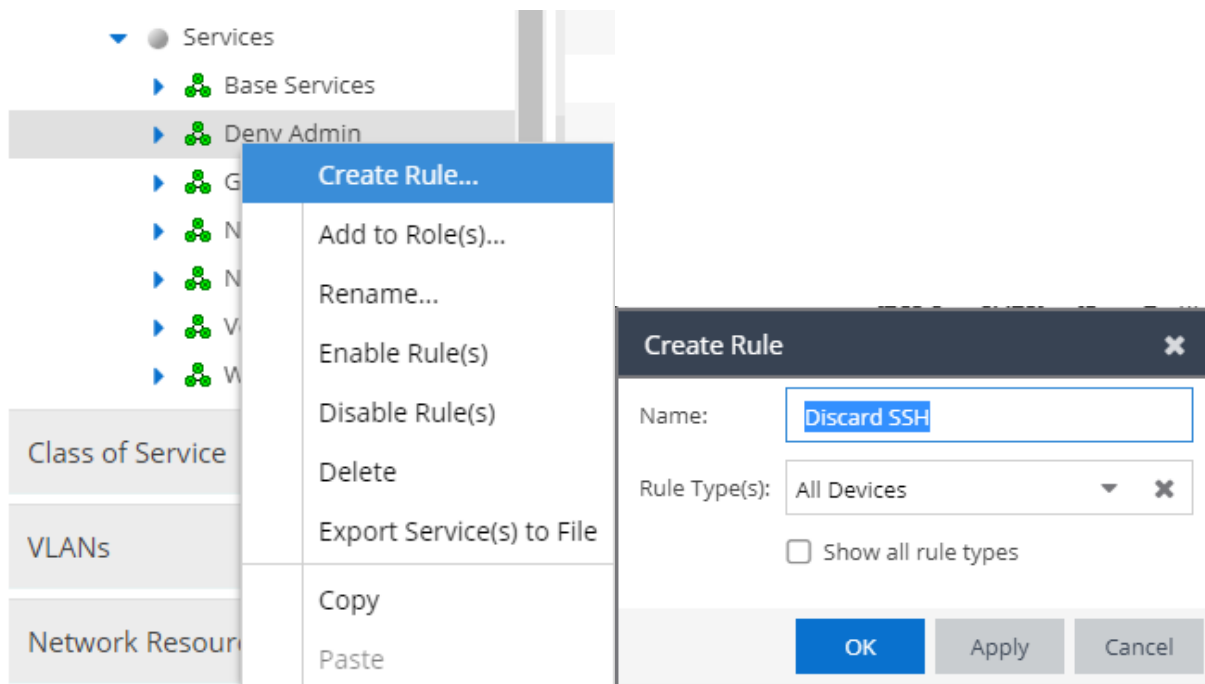
1. Deny Admin Service

The purpose of this service is to deny all management traffic and applications and it is applied to all roles that are not Administrator.

- New services can be added from **Policy tab → Roles/Services → Service Repository → Local Services**, right click on **Services** and select **Create Service**:



- Each service is formed of one or more rules. To add a rule to a service, right click on the service name and select **Create Rule**.



- Once created, the rule will appear under the service. To configure the rule, click on its name to open the configuration panel.

The image shows a configuration page for a rule named "Discard SSH". The page is divided into several sections:

- Header:** "Rule: Discard SSH"
- Service Name:** "Deny Admin"
- Description:** (Empty text field)
- Rule Status:** "Enabled" (dropdown menu)
- Rule Type:** "All Devices" (dropdown menu) with a checkbox "Show all rule types".
- TCl Overwrite:** "Disabled" (dropdown menu)
- Traffic Description:**
 - Type: "IP TCP Port Bilateral" (dropdown menu)
 - Value: "SSH" (text field)
 - Buttons: "Remove", "Edit..."
- Actions:**
 - Access Control: "Deny Traffic" (dropdown menu)
 - Class of Service: "None" (dropdown menu)
 - System Log: "Disabled" (dropdown menu)
 - Audit Trap: "Disabled" (dropdown menu)
 - Disable Port: "Disabled" (dropdown menu)
 - HTTP Redirect: "Disabled" (dropdown menu)
 - Traffic Mirror: "Disabled" (dropdown menu) with checkbox "Mirror First 15 Packets"
 - Quarantine Role: "Disabled" (dropdown menu)
 - Contain to VLAN: "Disabled" (dropdown menu)

Callouts in the main screenshot:

- "Enable Rule for settings to take effect." (points to Rule Status)
- "Click Edit to define the type of traffic the rule will affect." (points to Edit... button)
- "Define the actions that will be taken when the user traffic matches the definition in the Traffic Description section." (points to Contain to VLAN)

The "Edit Traffic Description" dialog box is open, showing:

- Traffic Classification Layer: "All Layers" (dropdown menu)
- Traffic Classification Type: "IP TCP Port Bilateral" (dropdown menu)
- Traffic Classification Value:
 - Well-Known Value: "SSH (22)" (radio button selected, dropdown menu)
 - Single Value: "22" (text field)
 - Range: Start Value: (text field), End Value: (text field)
- Traffic Classification Optional Value:
 - Value: (text field)
- Buttons: "OK", "Cancel"

Callouts in the dialog box:

- "Select Traffic Classification layer and Type." (points to Layer and Type dropdowns)
- "Select Traffic Classification Value." (points to Well-Known Value dropdown)

- The Deny Admin service has the following rules defined. In addition to specific applications being blocked, entire subnets can also be denied access:

Rule ↑	Summary
Deny Storage Test network	[IPDST : 172.90.4.0/24] -> [Deny Traffic]
Deny Storage network	[IPDST : 172.90.3.0/24] -> [Deny Traffic]
Deny Test network	[IPDST : 172.90.2.0/24] -> [Deny Traffic]
Discard SSH	[TCP Bil : SSH] -> [Deny Traffic]
Discard Src 443	[TCP Src : HTTPS]
Discard TCP Src 20 - FTP Data	[TCP Src : FTP Data] -> [Deny Traffic]
Discard TCP Src 21 - FTP	[TCP Src : FTP Data] -> [Deny Traffic]
Discard TCP Src 25 - SMTP	[TCP Src : SMTP] -> [Deny Traffic]
Discard TCP Src 53 - DNS	[TCP Src : DNS] -> [Deny Traffic]
Discard TCP Src 80 - HTTP	[TCP Src : HTTP] -> [Deny Traffic]
Discard TCP Src SQL Server	[TCP Src : 1433] -> [Deny Traffic]
Discard Telnet	[TCP Src : Telnet] -> [Deny Traffic]
Discard UDP 161 - SNMP	[TCP Bil : SNMP] -> [Deny Traffic]
Discard UDP 162 - SNMP Traps	[TCP Bil : 162] -> [Deny Traffic]
Discard UDP 53 - DNS Imposters	[UDP Src : DNS] -> [Deny Traffic]
Discard UDP 69 - TFTP	[TCP Bil : TFTP] -> [Deny Traffic]
Discard UDP Src 1812 - Radius	[UDP Src : RADIUS] -> [Deny Traffic]
Discard UDP Src 1813 Radius Acct	[UDP Src : RADIUS Accounting] -> [Deny Traffic]
Discard UDP Src 67 - Bootps	[UDP Src : BootP Server] -> [Deny Traffic]
Discard UDP Src SQL Server	[UDP Src : 1433] -> [Deny Traffic]

2. Guest Access Service

- This service was created to allow DHCP, DNS, HTTP and ICMP traffic and it is assigned to Guest Access role.

Rule ↑	Summary
Allow HTTPS	[TCP Dst : HTTPS] -> [Permit Traffic]
Permit HTTP	[TCP Dst : HTTP] -> [Permit Traffic]
Permit ICMP	[IPProto : ICMP] -> [Permit Traffic]
Permit- Ethertype ARP	[Ether : ARP] -> [Permit Traffic]
Permit- IP UDP Port Destination B...	[UDP Dst : BootP Server] -> [Permit Traffic]
Permit- IP UDP Port Destination D...	[UDP Dst : DNS] -> [Permit Traffic]

3. Network Management Service

- This service is applied only to the Administrator role and allows management traffic having as its destination the network devices in the Automated Campus Validated Design, and a CoS Priority 5.

Rule ↑	Summary
● Campus1-Acc1 switch	[PBIL : 172.9.90.11/32] -> [Permit Traffic/Network Management]
● Campus1-Acc2 switch	[PBIL : 172.9.90.12/32] -> [Permit Traffic/Network Management]
● Campus1-BEB-40	[PBIL : 10.0.0.40/32] -> [Permit Traffic/Network Management]
● Campus1-BEB-50	[PBIL : 10.0.0.50/32] -> [Permit Traffic/Network Management]
● Campus2-Acc1 switch	[PBIL : 172.9.90.13/32] -> [Permit Traffic/Network Management]
● Campus2-Acc2 switch	[PBIL : 172.9.90.14/32] -> [Permit Traffic/Network Management]
● Campus2-BEB-110	[PBIL : 10.0.0.110/32] -> [Permit Traffic/Network Management]
● Campus2-BEB-120	[PBIL : 10.0.0.120/32] -> [Permit Traffic/Network Management]
● EWC appliances	[PBIL : 172.9.98.0/24] -> [Permit Traffic/Network Management]
● FabricCore-BCB-30	[PBIL : 10.0.0.30/32] -> [Permit Traffic/Network Management]
● FabricCore-BEB-10	[PBIL : 10.0.0.10/32] -> [Permit Traffic/Network Management]
● FabricCore-BEB-20	[PBIL : 10.0.0.20/32] -> [Permit Traffic/Network Management]
● Internet-GW	[PBIL : 10.0.0.180/32] -> [Permit Traffic/Network Management]
● Server1-BEB-60	[PBIL : 10.0.0.60/32] -> [Permit Traffic/Network Management]
● Server1-BEB-70	[PBIL : 10.0.0.70/32] -> [Permit Traffic/Network Management]
● Server2-BEB-150	[PBIL : 10.0.0.150/32] -> [Permit Traffic/Network Management]
● Server2-BEB-160	[PBIL : 10.0.0.160/32] -> [Permit Traffic/Network Management]
● XMC appliances	[PBIL : 172.9.99.0/24] -> [Permit Traffic/Network Management]

4. VoIP Phone Service

- The VoIP Phone service is created to allow voice applications access and if desired, priority. Rules can be created to match VoIP services on several criteria and set corresponding CoS profiles, including specific L4 ports, VoIP phone DSCP values, or the MAC OUI of the VoIP vendor:

Rule ↑	Summary
● Allow DSCP 46	[IPToS : 0xB8] -> [Permit Traffic/RTP/Voice/Video]
● SIP	[TCP Dst : 5060] -> [Permit Traffic/RTP/Voice/Video]
● VOIP OUI	[MAC Src : 00:54:01:00:00:00/24] -> [Permit Traffic/RTP/Voice/Video]

5. Redirect Web Services

- Redirect Web Services is used to redirect HTTP traffic of unregistered users to the Captive Portal for authentication.

Rule: Allow HTTP and Redirect

Service Name:

Description:

Rule Status:

Rule Type: Show all rule types

TCI Overwrite:

Traffic Description

Type:

Value:

Actions

Access Control:

Class of Service:

System Log:

Audit Trap:

Disable Port:

HTTP Redirect: Mirror First 15 Packets

Quarantine Role:

Redirect Group 1

- Click **Add Group Index Config**. To have Captive Portal Redundancy between two ExtremeControl engines, use a single FQDN address for the captive portal redirect configuration.

Rule: Allow HTTP and Redirect

HTTP Redirect Configuration

Rule level redirect is only supported by the wireless controller (EWC), which supports only a single URL per group. If multiple rules in the same role specify HTTP Redirect, they must use the same redirect group. Also, the EWC does not support specifying the sockets that apply to redirect directly, but instead uses the socket from the rule definition itself (only L4 TCP Rules are supported). Other platforms support only role level redirect, support 2 URLs per group (allowing for load balancing and fault tolerance), and only redirect traffic on the sockets specified below.

Listen Sockets:

+ Add Group Index Config
 ✎ Edit Group Index Config
 - Remove Group Index

Group Index ↑	Server Index	URL
1	1	http://nacappliance.sqa.net:80/static/index.jsp

Edit Redirect Group

Group Index:

URL (Server Index 1):

Add Secondary URL
OK
Cancel

- In the DNS server(s), add both ExtremeControl IPs to the FQDN address. Make sure that all hardware and applications use the DNS server where the entries reside.

SQA.net 18 record(s)

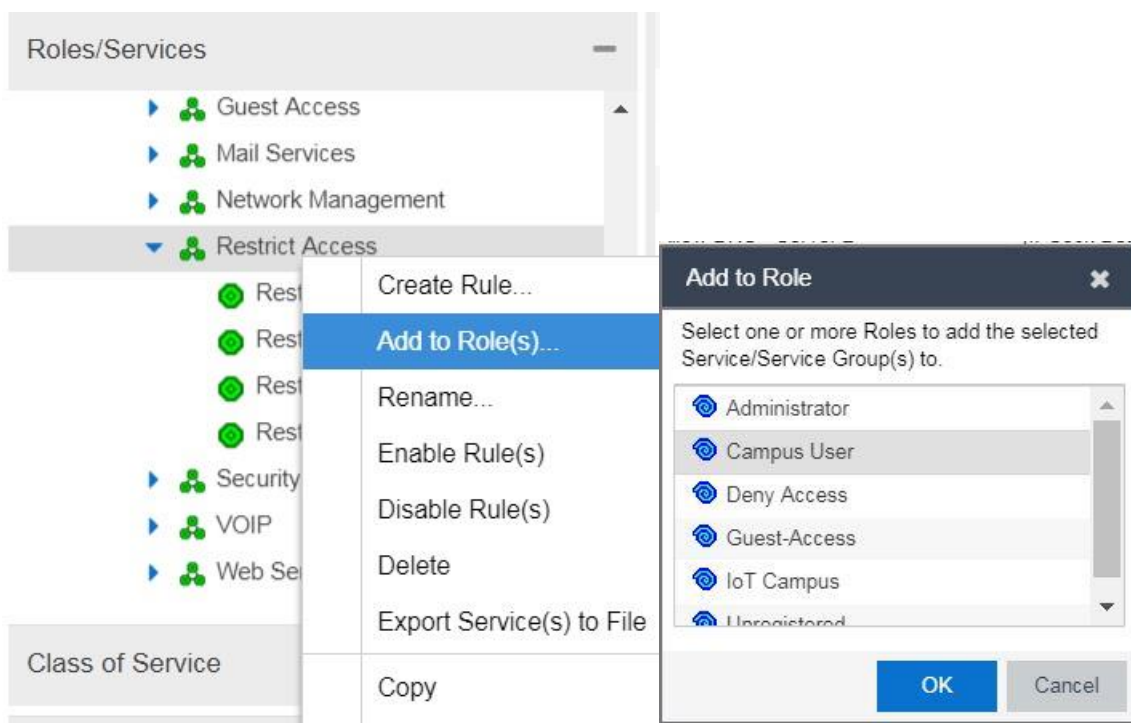
Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[2954], 2008serverr2.sqa.n...	static
(same as parent folder)	Name Server (NS)	2008serverr2.sqa.net.	static
(same as parent folder)	Host (A)	172.9.99.105	static
2008serverr2	Host (A)	172.9.99.105	static
2008serverr2	IPv6 Host (AAAA)	2002:ac09:6369:0000:0000...	static
EWC 1a	Host (A)	172.9.98.106	static
EWC 1b	Host (A)	172.9.98.107	static
Hpurview	Host (A)	172.9.99.108	static
nac1new813	Host (A)	172.9.99.120	6/12/2018 8:00:00 AM
nac2new813	Host (A)	172.9.99.121	6/11/2018 9:00:00 AM
nacappliance	Host (A)	172.9.99.120	
nacappliance	Host (A)	172.9.99.121	

6. Switch and Appliance Restricted Access

- Security of the network devices and appliances is of the utmost importance. To block access to the switches and appliances, a Global Security Service can be created with a rule to either deny or allow limited access to those devices. A subnet or single IP can be entered if a Layer 3 Traffic Classification is chosen. Layers 2, 4 and 7 can also be selected with the appropriate configuration.

Rule ↑	Summary
Allow DHCP - Server 1	[IPSock Dst : 172.9.99.105:BootP Server] -> [Permit Traffic]
Allow DHCP - Server 2	[IPSock Dst : 172.9.99.115:BootP Server] -> [Permit Traffic]
Allow DNS - Server 1	[IPSock Dst : 172.9.99.105:DNS] -> [Permit Traffic]
Allow DNS - Server 2	[IPSock Dst : 172.9.99.115:DNS] -> [Permit Traffic]
Restrict Campus1 Summit Access	[IPDST : 172.10.10.0/24] -> [Deny Traffic]
Restrict Campus2 Summit Access	[IPDST : 172.20.10.0/24] -> [Deny Traffic]
Restrict EWC	[IPDST : 172.9.98.0/24] -> [Deny Traffic]
Restrict VSP Access	[IPDST : 10.0.0.0/24] -> [Deny Traffic]
Restrict XMC	[IPDST : 172.9.99.0/24] -> [Deny Traffic]

- Once the Services and Rules are created, it must be added to the appropriate Roles within their respective Domains. To add to the appropriate Roles, right-click on the Service and select add to Roles. Multiple Roles can be selected as well.



Role Configuration – ERS Access Switches

Although ERS access switches do not support Extreme Policy, the same policy profile structure is used to assign the authorized profile to authenticated users.

- From the Default Policy domain, create the required roles, as illustrated in previous section. **No parameter settings are required in this step.**

- Create any remaining roles required for users connecting to ERS access switches.

- An Access Point role is also created to assign the required RADIUS attributes to the ERS to facilitate wireless functionality:

Role: Access Point - Campus3

General | VLAN Egress | Mappings | Port Default Usage

Name: Access Point - Campus3

Description:

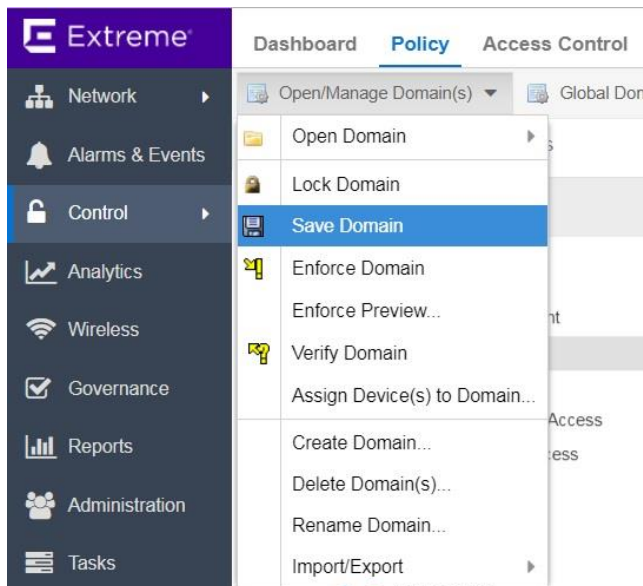
TCI Overwrite: Disabled

Default Actions

Access Control:	None	▼
VLAN:	Disabled	▼
Service ID:	N/A	▲▼
Class of Service:	None	▼
System Log:	Disabled	▼
Audit Trap:	Disabled	▼
Disable Port:	Disabled	▼
AP Aware:	Disabled	▼
HTTP Redirect:	Disabled	▼
Traffic Mirror:	Disabled	▼ <input type="checkbox"/> Mirror First 15 Packets

Saving and Enforcing Domain

- Go to the Control → Policy tab and click **Open/Manage Domain(s)**. Select **Save Domain** from the drop-down list.



- Once the access switches have been deployed (See **Wired User Access**), enforce policy configuration on the domain member network devices. Policy settings will be created automatically.

Note

When using ERS access switches, saving the domain is all that is required. No enforcement is needed.

Roles/Services —


- ▼ ● Roles
 - Administrator
 - Campus User
 - Deny Access
 - Guest-Access
 - IoT Campus
 - Unregistered
- ▶ ● Service Repository

Class of Service +

VLANs +

Network Resources +

Devices/Port Groups +

 Enforce Auto Collapse Panel

Warning

If using more than one Policy Domain, ensure the proper Policy Domain is selected before enforcing the domain.

ExtremeControl Configuration

The Access Control tab provides support for controlling the user connection experience and network access based on a variety of criteria including authentication, user name, MAC-address, time of day, or location.

LDAP Configuration

This solution uses LDAP together with RADIUS and netlogin to control user access to network resources. LDAP is an application protocol used for accessing and maintaining distributed directory information. LDAP can be configured through Extreme Management Center via **Control → Access Control → Configuration → AAA → LDAP Configurations**. To display all the necessary LDAP configuration options, the **Make Advanced** option must be selected from the menu under the **AAA** drop-down menu, by right-clicking on the **Default** profile option and select **Make Advanced**.

Note

Once selected, the “Make Advanced” option is no longer available, and the Default page will retain and display the Advanced options.

1. Click **Add** to add a new LDAP configuration. Click **Add** again to add a new LDAP URL.

The screenshot displays the 'LDAP Configurations' management interface. The main window has a sidebar with a tree view containing 'Configurations', 'AAA', 'Default', 'LDAP Configurations', 'RADIUS Servers', 'Profiles', and 'Captive Portals'. The main content area shows a list of configurations with an 'Add...' button circled in red. A modal dialog titled 'Add LDAP Configuration' is open, featuring fields for 'Configuration Name', 'LDAP Connection URLs', 'Authentication Settings' (Administrator Username, Administrator Password, Timeout), and 'Search Settings' (User Search Root, Host Search Root, OU Search Root). Within this dialog, the 'LDAP Connection URLs' section has its own 'Add...' button, also circled in red, which has triggered a smaller sub-dialog titled 'LDAP Connection URL'. This sub-dialog contains a text input field with the URL 'ldaps://172.9.99.105:636' and 'OK' and 'Cancel' buttons. The main dialog also includes 'Test...' and 'Populate Default Values' buttons at the bottom, and 'Save' and 'Cancel' buttons at the very bottom.

2. Fill in the rest of the fields as shown and click **Save** to finish the configuration:

Configuration Name:

LDAP Connection URLs

ldaps://172.9.99.105:636
ldaps://172.9.99.115:636

Authentication Settings

Administrator Username:

Administrator Password:

Timeout (seconds):

Search Settings

User Search Root:

Host Search Root:

OU Search Root:

Schema Definition

User Object Class:

User Search Attribute:

Keep Domain Name for User Lookup:

User Authentication Type:

User Password Attribute:

Host Object Class:

Host Search Attribute:

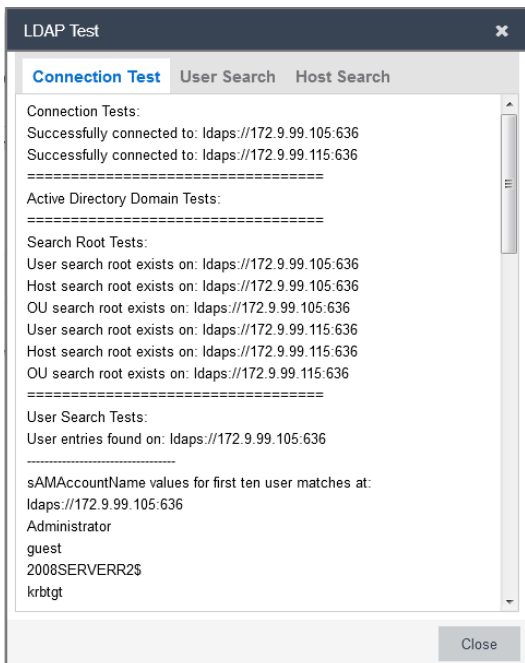
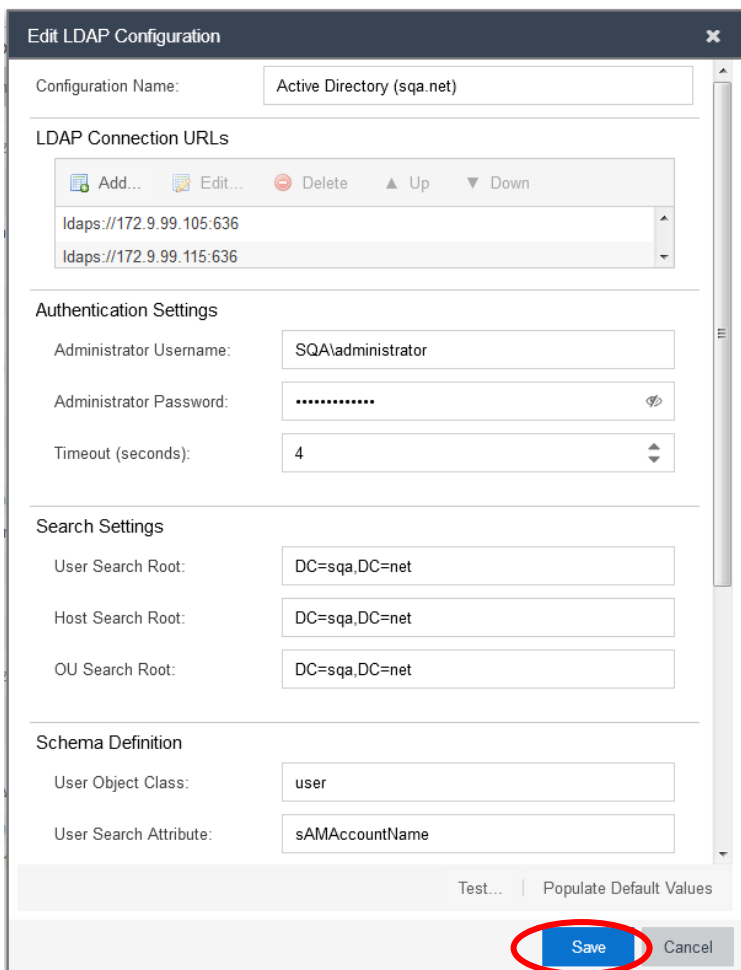
Use Fully Qualified Domain Name:

OU Object Classes:

|

For redundancy, two LDAP URLs are made. Each entry points to a different third-party LDAP server, also called Directory System Agent (DSA)

- You can use the **Test** option to verify that the LDAP server is configured correctly and answering the request. One way to test an LDAP configuration is to select the desired entry, click **Edit**, and then click **Test**. The test might take a few minutes to complete.



3. Configure ExtremeControl to use LDAP for interrogating user credentials. To accomplish this, you must create a new authentication rule to set LDAP as the authentication method. You can add an authentication rule from **Control** → **Access Control** → **Configuration** → **Configurations** → **Default** → **AAA: Default** by clicking **Add** in the **Authentication Rules** section. The rules for Automated Campus were configured as shown in the following pictures.

The screenshot shows the Extreme Networks configuration interface. The left sidebar contains navigation options: Network, Alarms & Events, Control, Analytics, Wireless, Governance, Reports, Administration, and Tasks. The main content area is titled 'Advanced AAA Configuration - Default'. It includes a 'Select AAA Configuration' section with checkboxes for 'Authenticate Requests Locally for:' (MAC (All), MAC (PAP), MAC (CHAP), MAC (MsCHAP), MAC (EAP-MD5)). Below this are dropdown menus for 'Local Password Repository' (Default) and 'Join AD Domain' (Auto Detect). There is also an 'Update Trusted Authorities' section with a 'Trusted Certificate Authority' set to 'none'. At the bottom, the 'Authentication Rules' section is visible, with the 'Add...' button circled in red.

The screenshot shows the 'Edit User to Authentication Mapping' dialog box. It contains the following fields and values:

- Authentication Type: Any
- User/MAC/Host: Pattern Group *
- Location: Any
- Authentication Method: LDAP Authentication
- LDAP Authentication Type: NTLM Authentication
- Supported RADIUS Type: PAP, MsCHAP, PEAP, EAP-MsCHAPV2, and EAP-TTLS with tunneled PAP.
- LDAP Configuration: Active Directory (sqa.net)
- LDAP Policy Mapping: Default

Callouts provide instructions:

- Select LDAP authentication from the available options.
- NTLM authentication is automatically selected as LDAP Authentication method for Microsoft Active directory
- Select the LDAP configuration previously created.

Buttons: OK, Cancel

Configuration

- Configurations
 - Default
 - Rules
 - AAA: Default
 - Portal: Default
- AAA
 - Default
 - LDAP Configurations
 - RADIUS Servers
 - Profiles
 - Captive Portals

Advanced AAA Configuration - Default

Select AAA Configuration

Authenticate Requests Locally for: MAC (All) MAC (PAP) MAC (CHAP) MAC (MsCHAP) MAC (EAP-MD5)

Local Password Repository:

Join AD Domain:

Update Trusted Authorities No information available.

Authentication Rules

Authenticat...	User/MAC/...	Location	Authenticat...	Primary RA...	Backup RA...	Tertiary RA...	Quaternary ...	Inject Auth...	Inject Acco...	LDAP Confi...	LDAP Polic...
Any	*	Any	LDAP Authe...	None	None	None	None	None	None	Active Direct...	Default

RADIUS Configuration

Two RADIUS servers are configured for redundancy. In case the primary server fails, the second one is used for authentication. There's a radius server connected in each server room.

The Timeout and Number of Retries have the default values. The shared secret must be configured and must be the same on ExtremeControl and on the RADIUS server. ExtremeControl will check the RADIUS server is up at every check interval. Verification is done by using a "fakeUser" RADIUS request with a username and password. The username may or may not exist on the RADIUS server. The ExtremeControl considers the RADIUS server to be alive whenever the ExtremeControl receives a RADIUS response, either Reject or Accept. MS Radius servers may log an error for this process. The Health Check parameters can be modified from the Advanced section of the RADIUS configuration window. The default values are used here.

Note

To avoid accumulating log errors because of the Health Check process that may occur for topologies using a Microsoft-based RADIUS server, the Health Check feature can be disabled by unchecking the **Use Server-Status Request** box and the **Use Access Request** box, click **OK**, then **Save**. Alternatively, a replacement user already entered in the RADIUS server can be configured to replace the **fakeUser** configuration.

- To configure a RADIUS server, go to **Control** → **Access Control** → **Configuration** → **AAA** → **RADIUS Servers** and click **Add** to create a new entry:

The screenshot shows the 'Add RADIUS Server' configuration form. The form is divided into two main sections: 'Add RADIUS Server' and 'Advanced RADIUS Server Configuration'.

Add RADIUS Server Section:

- RADIUS Server IP: 172.9.99.105
- Response Window (5-60 sec): 20
- Authentication via Extreme Management Center or Captive Portal:
 - Timeout Duration (2-60 sec): 2
 - Number of Retries (0-20): 1
- Configuration:
 - Auth. Client UDP Port: 1812
 - Proxy RADIUS Accounting Requests
 - Accounting Client UDP Port: 1813
- Change Server Shared Secret:
 - Server Shared Secret: radius

Advanced RADIUS Server Configuration Section:

- Username Format: Keep Domain Name
- Require Message-Authenticator
- Health Check:
 - Use Server-Status Request
 - Use Access Request
 - Username: fakeUser
 - Password: [masked]
 - Check Interval (in sec): 30
 - Number of Answers to Alive: 3
 - Revive Interval (in sec): 60

Buttons: 'Add...' (circled in red), 'Advanced' (circled in red), 'Save', 'Cancel', 'OK' (circled in red), 'Cancel'.

- The configured RADIUS servers are listed:

The screenshot shows the 'RADIUS Servers' configuration page. The table below lists the configured RADIUS servers.

RADIUS Server	Auth Port	Acct Port	Timeout Du...	Number of ...	Shared Sec...
172.9.99.105	1812	1813	2	1	*****
172.9.99.115	1812	1813	2	1	*****

ExtremeControl Engine Configuration

Two ExtremeControl engines are in the server rooms connected to different switches. The use of two engines assures redundancy. Both ExtremeControl engines are configured identically, and if the primary ExtremeControl fails the secondary ExtremeControl will take over its attributions without affecting users. Both engines have authentication and assessment enabled.

To configure ExtremeControl engines, go to **Control** → **Access Control** → **Engines** → **Engine Groups** → **Default**, highlight an engine, and select **Engine Settings**:

The screenshot shows the ExtremeControl web interface. The left sidebar contains navigation options: Network, Alarms & Events, Control, Analytics, Wireless, Governance, Reports, Administration, and Tasks. The main content area is under 'Access Control' and shows a list of engines under the 'Default' group. Two engines are listed: 'NAC1/172.9.99.120' and 'NAC2/172.9.99.121'. The 'Engine Settings' button for the selected engine is circled in red. The right pane shows details for the selected engine, including IP Address (172.9.99.120), Type (Virtual Access Control Engine - IA-V), Version (8.1.4.40), and Serial Number (564d698a30d5630d-dd0e6f0125410fa6). The Management section includes buttons for 'Configuration...' and 'Engine Settings', along with server and capacity information. The License section shows a 'Valid Virtual Appliance License [NETSIGHTEVAL]' and an 'Update...' button. The Certificates section has a 'Manage...' button.

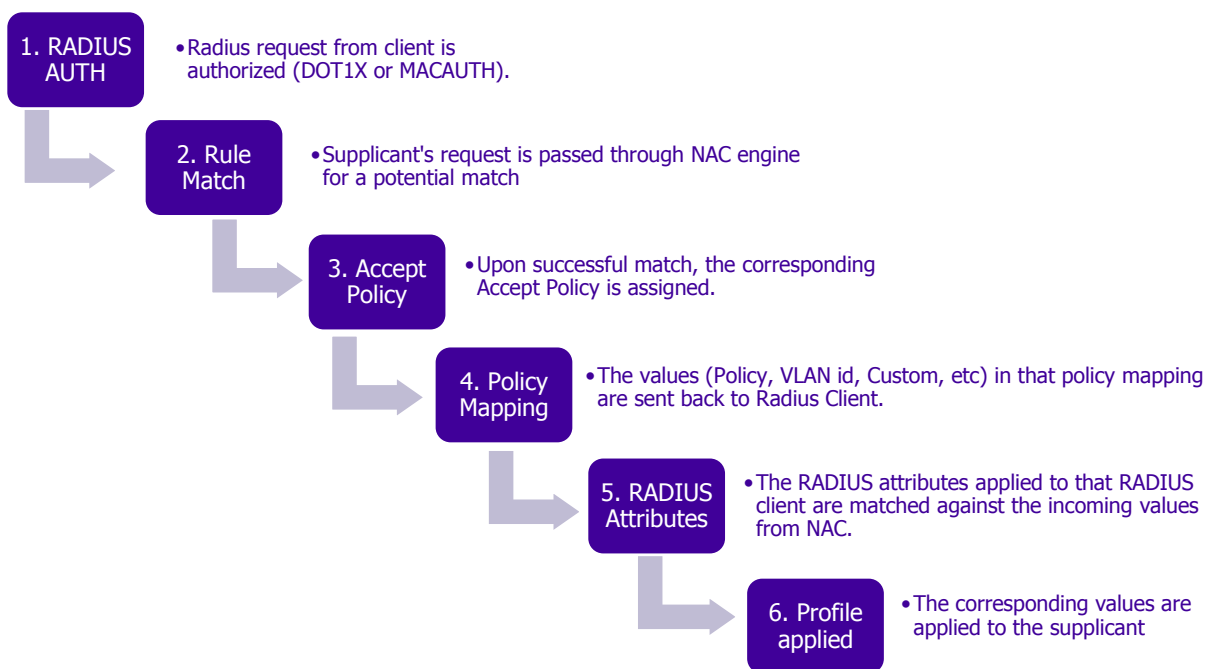
The screenshot shows the 'Engine Settings - Default' dialog box with the 'Credentials' tab selected. The 'Switch Configuration' section includes a 'Shared Secret' field containing the text 'radius', a 'RADIUS Timeout' field set to 10, a 'RADIUS Timeout Retry Count' field set to 3, and a checked checkbox for 'Use Primary RADIUS Server for Redundancy in a Single Engine Configuration. (Basic AAA Configuration only.)'. The 'Admin Web Page Credentials' section has a 'Username' field set to 'admin'. A callout box with a blue border and arrow points to the 'Shared Secret' field, containing the text: 'Enter the Shared Secret matching the network radius server. Click Save.' The dialog box has 'Save' and 'Cancel' buttons at the bottom.

ExtremeControl Profiles and Policy Mapping

ExtremeControl Profiles define the authorization requirements for the end-systems connecting to the network. Each profile has an Accept Policy which is applied to an end-system when it has been authorized locally by the ExtremeControl engine and authentication is configured to replace the attributes returned from the RADIUS server with the Accept Policy.

Each Accept Policy is associated with a Policy Mapping, which defines exactly how end-system traffic is handled on the network. Each mapping specifies a Policy Role (created in the Policy tab) and/or any additional RADIUS attributes included as part of a response to a RADIUS client.

When an end-system authenticates to the network, the ExtremeControl profile is applied and the appropriate RADIUS response attributes are extracted from the mapping and returned in the RADIUS Accept response.



- When a Policy Role (ex: “Campus User”) is created in any Policy Domain, a corresponding Access Control Profile is automatically created under **Control→Access Control → Configuration→Profiles**.

Dashboard Policy **Access Control** End-Systems Reports

Configuration

- Profiles
 - Access Point NAC Profile
 - Admin NAC Profile
 - Administrator NAC Profile
 - Allow NAC Profile
 - Assessing Profile (Auto)
 - Campus User Profile (Auto)**
 - Default NAC Profile
 - Enterprise Access NAC Profile
 - Failsafe Profile (Auto)

Access Control Profile - Campus User Profile (Auto)

Reject Authentication Requests

Authorization

Accept Policy: **Campus User**

Replace RADIUS Attributes with Accept Policy

Use Quarantine Policy Quarantine

Use Failsafe Policy on Error Failsafe

Restrict to End-System Zone None

The same Policy Role is selected as the Accept Policy for this profile by default.

- From the Accept Policy drop-down, click on the gear icon for this Accept Policy to access the Policy Mapping:

Access Control Profile - Campus User Profile (Auto)

Reject Authentication Requests


Authorization

Accept Policy: **Campus User**

Replace RADIUS Attributes with Accept Policy

Use Quarantine Policy

Use Failsafe Policy on Error

Campus User 

- Summit switches:** From the Policy Mapping Edit screen, ensure the Filter field has the exact Policy Role name entered:

Edit Policy Mapping

Name: Campus User

Map to Location: Any

Policy Role: Campus User

VLAN [ID] Name: None

VLAN Egress: Untagged U

Filter: Campus User

Port Profile:

Virtual Router:

Save Cancel

This is associated to the Role created in Policy Manager.

As the Campus User VLAN id is dependent on its location, this field is not required for Summit access switches. The VLAN id will be assigned based on the Policy Role configuration from the appropriate Domain.

This maps to the Filter-id RADIUS attribute used by ExtremeWireless for Role assignment.

- ERS switches:** The Policy Mappings for ERS switches should specify values that match against the corresponding ERS RADIUS Attributes configuration.

Edit Policy Mapping

Name: Campus3-Administrator

Map to Location: Any

Policy Role: Campus3-Administrator

VLAN [ID] Name: [302] v302

VLAN Egress: Untagged U

Filter:

Port Profile:

Virtual Router:

Login-LAT-Group:

Login-LAT-Port:

Custom 1: 1

Custom 2: 1030302

Custom 3:

Save Cancel

This is associated to the Role created in Policy Manager.

From the VLAN Name drop-down menu, choose New, and enter the corresponding VLAN id and name for this Policy Profile.

In the Custom 1 field, enter a value of "1" to enable the "VLAN_Create" RADIUS attribute.

In the Custom 2 field, enter the corresponding I-SID value for this profile..

- ERS-Connected Access Points:** A profile is required for Extreme Access Points connecting to ERS switches to indicate that a trusted FA Client is connected:

The screenshot shows the 'Edit Policy Mapping' window with the following configuration details:

- Name: Access Point - Campus3
- Map to Location: Any
- Policy Role: Access Point - Campus3
- VLAN [ID] Name: [300] v300
- VLAN Egress: Untagged
- Filter: Access Point - Campus3
- Port Profile:
- Virtual Router:
- Login-LAT-Group:
- Login-LAT-Port:
- Custom 1: 1
- Custom 2: 1030300
- Custom 3: 1
- Custom 4:
- Custom 5:
- RADIUS Attribute Lists: Organization 1:

Callout boxes provide the following instructions:

- Pointing to the Policy Role field: "This is associated to the default Role in Policy Manager."
- Pointing to the VLAN [ID] Name field: "From the VLAN Name drop-down menu, choose **New**, and enter the corresponding VLAN id for the FA Mgmt VLAN."
- Pointing to the Custom 1 field: "In the Custom 1 field, enter a value of '1' to enable the 'VLAN_Create' RADIUS attribute."
- Pointing to the Custom 2 field: "In the Custom 2 field, enter the corresponding I-SID value for the FA Mgmt VLAN."
- Pointing to the Custom 3 field: "In the Custom 3 field, enter a value of '1' to enable the 'FA-Client-Trust' attribute."

Repeat this process for each Policy Mapping required on the network.

- **Network Management Login:** For authenticated management access to network devices, a separate policy profile/mapping (such as “Netadmin” below) can be created containing the necessary attributes for authenticated login. Some network devices in this EVD require specific attributes for login access. The Fabric Connect switches and the Wireless Controllers are highlighted below:

Edit Policy Mapping [X]

Name: Netadmin (Administrator)

Policy Role: Administrator

Login-LAT-Port: 1

Custom 1: 6

Management

Access: User Defined

Management: mgmt=su:

Mgmt Service Type: 6

CLI Access: Administrative

[Save] [Cancel]

The value “6” is required for VSP authenticated login.

Required for EWC authenticated login.

Access Control Rule Configuration

This solution requires the use of the ExtremeControl engines, which are configured with unique rules for user authentication and traffic classification. Each rule consists of a name, a set of conditions, and a set of actions that associates it with an Accept Policy. Each Accept Policy is mapped to a role from the Policy tab. Multiple Accept Policies can point to the same role. All conditions defined for a rule must be met; otherwise the rule is not matched.

When ExtremeControl receives an authentication request, all rules are verified in order until one is matched. When a rule is matched, the existing RADIUS attributes are replaced with the rule's Accept policy. The Unregistered rule is placed at the bottom of the access rules list and has a catch-all purpose. It will be matched by default by all traffic that doesn't meet all conditions of any of the previous rules.

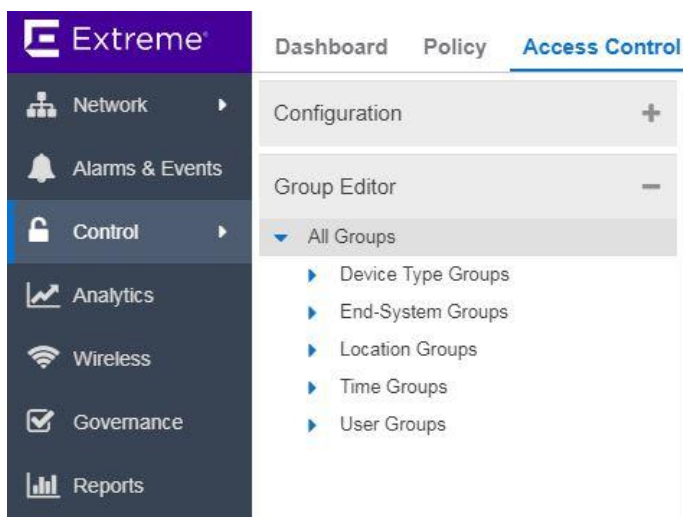
Note

This section details the creation of rules for the ExtremeControl engine to enforce. These are examples, and every customer environment has different security requirements. It is recommended to review the implementation of these requirements with Extreme Networks.

- Before creating a rule, determine the conditions that must be met to assign a role to an end-system attempting access. This can be one condition or several. For example, an end-system authenticating must pass the following criteria:
 - Using 802.1X authentication.
 - Passed login credentials for the Administrator group.
 - Attempted to join the SSID "AC-Campus".
- Each of these conditions can be created in the **Group Editor**, which is used to define the criteria for the rules used in the ExtremeControl configuration. This can be accessed under **Control**→**Access Control**:

Note

The creation of Group Editor profiles is beyond the scope of this document. Please refer to ExtremeControl documentation for further information on Group configuration.

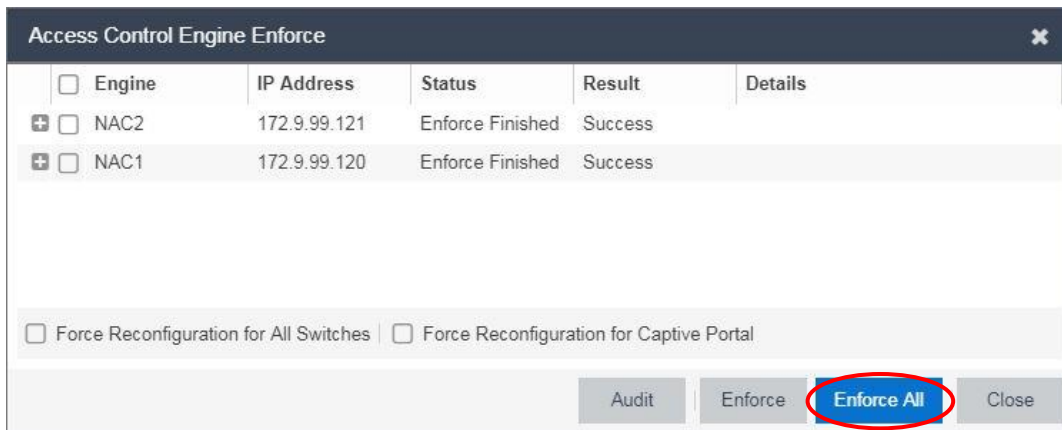


3. To create a new rule, go to **Control** → **Access Control** → **Configuration** → **Rules** and click **Add**:

The screenshot shows the 'Edit Rule' dialog in the Extreme Networks configuration tool. The dialog is titled 'Administrator 802.1x Wireless' and has a 'Rule Enabled' checkbox checked. The 'Name' field contains 'Administrator 802.1x Wireless'. The 'Description' field is empty. The 'Group Label' is set to 'None'. The 'Conditions' section includes: Authentication Method: 802.1X, User Group: Administrators, End-System Group: Any, Device Type Group: Any, Location Group: AC-Campus, and Time Group: Any. The 'Actions' section has a profile set to 'Administrator NAC Profile'. The 'Save' button is circled in red. Annotations include: 'Add...' button circled in red; 'Name the rule.' pointing to the rule name; 'Based on the example conditions described in step one, choose the conditions created in the Group Editor.' pointing to the conditions; and 'Select the profile to apply when conditions are met.' pointing to the profile selection.

4. After changes are made on the Access Control tab, the configuration must be enforced on the ExtremeControl engines.

The screenshot shows the 'Access Control' tab in the Extreme Networks configuration tool. The 'Enforce' button is circled in red. A yellow warning icon is visible next to the 'Engines' button. An annotation with a blue box and arrow points to the warning icon, stating 'Indicates unsaved changes.'



5. The following are the ExtremeControl rules configuration for Automated Campus:

Rules			
Ena...	Rule Name	Conditions	Actions
✓	Blacklist	End-System is in <u>Blacklist</u>	Profile: <u>Quarantine NAC Profile</u> Accept Policy: <u>Deny Access</u> Portal: <u>Default</u> User will be redirected to the Blacklist notification web page.
✓	Assessment Warning	End-System is in <u>Assessment Warning</u>	Profile: <u>Notification NAC Profile</u> Accept Policy: <u>Notification</u>
✓	Access Point	End-System is in <u>Access Points</u>	Profile: <u>Access Point NAC Profile</u> Accept Policy: <u>Access Point</u>
✓	Printer	End-System is in <u>Printers</u>	Profile: <u>Printer NAC Profile</u> Accept Policy: <u>Printer</u>
✓	Administrator MAC Wired	Authentication is <u>MAC</u> and End-System is in <u>Admin MACs</u> and Location is in <u>Campus Access</u>	Profile: <u>Administrator NAC Profile</u> Accept Policy: <u>Administrator</u>
✓	Administrator 802.1x Wired	Authentication is <u>802.1X</u> and User is in <u>Administrators</u> and Location is in <u>Campus Access</u>	Profile: <u>Administrator NAC Profile</u> Accept Policy: <u>Administrator</u>
✓	Administrator 802.1x Wireless	Authentication is <u>802.1X</u> and User is in <u>Administrators</u> and Location is in <u>AC-Campus</u>	Profile: <u>Administrator NAC Profile</u> Accept Policy: <u>Administrator</u>
✓	Campus User 802.1x Wired	Authentication is <u>802.1X</u> and User is in <u>Technician</u> and Location is in <u>Campus Access</u>	Profile: <u>Campus User Profile (Auto)</u> Accept Policy: <u>Campus User</u>
✓	Campus User MAC Wired	Authentication is <u>MAC</u> and End-System is in <u>Campus MACs</u> and Location is in <u>Campus Access</u>	Profile: <u>Campus User Profile (Auto)</u> Accept Policy: <u>Campus User</u>
✓	Campus User 802.1x Wireless	Authentication is <u>802.1X</u> and User is in <u>Technician</u> and Location is in <u>AC-Campus</u>	Profile: <u>Campus User Profile (Auto)</u> Accept Policy: <u>Campus User</u>

✓	Deny Access	Authentication is <u>MAC</u> and End-System is Not in <u>IOT-Legacy</u> and Location is in <u>Open</u>	Profile: <u>Quarantine NAC Profile</u> Accept Policy: <u>Deny Access</u>
✓	IoT Campus MAC Wired	Authentication is <u>MAC</u> and End-System is in <u>IoT MACs</u> and Location is in <u>Campus Access</u>	Profile: <u>IoT Campus Profile (Auto)</u> Accept Policy: <u>IoT Campus</u>
✓	IoT Campus 802.1x Wired	Authentication is <u>802.1X</u> and User is in <u>IOT</u> and Location is in <u>Campus Access</u>	Profile: <u>IoT Campus Profile (Auto)</u> Accept Policy: <u>IoT Campus</u>
✓	IoT Campus 802.1x Wireless	Authentication is <u>802.1X</u> and User is in <u>IOT</u> and Location is in <u>AC-Campus</u>	Profile: <u>IoT Campus Profile (Auto)</u> Accept Policy: <u>IoT Campus</u>
✓	IoT-Legacy	Authentication is <u>MAC</u> and End-System is in <u>IOT-Legacy</u> and Location is in <u>Open</u>	Profile: <u>IoT Campus Profile (Auto)</u> Accept Policy: <u>IoT Campus</u>
✓	Surveillance MAC wired	Authentication is <u>MAC</u> and End-System is in <u>Multicast-MAC</u>	Profile: <u>Surveillance Profile (Auto)</u> Accept Policy: <u>Surveillance</u>
✓	Netadmin	User is in <u>Netadmin</u>	Profile: <u>Netadmin NAC Profile</u> Accept Policy: <u>Netadmin (Administrator)</u>
✓	Wired IoT Bridged MAC	Authentication is <u>MAC</u> and End-System is in <u>Medical Devices</u>	Profile: <u>Wired IoT Bridged Profile (Auto)</u> Accept Policy: <u>Wired IoT Bridged</u>
✓	Registration Denied Access	End-System is in <u>Registration Denied Access</u>	Profile: <u>Registration Denied Access NAC Profile</u> Accept Policy: <u>Deny Access</u>
			Portal: <u>Default</u> User will be notified that they were denied access to the network.
✓	Web Authenticated Users	End-System is in <u>Web Authenticated Users</u>	Profile: <u>Guest-Access Profile (Auto)</u> Accept Policy: <u>Guest-Access</u>
			Portal: <u>Default</u> The user will be granted access and accepted onto the network.
✓	Registered Guests	End-System is in <u>Registered Guests</u>	Profile: <u>Guest-Access Profile (Auto)</u> Accept Policy: <u>Guest-Access</u>
			Portal: <u>Default</u> The user will be granted access and accepted onto the network.
✓	Registration Pending Access	End-System is in <u>Registration Pending Access</u>	Profile: <u>Unregistered NAC Profile</u> Accept Policy: <u>Unregistered</u>
			Portal: <u>Default</u> User will be denied full access until sponsored.
✓	Unregistered	catch-all rule	Profile: <u>Unregistered NAC Profile</u> Accept Policy: <u>Unregistered</u>
			Portal: <u>Default</u> Unregistered user will be redirected to Registration web page.
✓	Default Catchall	catch-all rule	Profile: <u>Default NAC Profile</u> Accept Policy: <u>Unregistered</u>

6. Rules for wired users in a campus of ERS switches are configured in much the same manner. The rest of the rules above still apply:

✓	Access Point - Campus3	End-System is in <u>Access Points</u> and Location is in <u>Campus3</u>	Profile: <u>Access Point - Campus3 Profile (Auto)</u> Accept Policy: <u>Access Point - Campus3_v300[300]</u>
✓	Campus3-Admin-MAC	Authentication is <u>MAC</u> and End-System is in <u>Campus3-Admin</u> and Location is in <u>Campus3</u>	Profile: <u>Campus3-Administrator Profile (Auto)</u> Accept Policy: <u>Campus3-Administrator_v302[302]</u>
✓	Campus3-Admin-dot1x	Authentication is <u>802.1X</u> and User is in <u>Administrators</u> and Location is in <u>Campus3</u>	Profile: <u>Campus3-Administrator Profile (Auto)</u> Accept Policy: <u>Campus3-Administrator_v302[302]</u>
✓	Campus3-IoT-MAC	Authentication is <u>MAC</u> and End-System is in <u>Campus3-IoT</u> and Location is in <u>Campus3</u>	Profile: <u>Campus3-IoT Profile (Auto)</u> Accept Policy: <u>Campus3-IoT_v301[301]</u>
✓	Campus3-IoT-dot1x	Authentication is <u>802.1X</u> and User is in <u>IoT</u> and Location is in <u>Campus3</u>	Profile: <u>Campus3-IoT Profile (Auto)</u> Accept Policy: <u>Campus3-IoT_v301[301]</u>
✓	Campus3-User-MAC	Authentication is <u>MAC</u> and End-System is in <u>Campus3-User</u> and Location is in <u>Campus3</u>	Profile: <u>Campus3-User Profile (Auto)</u> Accept Policy: <u>Campus3-User_v303[303]</u>
✓	Campus3-User-dot1x	Authentication is <u>802.1X</u> and User is in <u>Technician</u> and Location is in <u>Campus3</u>	Profile: <u>Campus3-User Profile (Auto)</u> Accept Policy: <u>Campus3-User_v303[303]</u>
✓	Campus3-Surveillance-MAC	Authentication is <u>MAC</u> and End-System is in <u>Campus3-Surveillance</u> and Location is in <u>Campus3</u>	Profile: <u>Campus3-Surveillance Profile (Auto)</u> Accept Policy: <u>Campus3-Surveillance_v304[304]</u>
✓	Campus3-IoTBridged-MAC	Authentication is <u>MAC</u> and End-System is in <u>Campus3-IoTBridged</u> and Location is in <u>Campus3</u>	Profile: <u>Campus3-IoT Bridged Profile (Auto)</u> Accept Policy: <u>Campus3-IoT Bridged_v907[907]</u>

A summary of the Non-Default rules:

- **Administrator:** Three rules are created - two for Wired and one for Wireless. Wired users can access the network through MAC authentication or 802.1X, whereas Wireless Administrator users may only access via 802.1X. When the conditions of a rule are met the corresponding Profile (which contains the Accept Policy Role) is assigned to that user.
- **Campus User and IoT Campus:** These rules are set up the same way as Administrator, with three rules each, with successful matching of conditions resulting in assignment to their corresponding Role and VLAN.
- **IoT-Legacy and Wired IoT Bridged MAC:** These rules are for 3rd party or legacy devices that may not be compatible with the supported authentication methods. In these cases, MAC authentication is used to assign them to the appropriate Role.
- **Deny Access:** Any MACs not authorized under IoT Legacy is assigned to the Quarantine role and denied access.
- **Surveillance MAC wired:** MAC authentication is used to identify the Vendor OUI of the IP Cameras.
- **Netadmin:** This is an 802.1X rule for administrators to authenticate when accessing network devices via SSH. When administrators authenticate via the LDAPs User Group “Netadmin”, the Netadmin Policy Mapping (noted in [Profiles and Policy Mappings](#)) is applied allowing CLI access.

- **Unregistered:** This rule is used as a catch-all for unauthenticated users, who are redirected to the Captive Portal for Registration to the network.
 - **Registered Guests:** Upon successful registration via the Portal, Guest Users then match this rule and are assigned the Guest-Access Role.
7. Upon successful passing of an ExtremeControl rule, the corresponding Accept Policy is sent back to the Radius Client (access switch or Access Point) to be applied to the end user.

Extreme Wireless Configuration

ExtremeWireless Controller Configuration

This section includes an easily implemented, efficient solution to service wireless users that require access to the network. The ExtremeWireless User Access uses two wireless controllers and multiple APs for redundancy. Each wireless controller is connected to separate Fabric Connect switches in the server rooms. This provides redundancy, so that if one of the controllers, switches, or server rooms fails, the other can assume control.

At all locations, access points are connected to the ExtremeSwitching access stacks. This architecture allows a pair of controllers to control many APs, making the administration and management of large networks much easier and adding a layer of protection for network availability.

This solution implements two ExtremeWireless Controller virtual appliances, to maximize flexibility, ease of installation, and support for a wide variety of APs. Extreme's virtual appliances have resiliency built in from the start. Running as active-active pairs, if an appliance happens to fail the other appliance can take over the full load while maintaining AP connectivity. Failover occurs within milliseconds; APs continue running without interruption to existing or new client connections.

Virtual Wireless Controller Configuration

Before configuring wireless network access, some basic accessibility settings must be made on the wireless controllers.

The ExtremeWireless appliance can be managed from a console, from a graphical interface, and from Extreme Management Center. For this Validated Design, only the graphical interface and Extreme Management Center configurations are presented. After the initial installation, the management IP address must be configured from the console. For more details on how to configure the virtual wireless controller from the console, see the GTAC Knowledge [documentation](#).

To access the configuration graphical interface, enter the following address into the browser https://<ip_address>:5825 .

All configurations are executed only on the primary wireless controller; they are automatically mirrored on the secondary wireless controller.

The NTP server must be configured to ensure that both wireless controllers have the same time. If the times are not synchronized, an error will be generated, and the pairing will not be completed. For details, refer to Network Time Protocol (NTP) in [Design Considerations](#).

Wireless controllers should be added to Extreme Management Center for Policy and ExtremeControl rules enforcement.

Pairing Configuration

To ensure redundancy, the two wireless controllers must maintain the same configuration. This is achieved by configuring pairing. To configure pairing, go to **Controller** → **Administration** → **Availability**.

ExtremeWireless Controller 1 (EWC1):

The screenshot shows the 'Availability Wizard' configuration for EWC1. The 'Controller Availability Settings' section is configured as follows:

- Availability Wizard:** Start button.
- Controller Availability Settings:**
 - Stand-alone:
 - Paired:
 - Wireless Controller IP Address:
 - Current Wireless Controller is primary connection point:
 - Fast Failover:
 - Detect link failure in: (2 - 30 seconds)
- Synchronization Option:**
 - Synchronize System Configuration:
 - Synchronize Guest Portal Accounts:

Annotations in the image:

- IP address of the Secondary Wireless Controller (EWC2) points to the 'Wireless Controller IP Address' field.
- Primary EWC requires that this checkbox be selected. points to the 'Current Wireless Controller is primary connection point' checkbox.

Footer: [EWC1a | V2110 Small | 03 days, 21:52] User: admin | Software: 10.41.07.0008 | Admin Users: 4 | © 2006-2018 Extreme Networks. All Rights Reserved.

ExtremeWireless Controller 2 (EWC2):

The screenshot shows the 'Availability Wizard' configuration for EWC2. The 'Controller Availability Settings' section is configured as follows:

- Availability Wizard:** Start button.
- Controller Availability Settings:**
 - Stand-alone:
 - Paired:
 - Wireless Controller IP Address:
 - Current Wireless Controller is primary connection point:
 - Fast Failover:
 - Detect link failure in: (2 - 30 seconds)
- Synchronization Option:**
 - Synchronize System Configuration:
 - Synchronize Guest Portal Accounts:

Annotations in the image:

- IP address of the Primary Wireless Controller (EWC1) points to the 'Wireless Controller IP Address' field.
- Secondary EWC requires that this checkbox not be selected. points to the 'Current Wireless Controller is primary connection point' checkbox.

Footer: [EWC1b | V2110 Small | 09 days, 20:55] User: admin | Software: 10.41.07.0008 | Admin Users: 3 | © 2006-2018 Extreme Networks. All Rights Reserved.

Host Attributes Configurations

The wireless controller's DNS host name, default gateway, DNS server address(es), and domain name are configured on the **Host Attributes** page. The Automated Campus solution uses two DNS servers for redundancy. **The settings must be made on both wireless controllers because they are not automatically mirrored.**

The controller sends the host name query to the first DNS server in the list. If this is not reachable then the controller sends the host name query to the second DNS server.

The **Host Attributes** page can be found under **Controller → Administration**.

EWC1 and EWC2

Host Attributes

Network Identification

Host Name: EWC1a

Domain Name: sqa.net

DNS

172.9.99.105
172.9.99.115
134.141.79.193

Remove selected server

Move up

Server Address: 172.9.99.105

Add Server

Default Gateway IP: 172.9.98.1

Save

Configure Host Name and Domain Name.

Add DNS server IP addresses.

Assign a Default Gateway IP.

Routing Configuration

The virtual wireless controllers are network devices and must be able to route user traffic to the different appliances and servers used in the Validated Design (ExtremeControl engines, DHCP, DNS, NTP servers). Also, the wireless controllers have networks directly connected, that must be advertised to the rest of the setup. For the Automated Campus solution, static routing was implemented.

First, the **esa0** interface must be created on both wireless controllers and on the VSP7xxx switches.

Refer to the DVR Configuration (Leaf) section for the IP interface configuration to connect the wireless controllers to the setup.

1. Configure an interface on Wireless Controllers to connect to the VSP 7200s.

To create the interface on the Wireless appliance, go to **Controller → Network** and click **New**.

EWC1

Topology: WlessContr1

General

Core

Name:
 Mode:
 3rd Party:

Layer 2

VLAN Setting: VLAN ID: (1 - 4094)
 Untagged Tagged
 Port:

Layer 3:
 Layer 3 - IPv4

Interface IP:
 Mask:
 DHCP:
 MTU:
 AP Registration:
 Management Traffic:

Buttons: New, New Group, Delete, Save

Annotations:

- Configure interface name and set the Mode to Physical.
- Configure a /24 IP interface in same subnet as the VSP7xxx Switch interface.
- Configure same VLAN id as VSP7xxx
- Configure interface to be available for AP Registration and Management Traffic.

EWC2

Topology: WlessContr2

General

Core

Name:
 Mode:
 3rd Party:

Layer 2

VLAN Setting: VLAN ID: (1 - 4094)
 Untagged Tagged
 Port:

Layer 3:
 Layer 3 - IPv4

Interface IP:
 Mask:
 DHCP:
 MTU:
 AP Registration:
 Management Traffic:

Buttons: New, New Group, Delete, Save

Annotations:

- Configure interface name and set the Mode to Physical.
- Configure a /24 IP interface in same subnet as the VSP7xxx Switch interface.
- Configure same VLAN id as VSP7xxx
- Configure interface to be available for AP Registration and Management Traffic.

2. Configure Default Route on Wireless Controllers to establish connectivity with network:

- To configure a static route on the esa0 interface go to **Controller → Network → Routing Protocols → Static Routes**.
- Click the **New** button to enter route configuration.

EWC1 and EWC2:

Note

Due to the DVR Domain configuration in the server rooms, the next hop gateway IP address will be the same on each EWC.

3. Verify forwarding table on EWCs.

To verify the status of the static route, click the forwarding table tab. A new browser page will open, and the routing table of the wireless controller is displayed.

Controller → Network → Routing Protocols → View Forwarding Table

Route #	Destination	Netmask	Gateway	Interface	Type	Status
1	0.0.0.0	0.0.0.0	172.9.98.1	WlessContr1	Static	Active
2	127.0.0.0	255.0.0.0		lo	Connected	Active
3	169.254.0.0	255.255.192.0		csi32	Connected	Active
4	172.9.98.0	255.255.255.0		WlessContr1	Connected	Active
5	172.31.0.16	255.255.255.240		tap0	Connected	Active
6	172.90.40.0	255.255.255.0		Guest	Connected	Active

Wireless Controller Access Control Configuration

The wireless controllers use the ExtremeControl servers to provide multiple services like authentication, role-based management for users, CoS marking, access control policies, and captive portal. Because of the VLAN's role and policy requirements, the wireless controllers have their own domain.

The wireless controllers will use the ExtremeControl engines as RADIUS servers, and both wireless controllers need to be added in the Switches list.

Note

To add the EWCs to the ExtremeControl engine, they must first be manageable via XMC.

- To add the EWCs to ExtremeControl, navigate to **Control → Access Control → Engines → Engine Groups → Default → Switches → Add**

Add Switches to Access Control Engine Group: Default

1. Expand to display the two EWC V2110 appliances and select.

2. Select from Switch Type: Layer 2 Out-of-Band

3. Select from Primary Engine: IP Primary Engine

4. Select from Secondary Engine: IP Secondary Engine

5. Select from Auth. Access Type: Any Access

6. Select from RADIUS Attributes to Send: Extreme Identifi Wireless

7. Select from RADIUS Accounting: Enabled

8. Select from Policy Domain: Wireless-Campus

Advanced Settings...

Save Close

- The wireless controllers will use the ExtremeControl engines as RADIUS servers, to authenticate users connecting to the secured wireless networks and for integration with DHCP. To define the ExtremeControl engines for DHCP integration go to **VNS → Global → NAC Integration → New** and add both ExtremeControl engines:

NAC DHCP Receiver Address

Nac Server Name (optional):

Address for DHCP Traffic:

Configure DHCP Receiver Address for NAC:
NAC Server Name: NAC1
Address for DHCP Traffic: 172.9.99.120

- Both ExtremeControl engines are added, for redundancy.

NAC Integration Options

DHCP Destination Addresses

Server	NAC Name	IP Address
<input type="checkbox"/> 1	NAC1	172.9.99.120
<input type="checkbox"/> 2	NAC2	172.9.99.121

NAC can accept DHCP messages from the controller's DHCP server and use them to fingerprint devices. At most 3 addresses can be entered, one per NAC. If no addresses are entered then the controller will not forward DHCP requests from stations to NAC.

- To define the ExtremeControl engines as RADIUS servers, go to **VNS → Global → Authentication → RADIUS Servers → New**

Both ExtremeControl engines are added, for redundancy.

RADIUS Settings

RADIUS Server

Server Alias:

Hostname/IP:

Shared Secret:

Default Protocol:

Authentication

Priority:

Total Number of Tries:

RADIUS Request Timeout: (seconds)

Port:

Accounting

Priority:

Total Number of Tries:

RADIUS Request Timeout: (seconds)

Interim Accounting Interval: (minutes)

Port:

Send Interim Accounting Records for:

Fast Failover Events:

Health Monitoring

Polling Mechanism:

Test Request Timeout: (seconds)

Add/Configure RADIUS Server for both NAC engines:
 NAC Server Name: NAC1 /NAC2
 Hostname/IP: 172.9.99.120/172.9.99.121

Configure a shared secret password that matches the shared secret in the ExtremeControl AAA setting
(Access Control→Configuration→AAA→Radius Servers)

RADIUS Servers

RFC 3580 (ACCESS-ACCEPT) Options

Strict Mode

Server	Default	Retries		Timeouts		Ports		Priority		
		Auth	Acct	Auth	Acct	Auth	Acct	Auth	Acct	
<input type="checkbox"/> Nac1	172.9.99.120	MS-CHAP2	3	3	5	5	1812	1813	3	3
<input type="checkbox"/> Nac2	172.9.99.121	MS-CHAP2	3	3	5	5	1812	1813	4	4

* RADIUS servers which are currently associated with WLAN Service(s) cannot be removed

MAC Address

MAC Address Format: (for MAC-Based authentication only)

Captive Portal Configuration

Captive portal is used by the wireless users connecting to the network as guests.

Captive portal must be configured on the ExtremeControl engines. The <Default> captive portal profile is used for the Automated Campus Validated Design and requires minimum configuration from the Extreme Management Center Control tab.

Control → Access Control → Configuration → Captive Portals

Name	Guest Registration	Authenticated Registration
Default	Disabled	Disabled

Guest Web Access and **Authenticated Registration** were selected. The default settings were used for the rest of the parameters. Enforce configuration on the ExtremeControl engines for the settings to take effect.

Control → Access Control → Configuration → Captive Portals → Website Configuration

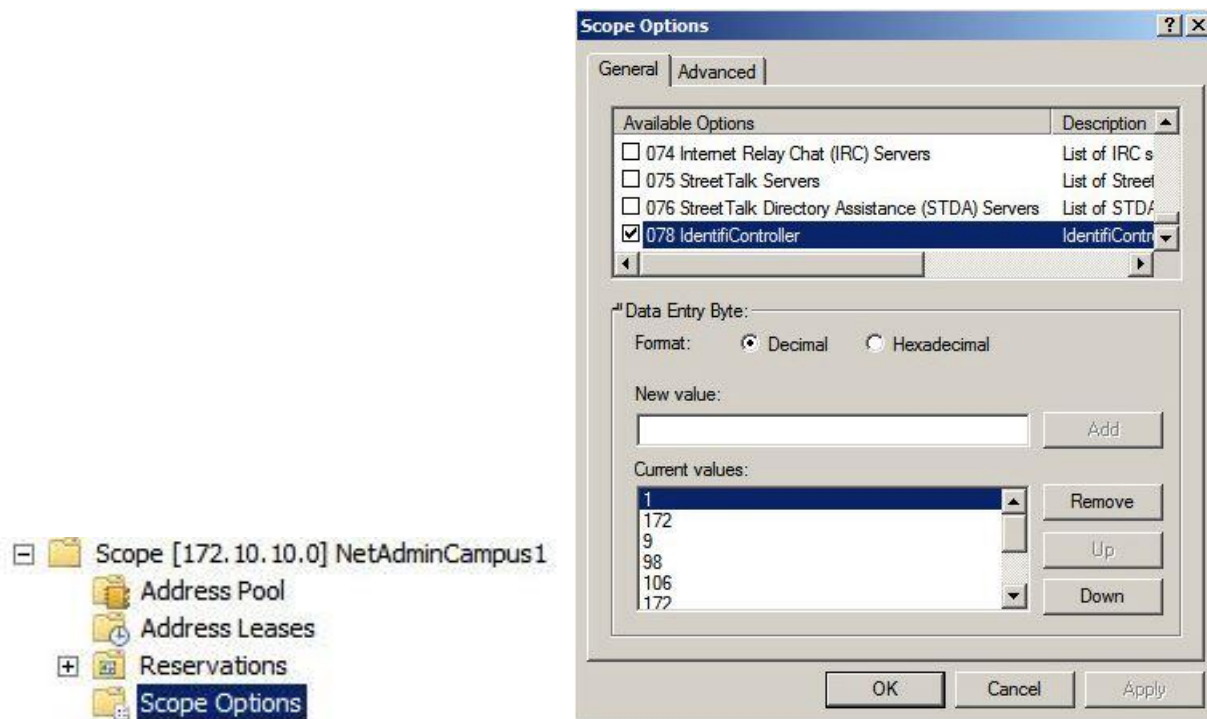
Select: Guest Settings | Guest Registration
Select: Authentication Settings | Authenticated Registration

Wireless AP Discovery

Ensure that the appropriate services on your enterprise network are prepared to support the discovery process. To use a DHCP server for wireless AP discovery, ensure that it supports option 78 (DHCP for SLP RFC2610). The APs use this method to discover the controller(s), and option 78 must be set for the subnets connected to the ports of the controller and the subnets connected to the APs.

Below is an example of how this might be configured in Windows Server 2008.

To configure DHCP option 78 on the DHCP server, right click on the **Scope Options** for the scope meant to service the APs and select **Configure Options**. Select option 78 and configure the IP addresses of both wireless controllers. Besides redundancy, this also ensures load balancing between the two appliances. The first value introduced must be 1. This value announces that the following fields represent IP addresses for wireless controllers. Use the **New Value** box to enter the addresses, byte by byte. For the Automated Campus solution, the **esa0** interface is used for AP connection.



The AP does not use the DNS information from the initial DHCP offer supplied from the DHCP server. After the IP setup stage, the AP decides whether to use the static controller IP or start its discovery methods. If SLP/DNS/VCI discovery is started, the AP sends periodic DHCP informs to get more data to complete its boot discovery methods. If the DHCP server does not reply to the inform, the process to contact the controller will fail and start over.

Wireless AP Registration

When the discovery process is successful, the AP registers with the wireless controller. At this point, the controller can be configured with one of the following security modes, which defines how the controller behaves when registering new/unknown devices:

- Allow all Wireless APs to connect: If the controller does not recognize the registering serial number, a new registration record is automatically created for the AP and receives a default configuration. If the controller recognizes the serial number, it indicates that the registering device is pre-registered with the controller and uses the existing registration record to authenticate the AP and the existing configuration record to configure the AP
- Allow only approved Wireless APs to connect (secure mode): If the controller does not recognize the AP, the AP's registration record is created in pending state and the administrator is required to manually approve a pending AP for it to provide active service. The pending AP receives minimum configuration only, which allows it to maintain an active link with the controller for future state change.

AP → Global → Registration

Wireless AP Registration

Security Mode:

Allow all Wireless APs to connect

Allow only approved Wireless APs to connect

Discovery Timers:

Number of retries: (1 - 255)

Delay between retries: (1 - 10 seconds)

SSH Access:

Password:

Confirm password:

Secure Cluster:

Cluster Shared Secret:

Use Cluster Encryption

- To verify the AP availability, go to Reports → APs → AP Availability

EWC1a - Reports - Wireless AP Availability

No refresh Refresh every secs

Availability Link is UP

Color Legend:

Wireless AP has active tunnel passing data Wireless AP has backup tunnel Wireless AP not connected No information

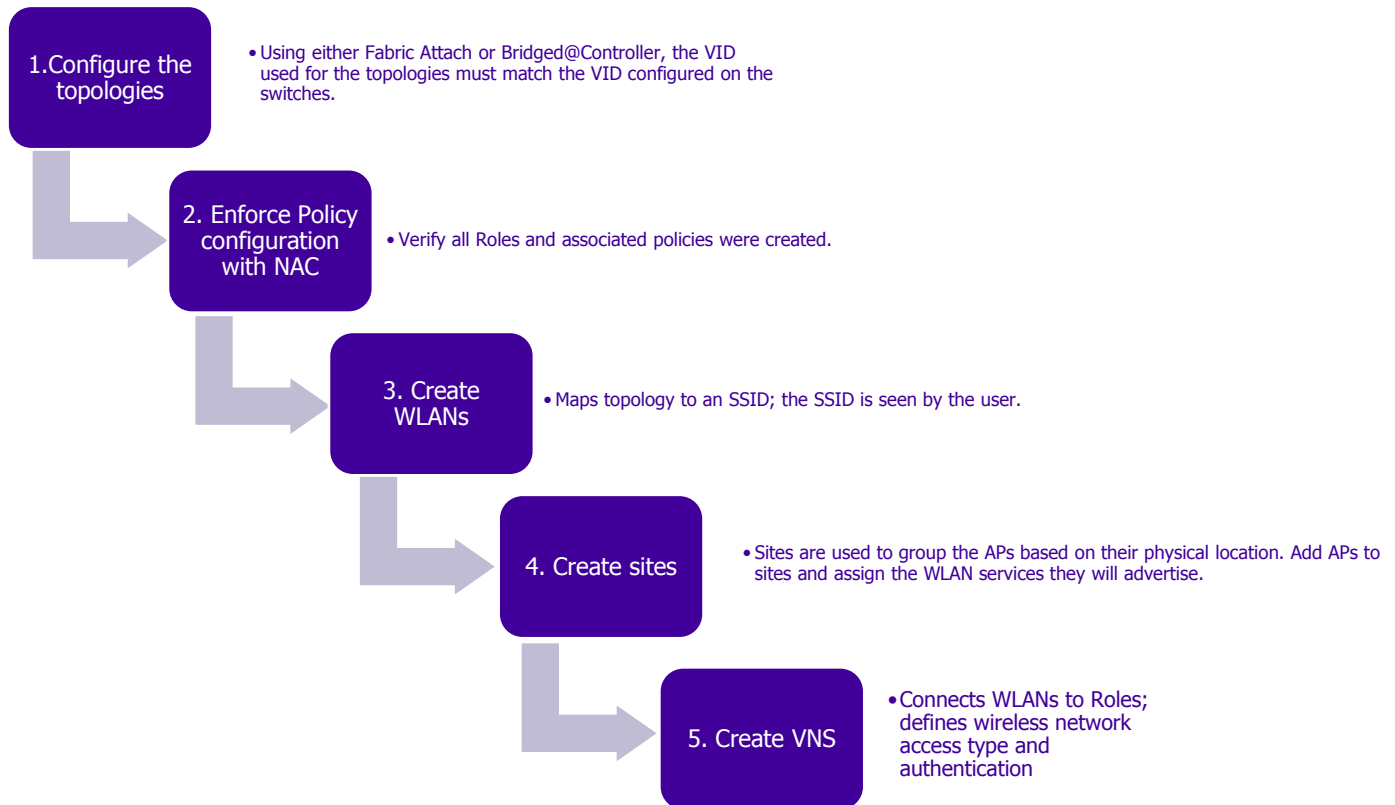
Wireless APs List:

<p>[Local] Acc120-57AA58 1624Y-1357300000 D8:84:66:57:AA:58 uptime: 4 d, 16:24:10 172.10.10.22</p> <p>Connected</p>	<p>[Foreign] Acc120-E32588 1745Y-1458900000 D8:84:66:E3:25:B8 uptime: 4 d, 16:24:11 172.10.10.21</p> <p>Connected</p>	<p>[Local] Acc121-257AAB 1746Y-1122400000 B4:2D:56:25:7A:AB uptime: N/A</p> <p>Not connected</p>
<p>[Foreign] Acc121-31D79A 1546Y-1001200000 D8:84:66:31:D7:9A uptime: 4 d, 16:35:15 172.10.10.23</p> <p>Connected</p>	<p>[Local] Acc220-4FA926 1608Y-1168800000 D8:84:66:4F:A9:26 uptime: N/A 172.20.10.23</p> <p>Connected</p>	<p>[Foreign] Acc220-4FA9BC 1608Y-1176300000 D8:84:66:4F:A9:BC uptime: N/A 172.20.10.22</p> <p>Connected</p>
<p>[Local] Acc221-4FA9B6</p>	<p>[Foreign] Acc221-7A04B7</p>	

Data as of Aug 30, 2018 01:53:59 pm

Wireless Network Configuration

For a wireless network to become accessible to users, configurations must be created in the following sections: **Topologies, Roles, WLAN Services, Virtual Networks and Sites**. There is a dependency between the sections and a configuration order must be followed.



1. Topology Configuration

In this section, the physical access provisioning for the user access is created. Every topology is essentially a VLAN. To add a new topology, go to **VNS → Topologies** and click **New**.

Topologies

Topology Name	Group	VLAN ID	Tagged	Port	IP Address	Mode
<input type="checkbox"/> Admin	×	-	×	Admin	Static: 192.168.10.4 Dynamic IP Address	Admin
<input type="checkbox"/> 100-Campus1 mgmt	×	100	✓	-	-	Fabric Attach
<input type="checkbox"/> 1050-Administrator	×	1050	✓	-	-	Fabric Attach
<input type="checkbox"/> 1051-CampusUser	×	1051	✓	-	-	Fabric Attach
<input type="checkbox"/> 1052-IOT	×	1052	✓	-	-	Fabric Attach
<input type="checkbox"/> 200-Campus2 Mgmt	×	200	✓	-	-	Fabric Attach
<input type="checkbox"/> Bridged at AP untagged	×	4093	×	-	-	B@AP

Internal VLAN ID:
 Multicast Support:

For the topologies that wireless users will use to connect to the network, one of two modes must be selected: **Bridge Traffic Locally at EWC** or **Fabric Attach**. The topology mode dictates how the traffic from the clients is going to be treated.

Bridge Traffic Locally at EWC - Users connecting to the wireless network send the traffic to the AP. The AP encapsulates the traffic and tunnels it to the controller. The controller de-encapsulates the traffic, processes it and sends to the network over the physical 1 interface in the user access VLAN.

Fabric Attach - The Fabric Attach topology type is similar to B@AP with the added I-SID parameter. Upon boot up with this topology mode set, the AP will send the configured VLAN/I-SID value to the FA Proxy, informing its requirement for communication.

- Fabric Attach can be configured on a controller anywhere a B@AP topology can be configured. Users connecting to the wireless network send the traffic to the AP. The AP sends the traffic to the network over its management port in the user access VLAN.

Topology:

In the Automated Campus solution, Guest and authenticated wireless user access is possible from all campuses. All Guest users are provisioned with a **Bridged@EWC** topology and are placed in the same network. All authenticated users are provisioned with **Fabric Attach** topologies and are placed in different VLAN/subnets, based on the campus they are connected to.

The following user access topologies were configured for the solution:

- **100-Campus1 Mgmt:**

Topology: 100-Campus1 mgmt

Used by Access Points (FA clients) and access switches (FA Proxies) for FA management to request I-SID information via LLDP, and also used for IP management of the Access Points by the EWCs. The routing is done on the VSP switch acting as the FA server. This VLAN is for use in Campus 1.

The IoT topology is configured as:

- Name: 100-Campus1 Mgmt
- Mode: Fabric Attach
- VLAN ID: 100

- **200-Campus2 Mgmt:**

Topology: 200-Campus2 Mgmt

General	Multicast Filters
<p>Core</p> <p>Name: 200-Campus2 Mgmt</p> <p>Mode: Fabric Attach</p>	<p>Layer 3: <input type="checkbox"/></p> <p>Layer 3 - IPv4</p> <p>Mask (optional):</p>
<p>Layer 2</p> <p>VLAN Setting: VLAN ID: 200 (1 - 4094)</p> <p><input checked="" type="radio"/> Tagged</p> <p>I-SID: 1020200</p> <p><input type="checkbox"/> ARP Proxy</p>	
<p>Status</p> <p>Synchronize: <input checked="" type="checkbox"/> [synchronized]</p> <p>Replicated when Synchronize Configuration is enabled</p>	
<p>New</p> <p>New Group</p> <p>Delete</p>	<p>Save</p>

Used by Access Points (FA clients) and access switches (FA Proxies) for FA management to request I-SID information via LLDP, and also used for IP management of the Access Points by the EWCs. The routing is done on the VSP switch acting as the FA server. This VLAN is for use in Campus 2.

The IoT topology is configured as:

- Name: 200-Campus2 Mgmt
- Mode: Fabric Attach
- VLAN ID: 200

- **300-Campus3-Mgmt:**

Topology: 300-Campus3-mgmt

General	Multicast Filters
<p>Core</p> <p>Name: 300-Campus3-mgmt</p> <p>Mode: Fabric Attach</p>	<p>Layer 3: <input type="checkbox"/></p> <p>Layer 3 - IPv4</p> <p>Mask (optional):</p>
<p>Layer 2</p> <p>VLAN Setting: VLAN ID: 300 (1 - 4094)</p> <p><input checked="" type="radio"/> Tagged</p> <p>I-SID: 1030300</p> <p><input type="checkbox"/> ARP Proxy</p>	
<p>Status</p> <p>Synchronize: <input checked="" type="checkbox"/> [synchronized]</p> <p>Replicated when Synchronize Configuration is enabled</p>	
<p>New</p> <p>New Group</p> <p>Delete</p>	<p>Save</p>

Wireless topologies connecting to ERS access switches are configured identically as for Summits. Used by Access Points (FA clients) and access switches (FA Proxies) for FA management to request I-SID information via LLDP, and also used for IP management of the Access Points by the EWCs. The routing is done on the VSP switch acting as the FA server. This VLAN is for use in Campus 3.

The IoT topology is configured as:

- Name: 300-Campus3 Mgmt
- Mode: Fabric Attach
- VLAN ID: 300
- I-SID: 1030300

- **1050-Administrator:**

Topology: 1050-Administrator

General		Multicast Filters	
Core		Layer 3: <input type="checkbox"/>	
Name: 1050-Administrator		Layer 3 - IPv4	
Mode: Fabric Attach		Mask (optional):	
Layer 2			
VLAN Setting: VLAN ID: 1050 (1 - 4094)			
<input checked="" type="radio"/> Tagged <input type="radio"/> Untagged			
I-SID: 1501050			
<input type="checkbox"/> ARP Proxy			
Status			
Synchronize: <input checked="" type="checkbox"/> [synchronized]			
Replicated when Synchronize Configuration is enabled			
New		Save	
New Group		Delete	

Used by Administrator users connecting to the network and are given the Administrator role. This topology is active in both campuses to allow wireless roaming. The routing is done on the VSP switches acting as the FA server.

The Administrator topology is configured as:

- Name: 1050-Administrator
- Mode: Fabric Attach
- VLAN ID: 1050
- I-SID: 1501050

- **1051-CampusUser:**

Topology: 1051-CampusUser

General		Multicast Filters	
Core		Layer 3: <input type="checkbox"/>	
Name: 1051-CampusUser		Layer 3 - IPv4	
Mode: Fabric Attach		Mask (optional):	
Layer 2			
VLAN Setting: VLAN ID: 1051 (1 - 4094)			
<input checked="" type="radio"/> Tagged <input type="radio"/> I-SID: 1501051 <input type="checkbox"/> ARP Proxy			
Status			
Synchronize: <input checked="" type="checkbox"/> [synchronized]			
Replicated when Synchronize Configuration is enabled			
New		New Group	
Delete		Save	

Used by end users with limited access connecting to the network and are given the Campus User role. This topology is active in both campuses to allow wireless roaming. The routing is done on the VSP switches acting as the FA server.

The Administrator topology is configured as:

- Name: 1051-CampusUser
- Mode: Fabric Attach
- VLAN ID: 1051
- I-SID: 1501051

- **1052-IOT:**

Topology: 1052-IOT

General		Multicast Filters	
Core		Layer 3: <input type="checkbox"/>	
Name: 1052-IOT		Layer 3 - IPv4	
Mode: Fabric Attach		Mask (optional):	
Layer 2			
VLAN Setting: VLAN ID: 1052 (1 - 4094)			
<input checked="" type="radio"/> Tagged <input type="radio"/> I-SID: 1501052 <input type="checkbox"/> ARP Proxy			
Status			
Synchronize: <input checked="" type="checkbox"/> [synchronized]			
Replicated when Synchronize Configuration is enabled			
New		New Group	
Delete		Save	

Used by IoT devices and users connecting to the network and are given the IoT-Campus role. This topology is active in both campuses to allow wireless roaming. The routing is done on the VSP switches acting as the FA server.

The Administrator topology is configured as:

- Name: 1052-IOT
- Mode: Fabric Attach
- VLAN ID: 1052
- I-SID: 1501052

• **Guest:**

Topology: Guest

Used by Guest users connecting to the network and are given the Guest-Access role. Access control is performed by the wireless controllers. User traffic is directly routed/tunneled to the EWCs rather than forwarded at the switch via I-SIDs. The EWCs de-encapsulate the tunnel header and egress the original packet back out that interface on VLAN 906. The Guest Wireless VLAN vid 906 is configured on the Server Room switches only.

The Layer 3 configuration allows for services (DHCP, captive portal, etc) to be accessed over this network segment in the server rooms. Configure an IP interface for VLAN 906 that corresponds to the EWC's own point of presence on the VLAN. In this case, the EWC interface is typically not the gateway for the Guest subnet, as that resides on the VSPs in the server rooms. For example, the VSP Controllers 910 and 920 have the physical interface of 172.90.40.2 and .3 configured, and they share the virtual gateway IP of 40.1 between them. Therefore, the redundant EWCs' interfaces are configured as 40.5 and 40.6, respectively. Specify the IP of the redundant EWC's Guest IP in the Remote Settings field of each EWC.

- The Guest topology is configured as:
- Name: Guest
 - Mode: Bridge Traffic Locally at EWC
 - VLAN ID: 906 Tagged

• **WlessContr1:**

Topology: WlessContr1

Used by the EWC as the management interface, this topology corresponds to VLAN Wireless WlessContr1 (vid 998). The routing is done on the VSP switch.

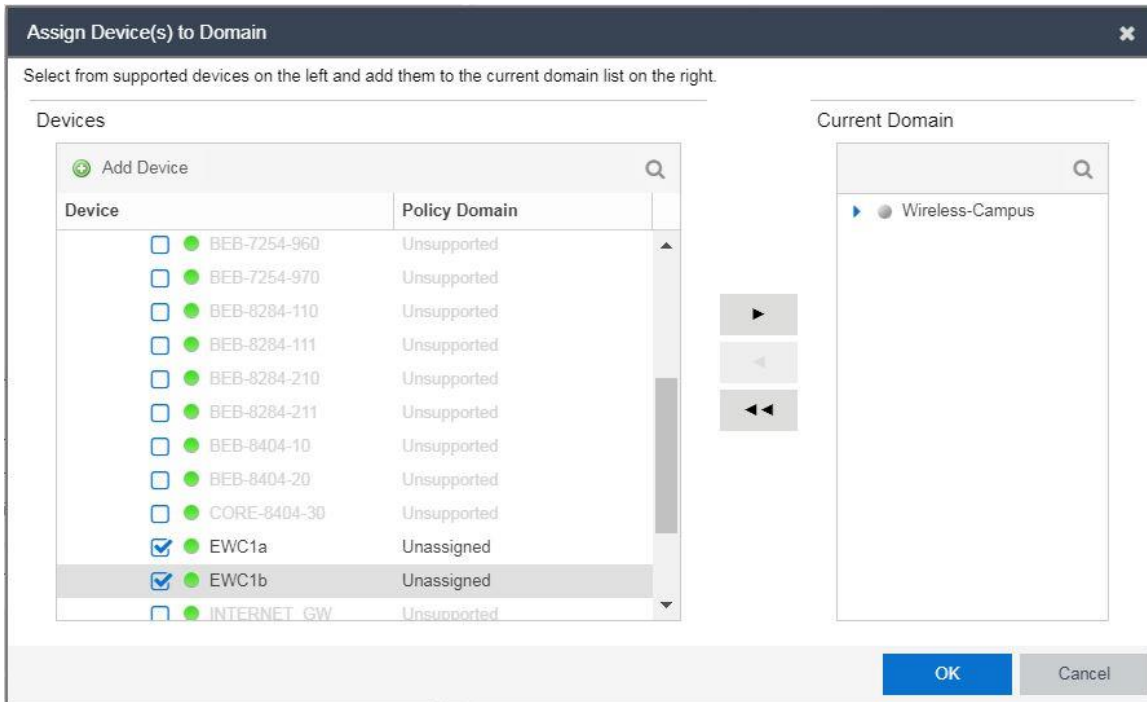
This VLAN is used as the mgmt. IP for the EWCs and AP discovery, as well as the tunnel endpoint for Guest traffic.

The WlessContr1 topology is configured as:

- Name: WlessContr1
- Mode: Physical
- VLAN: 998 Untagged

2. Enforce Policy Role Configuration:

The Roles are used for Access Control and will be enforced when ExtremeControl is configured. From **Control → Policy → Open Domain → Assign Devices to Domain**, add the EWCs to the **Wireless-Campus** policy domain:



- To verify the settings from Extreme Management Center after Policy Enforce completion, go to **VNS → Roles** and click on each role for detailed configuration:

Roles

Role Name	Action	Class of Service	Mode	Filter Defined
<input type="checkbox"/> Administrator	1050	No change	Fabric Attach	✓
<input type="checkbox"/> Campus User	1051	No change	Fabric Attach	✓
<input type="checkbox"/> Deny Access	Deny	No change	-	✓
<input type="checkbox"/> Guest-Access	Deny	No change	-	✓
<input type="checkbox"/> IoT Campus	1052	No change	Fabric Attach	✓
<input type="checkbox"/> Unregistered	Deny	No change	-	✓

New Delete Selected

The following roles were created in XMC and enforced to the controllers:

- **Administrator Role**

Role: Administrator

VLAN & Class of Service
Policy Rules

Core

Role Name:

Default Action

Access Control:

VLAN:

Default Class of Service:

Traffic Mirror:

Status

Synchronize: [synchronized]
Replicated when Synchronize Configuration is enabled

This role is applied to the Administrator users connecting to the network and is assigned to users authenticated as "Administrator". The access control is set to contain traffic to Administrator topology and to mark traffic with CoS priority 5.

Configure in the following manner:

- Role Name: Administrator
- Access Control: Containment VLAN
- VLAN: admin(1050)

Role: Administrator

VLAN & Class of Service
Policy Rules

Inherit filter rules from currently applied role i

Rules AP Filtering Custom AP Rules

Action	Name	Protocol	QoS	In	Out
Allow	00:54:01:00:00:00, 0.0.0.0/0	Any	RTP/Voice/Video	src	none
Allow	0.0.0.0/0:445	UDP	None	dest	none
Allow	0.0.0.0/0:389	UDP	None	dest	none
Allow	0.0.0.0/0:138 (Netbios Datagram Service)	UDP	None	dest	none
Allow	0.0.0.0/0:137 (Netbios Name Service)	UDP	None	dest	none
Allow	0.0.0.0/0:88	UDP	None	dest	none
Allow	0.0.0.0/0:67 (DHCP Server)	UDP	None	dest	none
Allow	0.0.0.0/0:53 (DNS)	UDP	None	dest	none
Allow	0.0.0.0/0:5060 (SIP)	TCP	RTP/Voice/Video	dest	none
Allow	0.0.0.0/0:3269	TCP	None	dest	none
Allow	0.0.0.0/0:3268	TCP	None	dest	none
Allow	0.0.0.0/0:636	TCP	None	dest	none
Allow	0.0.0.0/0:445	TCP	None	dest	none
Allow	0.0.0.0/0:389 (LDAP)	TCP	None	dest	none
Allow	0.0.0.0/0:139 (Netbios Session Service)	TCP	None	dest	none
Allow	0.0.0.0/0:137 (Netbios Name Service)	TCP	None	dest	none
Allow	0.0.0.0/0:88	TCP	None	dest	none
Allow	::/0	Any	RTP/Voice/Video	dest	none

* Multicast/Broadcast policy rules cannot be applied in the Out direction. Please use Topology Multicast Filters instead.

- Deny Access Role

Role: Deny Access

VLAN & Class of Service
Policy Rules

Core

Role Name:

Default Action

Access Control:

Default Class of Service:

Traffic Mirror:

HTTP Redirection

Redirection URL:

Note: token= <integer_val> & dest= <original_target_url> & hwcip= <hwc_ip> & hwcport= <hwc_port> will be APPENDED to the redirection URL

Status

Synchronize: [synchronized]
Replicated when Synchronize Configuration is enabled

This role is assigned to users who fail authentication. All traffic is dropped, except for the traffic explicitly allowed by the policy rules.

Configure in the following manner:

- Role Name: Deny Access
- Access Control: Deny
- Default CoS: No Change

Depending on the network's requirements, some traffic may need to be allowed by the **Deny Access** rule, whereas other networks require it to drop all traffic. The services allowed for this role can be defined in the Policy Rules section. All traffic except for the traffic explicitly allowed by the policy rules is dropped.

Role: Deny Access

VLAN & Class of Service
Policy Rules

Inherit filter rules from currently applied role 📌

Rules AP Filtering Custom AP Rules

Action	Name	Protocol	QoS	In	Out
Allow	0.0.0.0/0	Any	None	none	src

* Multicast/Broadcast policy rules cannot be applied in the Out direction. Please use Topology Multicast Filters Instead.

• **Campus User Role**

Role: Campus User

VLAN & Class of Service
Policy Rules

Core

Role Name:

Default Action

Access Control: ▼

VLAN: Edit New

Default Class of Service: Edit New

Traffic Mirror: ▼

Status

Synchronize: [synchronized]
Replicated when Synchronize Configuration is enabled

This role is assigned to users authenticated as Campus User. The access control is set to contain traffic to this topology.

Configure in the following manner:

- Role Name: Campus User
- Access Control: Containment VLAN
- VLAN: Campus User (1051)

Role: Campus User

VLAN & Class of Service
Policy Rules

Inherit filter rules from currently applied role ⓘ

AP Filtering Custom AP Rules

Rules

Action	Name	Protocol	QoS	In	Out
Allow	172.9.99.115/32:67	Any	None	dest	none
Allow	172.9.99.115/32:53	Any	None	dest	none
Allow	172.9.99.105/32:67	Any	None	dest	none
Allow	172.9.99.105/32:53	Any	None	dest	none
Deny	172.90.4.0/24	Any	None	dest	none
Deny	172.90.3.0/24	Any	None	dest	none
Deny	172.90.2.0/24	Any	None	dest	none
Deny	172.20.10.0/24	Any	None	dest	none
Deny	172.10.10.0/24	Any	None	dest	none
Deny	172.9.99.0/24	Any	None	dest	none
Deny	172.9.98.0/24	Any	None	dest	none
Deny	10.0.0.0/24	Any	None	dest	none
Deny	0.0.0.0/0:1813 (RADIUS Accounting)	UDP	None	src	none
Deny	0.0.0.0/0:1812 (RADIUS)	UDP	None	src	none
Deny	0.0.0.0/0:1433	UDP	None	src	none
Deny	0.0.0.0/0:67 (DHCP Server)	UDP	None	src	none
Deny	0.0.0.0/0:53 (DNS)	UDP	None	src	none
Allow	0.0.0.0/0:445	UDP	None	dest	none

* Multicast/Broadcast policy rules cannot be applied in the Out direction. Please use Topology Multicast Filters instead.

• Guest-Access Role

Role: Guest-Access

VLAN & Class of Service
Policy Rules

Core

Role Name:

Default Action

Access Control:

Default Class of Service:

Traffic Mirror:

Status

Synchronize: [synchronized]
Replicated when Synchronize Configuration is enabled

This role is assigned to users connecting to the network as guests through captive portal. Default Access Control is set to Deny for maximum security.

Configure in the following manner:

- Role Name: Guest-Access
- Access Control: Deny
- VLAN: Guest (906)

Role: Guest-Access

VLAN & Class of Service
Policy Rules

Inherit filter rules from currently applied role !

AP Filtering Custom AP Rules

Rules

Action	Name	Protocol	QoS	In	Out
Allow	0.0.0.0/0:67 (DHCP Server)	UDP	None	dest	none
Allow	0.0.0.0/0:53 (DNS)	UDP	None	dest	none
Allow	0.0.0.0/0:443 (HTTPS)	TCP	None	dest	none
Allow	0.0.0.0/0:80 (HTTP)	TCP	None	dest	none
Allow	0.0.0.0/0:0x0-FFFF	ICMP	None	dest	none
Allow	0x0806, ::/0	Any	None	dest	none
Allow	0.0.0.0/0	Any	None	none	src

* Multicast/Broadcast policy rules cannot be applied in the Out direction. Please use Topology Multicast Filters Instead.

IoT Campus Role

Role: IoT Campus

VLAN & Class of Service
Policy Rules

Core

Role Name:

Default Action

Access Control: Edit New

VLAN: Edit New

Default Class of Service: Edit New

Traffic Mirror:

Status

Synchronize: [synchronized]
Replicated when Synchronize Configuration is enabled

Advanced...

New
Delete
Save

This role is assigned to users and devices authenticating to the network as 'IoT'. Default Access Control is set containment to IoT Campus topology.

Configure in the following manner:

- Role Name: IoT Campus
- Access Control: Containment VLAN
- VLAN: Guest(1052)

Role: IoT Campus

VLAN & Class of Service
Policy Rules

Inherit filter rules from currently applied role !

AP Filtering Custom AP Rules

Rules

Action	Name	Protocol	QoS	In	Out
Deny	0.0.0.0/0:53 (DNS)	UDP	None	src	none
Allow	0.0.0.0/0:445	UDP	None	dest	none
Allow	0.0.0.0/0:389	UDP	None	dest	none
Allow	0.0.0.0/0:138 (Netbios Datagram Service)	UDP	None	dest	none
Allow	0.0.0.0/0:137 (Netbios Name Service)	UDP	None	dest	none
Allow	0.0.0.0/0:88	UDP	None	dest	none
Allow	0.0.0.0/0:67 (DHCP Server)	UDP	None	dest	none
Allow	0.0.0.0/0:53 (DNS)	UDP	None	dest	none
Deny	0.0.0.0/0:1433	TCP	None	src	none
Deny	0.0.0.0/0:162	TCP	None	src	none
Deny	0.0.0.0/0:161	TCP	None	src	none
Deny	0.0.0.0/0:80 (HTTP)	TCP	None	src	none
Deny	0.0.0.0/0:69	TCP	None	src	none
Deny	0.0.0.0/0:53	TCP	None	src	none
Deny	0.0.0.0/0:25 (SMTP)	TCP	None	src	none
Deny	0.0.0.0/0:23 (TELNET)	TCP	None	src	none
Deny	0.0.0.0/0:22 (SSH)	TCP	None	src	none
Deny	0.0.0.0/0:20 (FTP)	TCP	None	src	none

Add
Edit
Delete
Up
Down
Top
Bottom

* Multicast/Broadcast policy rules cannot be applied in the Out direction. Please use Topology Multicast Filters instead.

New
Delete
Save

• **Unregistered Role**

Role: Unregistered

VLAN & Class of Service
Policy Rules

Core

Role Name:

Default Action

Access Control:

Default Class of Service:

Traffic Mirror:

HTTP Redirection

Redirection URL:

Note: token= <integer_val> &dest= <original_target_url> &hwcpip= <hwc_ip> &hwcpport= <hwc_port> will be APPENDED to the redirection URL

Status

Synchronize: [synchronized]
Replicated when Synchronize Configuration is enabled

This is the initial role allocated to all wireless users attempting to join the Guest network. Users can move from this role to the Guest role through captive portal, or to Deny Access if authentication fails. A set of policies are configured to allow a user connecting to the network to obtain an IP address, to reach the DNS server, and to access the captive portal.

Configure in the following manner:

- Role Name: Unregistered
- Access Control: Deny

Role: Unregistered

VLAN & Class of Service
Policy Rules

Inherit filter rules from currently applied role ?

Rules AP Filtering Custom AP Rules

Action	Name	Protocol	QoS	In	Out
Allow	172.9.99.121/32:80	Any	None	dest	none
Allow	172.9.99.120/32:80	Any	None	dest	none
Allow	0.0.0.0/0:67 (DHCP Server)	UDP	None	dest	none
Allow	0.0.0.0/0:53 (DNS)	UDP	None	dest	none
Redirect	0.0.0.0/0:80 (HTTP)	TCP	None	dest	none
Allow	0x0806, ::/0	Any	None	dest	none
Allow	0.0.0.0/0	Any	None	none	src

* Multicast/Broadcast policy rules cannot be applied in the Out direction. Please use Topology Multicast Filters Instead.

3. WLAN Services Configuration

The RF configuration, authentication settings, and QoS attributes for a wireless network can be managed under a WLAN service. For the Automated Campus, three WLAN services are defined. The **AC-Guest** SSID, which uses the captive portal registration through policies enforced from Extreme Management Center, the **AC-Campus** SSID configured for 802.1X authentication, and an **AC-Open** SSID, which has authentication mode disabled, and uses MAC-based authentication.

- To Add a new WLAN service, go to **VNS → WLAN Services** and click **New**.

WLAN Services

Name	Type	Enabled	SSID	Privacy	Auth. Mode	Radio Mode
<input type="checkbox"/> AC-Campus	Standard	✓	AC-Campus	WPA	802.1x	g/a/n/ac
<input type="checkbox"/> AC-Guest	Standard	✓	AC-Guest	None	Firewall Friendly External	g/a/n/ac
<input type="checkbox"/> AC-Open	Standard	✓	AC-Open	None	Disabled	g/a/n/ac

Adding the first WDS/Mesh assignment or removing the last WDS/Mesh assignment will cause an AP to reboot.

- Configure **AC-Campus** WLAN service:

WLAN: AC-Campus

WLAN Services | Privacy | Auth & Acct | QoS

Core

Name: AC-Campus

Service Type: Standard

SSID: AC-Campus

Default Topology: Bridged at AP untagg...

Default CoS: No CoS

Default Traffic Mirror: * Enable both directions

Application Visibility:

Status

Synchronize: [synchronized]
Replicated when Synchronize Configuration is enabled

Enable:

* Traffic Mirror configure in WLAN service applied to tcp/udp only

This WLAN binds the AC-Campus SSID to the corresponding topology based on the client's 802.1X authentication credentials.

Configure in the following manner:

- Name: AC-Campus
- SSID: AC-Campus
- Default Topology: Bridged at AP untagged
- Default CoS: No CoS

WLAN: AC-Campus

WLAN Services	Privacy	Auth & Acct	QoS
<input type="radio"/> None <input type="radio"/> Static Keys (WEP) <input type="radio"/> Dynamic Keys (WEP) <input checked="" type="radio"/> WPA <input type="radio"/> WPA - PSK			
<input type="checkbox"/> WPA v.1 Encryption: TKIP only			
<input checked="" type="checkbox"/> WPA v.2 Encryption: AES only Key Management Options: None			
<input checked="" type="checkbox"/> Broadcast re-key interval: 3600 (30 - 86400 seconds)			
<input type="checkbox"/> Group Key Power Save Retry			
Management Frame Protection: Enabled			
<input type="checkbox"/> Fast Transition			
<small>Note: using WEP or WPAv1 privacy will limit 11n and 11ac performance to legacy AP rates.</small>			
New		Delete	
		Save	

WPA privacy is configured for this SSID.

Configure in the following manner:

- Select WPA radio button
- Select WPA v.2 checkbox
- Encryption: AES Only

WLAN: AC-Campus

WLAN Services	Privacy	Auth & Acct	QoS															
Authentication																		
Mode: 802.1x no HTTP Redirection Configure...																		
<input type="checkbox"/> Enable MAC-based authentication <input checked="" type="checkbox"/> Enable RADIUS Accounting																		
RADIUS Servers																		
<table border="1"> <thead> <tr> <th>Auth</th> <th>Accounting</th> </tr> </thead> <tbody> <tr> <td>Nac1</td> <td>Nac1</td> </tr> <tr> <td>Nac2</td> <td>Nac2</td> </tr> </tbody> </table>	Auth	Accounting	Nac1	Nac1	Nac2	Nac2	<table border="1"> <thead> <tr> <th>Select Radius</th> </tr> </thead> <tbody> <tr><td>New</td></tr> <tr><td>Move Up</td></tr> <tr><td>Move Down</td></tr> <tr><td>Configure</td></tr> <tr><td>Test</td></tr> <tr><td>Summary</td></tr> <tr><td>Remove</td></tr> <tr><td>Radius TLVs</td></tr> </tbody> </table>	Select Radius	New	Move Up	Move Down	Configure	Test	Summary	Remove	Radius TLVs		
Auth	Accounting																	
Nac1	Nac1																	
Nac2	Nac2																	
Select Radius																		
New																		
Move Up																		
Move Down																		
Configure																		
Test																		
Summary																		
Remove																		
Radius TLVs																		
<input checked="" type="checkbox"/> Collect Accounting Information of Wireless Controller																		
New		Delete																
		Save																

802.1X authentication is configured for the AC-Campus SSID. The two ExtremeControl engines are configured as the RADIUS servers on the EWC (which then use LDAP to query the actual server).

Configure in the following manner:

- Select 802.1X authentication mode
- Select no HTTP Redirection
- Select RADIUS Accounting checkbox
- Add ExtremeControl 1 and 2 for Authentication
- Add ExtremeControl 1 and 2 for Accounting
- Click "Radius TLVs" to configure.

RADIUS Access-Request Message Options [?] [X]

VSA's

Include the following Vendor-Specific-Attributes in RADIUS Requests:

<input type="checkbox"/> Ingress Rate Control	<input checked="" type="checkbox"/> VNS Name
<input type="checkbox"/> Egress Rate Control	<input checked="" type="checkbox"/> AP Name
<input checked="" type="checkbox"/> Topology Name	<input checked="" type="checkbox"/> SSID
<input checked="" type="checkbox"/> Role Name	<input checked="" type="checkbox"/> AP MAC

Optional TLVs

Include the following Standard-Attributes in RADIUS Requests:

Chargeable-User-Identity

Treat Access-Accept without Chargeable-User-Identity attribute as Access-Reject

Zone Support

RADIUS Request Called Station ID Options

Replace BSSID with Zone name

Replace BSSID with AP Ethernet MAC

Operator Name: Disabled ▼

OK Cancel

Select the Vendor-Specific-Attributes to be included in the Radius requests.

Click OK, then Save the VNS

- Configure **AC-Guest** WLAN service:

WLAN: AC-Guest

WLAN Services | Privacy | Auth & Acct | QoS

Core

Name: AC-Guest

Service Type: Standard

SSID: AC-Guest

Default Topology: Guest(906) ▼

Default CoS: No CoS ▼

Default Traffic Mirror: Enable both directions ▼

Application Visibility:

Status

Synchronize: [synchronized]
Replicated when Synchronize Configuration is enabled

Enable:

Wireless APs

Select APs: - ▼

Radio 1	Radio 2	Ports	AP Name
<input checked="" type="checkbox"/> a/n/ac	<input checked="" type="checkbox"/> g/n		Acc120-57AA58
<input checked="" type="checkbox"/> a/n/ac	<input checked="" type="checkbox"/> g/n		Acc120-E325B8[F]
<input checked="" type="checkbox"/> a/n/ac	<input checked="" type="checkbox"/> g/n	<input type="checkbox"/> p1	Acc121-257AAB
<input checked="" type="checkbox"/> off	<input checked="" type="checkbox"/> off		Acc121-31D79A[F]
<input checked="" type="checkbox"/> off	<input checked="" type="checkbox"/> off		Acc220-4FA926
<input checked="" type="checkbox"/> off	<input checked="" type="checkbox"/> off		Acc220-4FA9BC[F]
<input checked="" type="checkbox"/> off	<input checked="" type="checkbox"/> off		Acc221-4FA9B6
<input checked="" type="checkbox"/> a/n/ac	<input checked="" type="checkbox"/> g/n	<input type="checkbox"/> CAM	Acc221-7A04B7[F]

* Traffic Mirror configure in WLAN service applied to tcp/udp only

Advanced...

New Delete Save

This WLAN binds the AC-Guest SSID to the Guest topology and is intended to be used by Guest users connecting to the network. No privacy is provided, and access is through captive portal.

Configure in the following manner:

- Name: AC-Guest
- SSID: AC-Guest
- Default Topology: Guest(906)

WLAN: AC-Guest

Guest Access uses the captive portal through policies enforced from Extreme Management Center to initially register the device that is used to connect to the network. The Auth&Acct tab is configured in the following manner:

- Authentication mode: Firewall Friendly External*
- Enable MAC-based authentication checkbox
- Enable RADIUS Accounting checkbox
- Add ExtremeControl 1 and 2 for MAC-based
- Add ExtremeControl 1 and 2 for Accounting

*This mode allows for better compatibility with firewalls that ExtremeControl may be positioned behind.

- Configure **AC-Open** WLAN service:

WLAN: AC-Open

Radio 1	Radio 2	Ports	AP Name
<input checked="" type="checkbox"/> a/n/ac	<input checked="" type="checkbox"/> g/n		Acc120-57AA58
<input checked="" type="checkbox"/> a/n/ac	<input checked="" type="checkbox"/> g/n		Acc120-E325B8[F]
<input checked="" type="checkbox"/> a/n/ac	<input checked="" type="checkbox"/> g/n	<input type="checkbox"/> p1	Acc121-257AAB
<input checked="" type="checkbox"/> off	<input checked="" type="checkbox"/> off		Acc121-31D79A[F]
<input checked="" type="checkbox"/> off	<input checked="" type="checkbox"/> off		Acc220-4FA926
<input checked="" type="checkbox"/> off	<input checked="" type="checkbox"/> off		Acc220-4FA9BC[F]
<input checked="" type="checkbox"/> off	<input checked="" type="checkbox"/> off		Acc221-4FA9B6
<input checked="" type="checkbox"/> a/n/ac	<input checked="" type="checkbox"/> g/n	<input type="checkbox"/> CAM	Acc221-7A04B7[F]

This WLAN binds the AC-Open SSID to the corresponding topology based on the client's MAC authentication credentials.

Configure in the following manner:

- Name: AC-Open
- SSID: AC-Open
- Default Topology: Bridged at AP untagged
- Default CoS: No CoS

WLAN: AC-Open

WLAN Services
Privacy
Auth & Acct
QoS

Authentication

Mode: Disabled

Enable MAC-based authentication Configure...

Enable RADIUS Accounting

RADIUS Servers

MAC	+	Select Radius
Nac1		New
Nac2		Move Up
		Move Down
		Configure
		Test
		Summary
		Remove
		Radius TLVs

Collect Accounting Information of Wireless Controller

New
Delete
Save

MAC Authentication is configured for the AC-Open SSID. The two ExtremeControl engines are configured as the RADIUS servers on the EWC (which handle the MAC authentication via configured ExtremeControl rules).

Configure in the following manner:

- Select Disabled authentication mode
- Select Enable MAC-based

4. Site Configuration

- A site provides a way to group Roles, WLANs, and APs under one logical entity for easier management. For the Automated Campus solution, two sites were created based on location. To create a new site, go to **VNS** → **Sites** and click **New**.

Sites

Name	Local RADIUS	Band Pref.	Secure Tunnel	APs Assigned	WLANs Assigned
<input type="checkbox"/> Campus1	×	×	×	4	3
<input type="checkbox"/> Campus2	×	×	×	4	3

New
Delete Selected

- The Campus 1 site was configured as below. The Campus 2 site was configured the same way.

Site: Campus1

Configuration | AP Assignments | WLAN Assignments

Site Name:

Local Radius Authentication
Default DNS Server

Roles to download to member APs:

- Administrator
- Campus User
- Deny Access
- Guest-Access
- IoT Campus
- Unregistered

CoS to download to member APs:

- No CoS
- Network Management
- RTP/Voice/Video

Status

Synchronize: [synchronized]
Replicated when Synchronize Configuration is enabled

- All topologies are downloaded to APs at the site.
- DNS server only needs to be configured if RADIUS servers assigned are identified by DNS name

Advanced...

New Delete **Save**

All roles are selected to be downloaded to the APs connected to Campus 1.

Configure in the following manner:

- Site Name: Campus 1
- Uncheck the Local RADIUS Authentication checkbox
- Select all checkboxes: Roles to download to member APs

- On the **AP Assignments** tab, all APs physically connected to Campus 1 are selected:

Site: Campus1

Configuration | **AP Assignments** | WLAN Assignments

AP Name	
Acc120-57AA58	<input checked="" type="checkbox"/>
Acc120-E325B8[F]	<input checked="" type="checkbox"/>
Acc121-257AAB	<input checked="" type="checkbox"/>
Acc121-31D79A[F]	<input checked="" type="checkbox"/>
Acc220-4FA926*	<input type="checkbox"/>
Acc220-4FA9BC[F]*	<input type="checkbox"/>
Acc221-4FA9B6*	<input type="checkbox"/>
Acc221-7A04B7[F]*	<input type="checkbox"/>

* AP assigned to another site.

New Delete **Save**

These APs will have the same role and WLAN settings.

Configure in the following manner:

- Select checkboxes of desired APs in this campus site

- On the **WLAN Assignments** tab, select the WLAN services that are supposed to be accessible from Campus 1. This selection also enables the APs selected in the **AP Assignments** tab to advertise these WLANs:

Site: Campus1

WLAN Name	Airtime (%)	Radio 1	Radio 2	Ports
AC-Campus	-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> P1/CAM <input type="checkbox"/> P2 <input type="checkbox"/> P3
AC-Guest	-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> P1/CAM <input type="checkbox"/> P2 <input type="checkbox"/> P3
AC-Open	-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> P1/CAM <input type="checkbox"/> P2 <input type="checkbox"/> P3

- Configure in the following manner:
- Select AP Radio Checkboxes
 - Select AP Port Checkboxes

5. Virtual Network Services Configuration

The virtual network configuration binds together the WLANs and the roles, for access control. There are conceptually hierarchical dependencies on the configuration elements of a VNS and for service activation, all the pieces will need to be in place, or defined during VNS configuration.

- To create a new VNS entry, go to **VNS → Virtual Networks** and click **New**.

Defined VNS

VNS	Enabled	WLAN Service	Auth	Privacy	Def Role	Action	Mode
<input type="checkbox"/> AC-Campus	✓	AC-Campus	802.1x	WPA	Unregistered	Deny	-
<input type="checkbox"/> AC-Guest	✓	AC-Guest	FFECF	None	Unregistered	Deny	-
<input type="checkbox"/> AC-Open	✓	AC-Open	Disabled	None	Unregistered	Deny	-

The following virtual networks are configured for both Campuses:

VNS: AC-Campus

General

Core

VNS Name:

WLAN Service

WLAN Service:

Default Roles

Non-Authenticated:
Action:Deny Class of Service:No CoS

Authenticated:
Action:Deny Class of Service:No CoS

Status

Synchronize: [synchronized]
Replicated when Synchronize Configuration is enabled

Enable:

This VNS is bound to the AC-Campus WLAN. The default role for non-authenticated users can be set to Unregistered. After authentication, the role is assigned by ExtremeControl (via the Filter id field) and access control will be done on the switch because the topologies are set to Fabric Attach.

Configure in the following manner:

- VNS Name: AC-Campus
- WLAN Service: AC-Campus
- Non-Authenticated: Unregistered
- Authenticated: Same as non-auth
- **Enable Checkbox** Checked

VNS: AC-Guest

General

Core
VNS Name: AC-Guest

WLAN Service
WLAN Service: AC-Guest

Default Roles
Non-Authenticated: Unregistered
 Action:Deny Class of Service:No CoS
Authenticated: Guest-Access
 Action:Deny Class of Service:No CoS

Status
Synchronize: [synchronized]
 Replicated when Synchronize Configuration is enabled
Enable:

This VNS is bound to the AC-Guest WLAN. The default role for non-authenticated users is Unregistered. After users connect to captive portal, they are considered authenticated and ExtremeControl assigns the Guest Access role (via the Filter id field).

Configure in the following manner:

- VNS Name: AC-Guest
- WLAN Service: AC-Guest
- Non-Authenticated: Unregistered
- Authenticated: Guest Access
- **Enable** Checkbox Checked

VNS: AC-Open

General

Core
VNS Name: AC-Open

WLAN Service
WLAN Service: AC-Open

Default Roles
Non-Authenticated: Unregistered
 Action:Deny Class of Service:No CoS
Authenticated: <Same as non-authenticated>
 Action:Deny Class of Service:No CoS

Status
Synchronize: [synchronized]
 Replicated when Synchronize Configuration is enabled
Enable:

This VNS is bound to the AC-Open WLAN. The default role for non-authenticated users is Unregistered. After users MAC-authenticated, ExtremeControl assigns the corresponding role (via the Filter id field).

Configure in the following manner:

- VNS Name: AC-Open
- WLAN Service: AC-Open
- Non-Authenticated: Unregistered
- Authenticated: Same as non-auth
- **Enable** Checkbox Checked

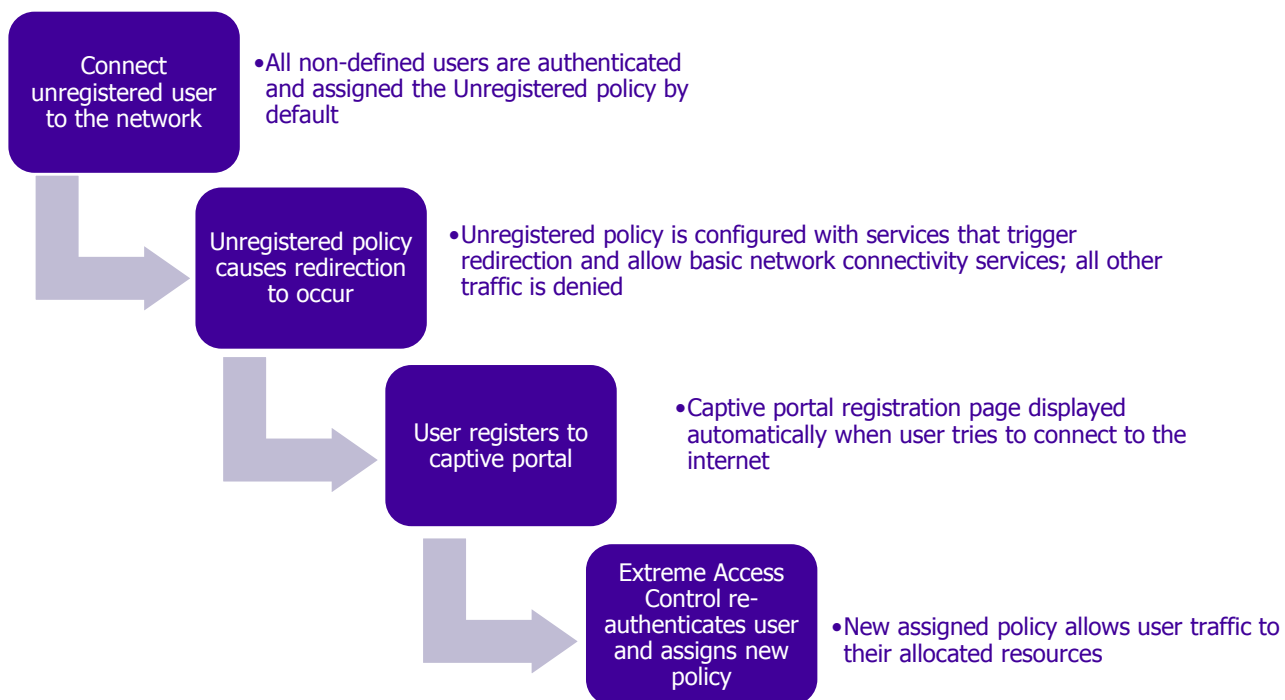
Guest Access (Captive Portal)

Captive portal provides a way to allow unregistered users to connect to the network as guests. All guests are redirected to a registration page before being allowed access.

In order for redirection to occur, the network must be able to identify a guest user's traffic and assign a policy that triggers the redirection. In this instance, traffic is assigned the "Unregistered" policy, configured to redirect web traffic to a specific URL where the policy is applied. The DNS, DHCP, ARP, and http/https redirect rules for the "Unregistered" Role are configured in Extreme Management Center via Policy, then enforced onto the corresponding platform.

When an unregistered user attempts to access the internet, the HTTP traffic is intercepted and redirected to the Extreme Access Control captive portal. In a wired environment, this is the physical switch port. In a wireless environment, this is either the AP or the controller, depending on the deployment. The user is then able to fill in the required information that will yield access to the network. Once the captive portal process is complete, the user is removed from the policy that triggered redirection and assigned a new policy to allow normal traffic flow.

General Flow required for captive portal redirection:



Wired User Access

With Fabric Connect and the Extreme Management appliances in place and configured, the access switches can now be deployed and provisioned to allow wired users to authenticate and access the network.

Summit Access Switch

The Summit access switches were used in separate stack formations in two campus segments. A variety of stack-heights were incorporated into the topology, connected to form a ring within each stack. Combining the switches in stack formation allowed for easier administration of the switches.

The stack operates as if it were a single switch with a single IP address and a single point of authentication. One switch – called the master switch – is responsible for running network protocols and managing the stack. The master runs ExtremeXOS software and maintains all the software tables for all the switches in the stack. All switches in the stack, including the master switch, are also referred to as nodes.

The nodes can be physically connected within a server rack to create a stack in one of two ways:

- Native Stacking - switches are connected using either designated Ethernet data ports or dedicated stacking connectors.
- Alternate Stacking - switches are connected using 10-Gbps Ethernet data ports that have been configured for stacking. These ports are located either on the switch itself or on option cards installed on the rear of the switch

Note that in this EVD, **Alternate Stacking in a ring topology** is used with 10-Gbps links connecting the individual switches to form a stack. The high-speed stacking links function like the backplane links of a chassis.

The procedure for creating a Summit access stack is outside the scope of this document. This information can be found in existing GTAC knowledgebase articles and other CLI documentation. The GTAC Knowledgebase documentation can be found at the following link below.

How to Create a Stack with Summit Switches

The resulting stack should appear similar to the output below.

```
Slot-1 Stack.1 # show stacking
Stack Topology is a Ring
Active Topology is a Ring
Node MAC Address      Slot  Stack State  Role      Flags
-----
*00:04:96:a0:ad:fe    1     Active       Master    CA-
 00:04:96:a0:ae:67    2     Active       Backup    CA-
 00:04:96:a1:bf:67    3     Active       Standby   CA-
* - Indicates this node
Flags: (C) Candidate for this active topology, (A) Active Node
      (O) node may be in Other active topology
(Software Update Required) Slot-1 Stack.2 #
```

A successfully configured stack will assign each switch within the stack a unique slot number and will be given one of three assignments: master, backup, or standby. Each stack only has one master and one backup but can have more than one standby. The backup node will take the place of the master node if the master node fails. A standby node will take the place of the backup node if the backup node becomes the master node.

In this EVD, the access switches are managed in-band via a static IP configured on the FA Management VLAN for each campus.

Summit Access Switch Provisioning/Fabric Attach

After the stacking configuration is complete, it is provisioned for user network access.

Warning

To avoid potential network issues, it's recommended to enter the base configuration below before connecting to the network.

- Before deploying, configure the access switch with basic commands to establish initial IP and SNMP connectivity to the XMC and allow network provisioning.

```

create vlan 100
configure vlan 100 ipaddress 172.10.10.11 255.255.255.0
enable ipforwarding vlan 100
configure iproute add default 172.10.10.1
enable sharing 1:50 grouping 1:50,2:50

config snmpv3 add user xmc_v3 authentication sha extreme11 privacy aes 128 extreme12extreme
config snmpv3 add group snmpv3group user xmc_v3 sec-model usm
config snmpv3 add access snmpv3group sec-model usm sec-level priv read-view defaultAdminView
write-view defaultAdminView notify-view defaultAdminView
configure snmpv3 add community "private" name "private" user "vlv2c_rw"
configure snmpv3 add community "public" name "public" user "vlv2c_ro"
enable snmp acc snmpv3

enable policy
save config
  
```

Configure the FA mgmt. VLAN, setting the IP address and gateway.

Configure uplink for static LAG.

Configure SNMPv3 parameters. Refer to **Design Considerations** for more information.

Enable policy to allow dynamic Role assignment upon authentication.

Note

For more information on the commands used below, including configuring an SNMPv3 profile in XMC, refer to **Design Considerations**

- Configure netlogin and network tools settings:

```

enable netlogin dot1x mac
configure netlogin authentication protocol-order dot1x mac web-based
enable netlogin ports 1:1-49,2:1-49,3:1-49 dot1x
enable netlogin ports 1:1-49,2:1-49,3:1-49 mac
configure netlogin add mac-list ff:ff:ff:ff:ff:ff 48

configure dns-client add name-server 172.9.99.105 vr VR-Default
configure dns-client add name-server 172.9.99.115 vr VR-Default

configure timezone name EST -300 autodst
configure snmp-client primary 134.141.79.190 vr VR-Default
configure snmp-client secondary 134.141.79.191 vr VR-Default
configure snmp-client update-interval 60
enable snmp-client
disable telnet
  
```

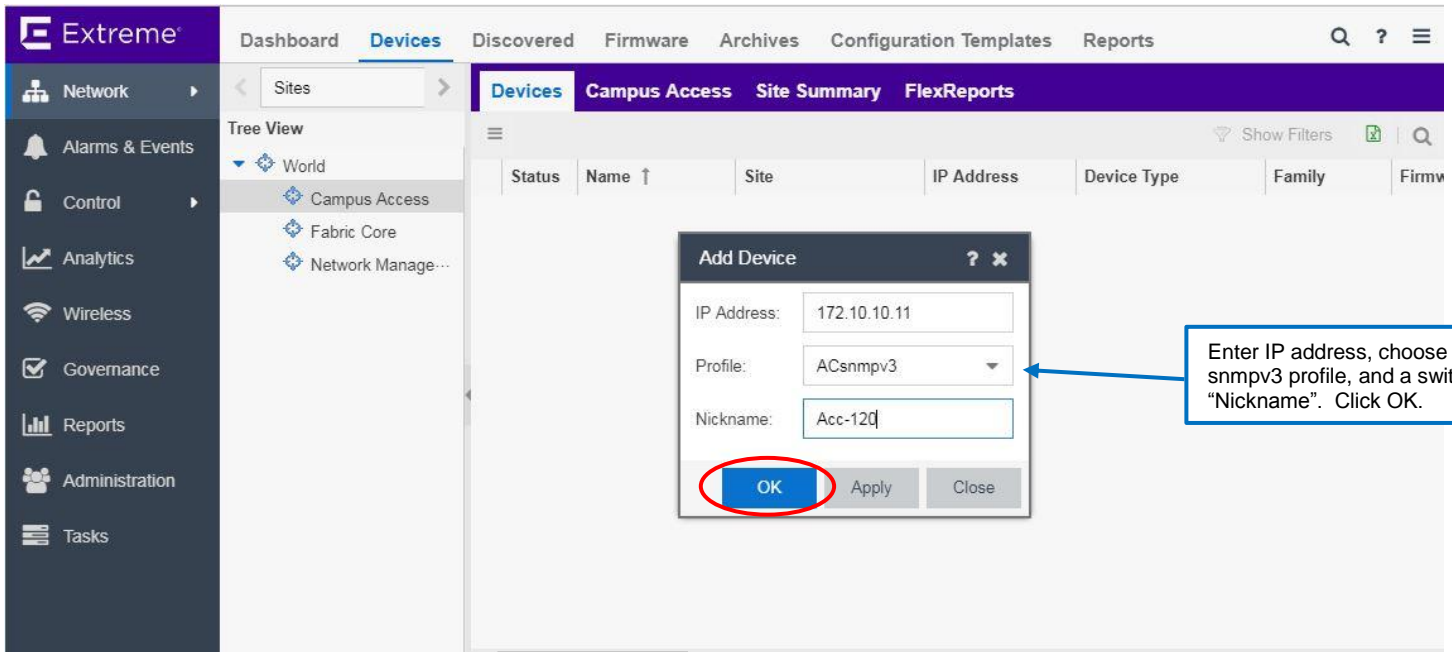
Configure netlogin authentication methods, enable on desired ports and set mac mask for MACAUTH.

Configure DNS and SNTP client parameters.

Disable telnet, then enable SSH2 to allow secure mgmt. login via ExtremeControl. NOTE: Enabling SSH will prompt a "yes" response.

```
enable ssh
yes
save config
```

- In XMC, under **Network→Devices**, right-click the **Campus Access** Site and choose **Add Device**:

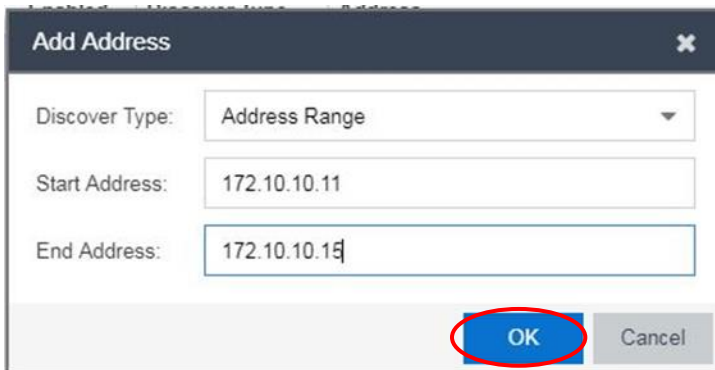


The screenshot shows the Extreme XMC interface. The left sidebar contains navigation options like Network, Alarms & Events, Control, Analytics, Wireless, Governance, Reports, Administration, and Tasks. The main area is titled 'Devices' and shows a table with columns for Status, Name, Site, IP Address, Device Type, Family, and Firmware. An 'Add Device' dialog box is open, displaying the following fields:

- IP Address: 172.10.10.11
- Profile: ACsnmpv3
- Nickname: Acc-120

The 'OK' button is circled in red. A callout box points to the Profile dropdown with the text: "Enter IP address, choose the snmpv3 profile, and a switch 'Nickname'. Click OK."

- Repeat this for any other deployed access switches in this Policy Domain.
 - To discover multiple access switches at once, an address range can be specified. Navigate to **Network→Devices→Sites→Campus Access→Discover**. Under **Addresses**, click **Add**:
 - Choose **Address Range** from the drop-down, and fill in parameters. Click **OK**:



The screenshot shows the 'Add Address' dialog box. The 'Discover Type' is set to 'Address Range'. The 'Start Address' is 172.10.10.11 and the 'End Address' is 172.10.10.15. The 'OK' button is circled in red.

- Under **Profiles**, check the desired SNMP profile to apply. Click Save, then Discover:

The screenshot shows the Extreme Networks management interface. The left sidebar contains navigation options like Network, Alarms & Events, Control, Analytics, Wireless, Governance, Reports, Administration, and Tasks. The main area is divided into several tabs: Dashboard, Devices, Discovered, Firmware, Archives, Configuration Templates, and Reports. Under the **Devices** tab, there are sub-tabs for **Campus Access**, **Site Summary**, and **FlexReports**. The **Discover** sub-tab is active, showing a table of discovered addresses and a list of profiles.

Addresses Table:

Enabled	Discover Type	Address
<input checked="" type="checkbox"/>	Address Range	172.10.10.11 - 172.10.10.15
<input checked="" type="checkbox"/>	Address Range	172.20.10.11 - 172.20.10.15

Profiles Table:

Accept	Name	Reject
<input type="checkbox"/>	BOSS_4800_v1_Profile	<input type="checkbox"/>
<input type="checkbox"/>	BOSS_v1_Profile	<input type="checkbox"/>
<input type="checkbox"/>	VOSS_v2_Profile	<input type="checkbox"/>
<input type="checkbox"/>	BOSS_ESM_v2_Profile	<input type="checkbox"/>
<input type="checkbox"/>	BOSS_4800_v2_Profile	<input type="checkbox"/>
<input type="checkbox"/>	BOSS_v2_Profile	<input type="checkbox"/>
<input type="checkbox"/>	v3_wireless	<input type="checkbox"/>
<input type="checkbox"/>	v3_analytics	<input type="checkbox"/>
<input type="checkbox"/>	snmpv3_ssh_Profile	<input type="checkbox"/>
<input type="checkbox"/>	v3_nac	<input type="checkbox"/>
<input checked="" type="checkbox"/>	ACsnmpv3	<input type="checkbox"/>
<input type="checkbox"/>	v3_test	<input type="checkbox"/>

At the bottom of the interface, there are buttons for **Discover**, **Configure Devices...**, **Scheduler...**, and **Save**.

- When Discover complete, click **Configure Devices**. Highlight each of the newly discovered switches, and give each a System Name and (under Device Annotation tab) a Nickname:

The screenshot shows the **Configure Device** dialog box. It has a table at the top listing discovered devices and tabs for **Device**, **Device Annotation**, **VLAN Definition**, **Ports**, and **Vendor Profile**. The **Device** tab is active, showing configuration fields for a selected device.

Device ID	System Name	Device Nickname	Device Type	Poll Type	Site	Firmware
172.10.10.11	Stack	Stack	EXOS Stack	SNMP	/World/Campus Access	22.6.1.4
172.20.10.11	Stack	Acc-220	EXOS Stack	SNMP	/World/Campus Access	22.6.1.4

Device Configuration Fields:

- System Name:
- Contact:
- Location:
- Administration Profile:
- Replacement Serial Number:
- Remove from Service:
- Default Site:
- Poll Group:
- Poll Type:
- SNMP Timeout:
- SNMP Retries:
- Topology Layer:

At the bottom, there are buttons for **Reload Device**, **Sync from Site**, **Enforce Preview...**, and **Cancel**.

Configure Device

Device ID	System Name	Device Nickname	Device Type	Poll Type	Site	Firmware
172.10.10.11	Acc-120	Acc-120	EXOS Stack	SNMP	/World/Campus Access	22.6.1.4
172.20.10.11	Stark	Acc-120	EXOS Stack	SNMP	/World/Campus Access	22.6.1.4

Device Annotation | VLAN Definition | Ports | Vendor Profile

Nickname:

Asset Tag:

User Data 1:

User Data 2:

Reload Device | Sync from Site | **Enforce Preview...** | Cancel

- Click **Enforce Preview**, then **Enforce** to apply these settings:

Compare Device Configuration

Enabled	IP Address	Site	Match				Status	
			System	VLAN Definition	Port Alias	Port VLAN	Action	Progress
<input checked="" type="checkbox"/>	172.10.10.11	/World/Campus Access	✓	✓	✓	✗	Enforce Success	100
<input checked="" type="checkbox"/>	172.20.10.11	/World/Campus Access	✓	✗	✓	✗	Enforce No Cha...	100
<input checked="" type="checkbox"/>	172.10.10.12	/World/Campus Access	✓	✗	✓	✗	Enforce Success	100

Enforce Options: System VLAN Definition Port Alias Port VLAN

Device | VLAN Definitions | Ports

	Desired	Current
sysName	Acc-120	✓ Acc-120
sysContact	support@extremenetworks.com, +1 888 257 30...	✓ support@extremenetworks.com, +1 888 257 30...
sysLocation		✓

Refresh | **Enforce** | Cancel

- Navigate to **Control** → **Policy**, and Open the “**Wired-Campus1**” policy domain:

Extreme

Dashboard | **Policy** | Access Control | End-Systems

Open/Manage Domain(s) | Global Domain Settings

Open Domain

- Clear Domain
- Default Policy Domain
- Wired-Campus1**
- Wired-Campus2
- Wireless-Campus

Lock Domain

Save Domain

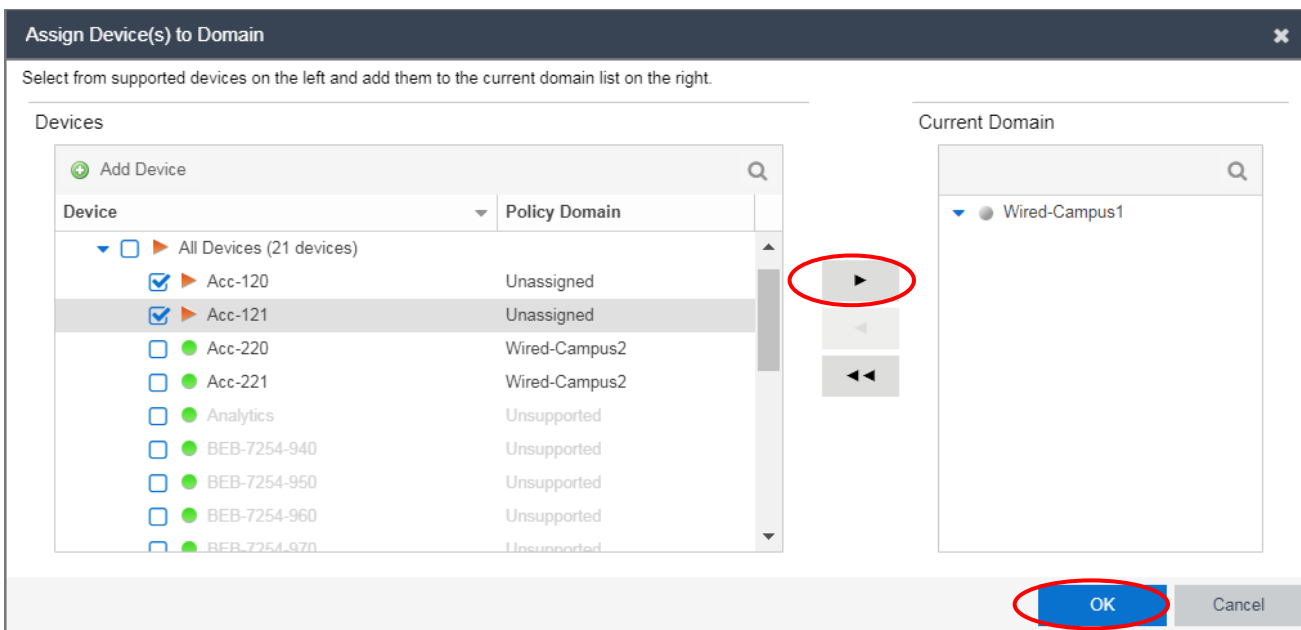
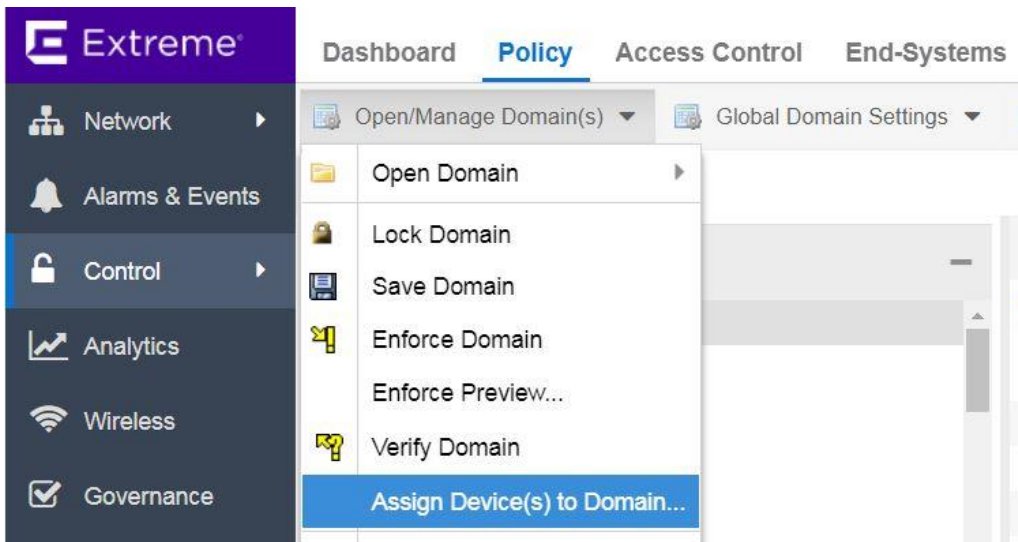
Enforce Domain

Enforce Preview...

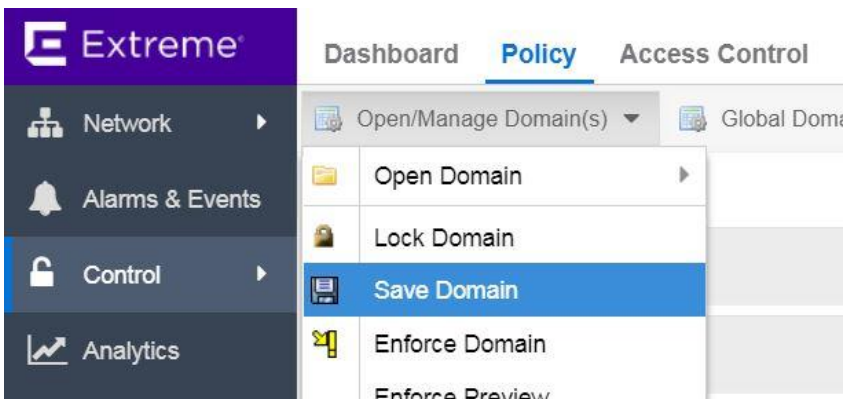
Verify Domain

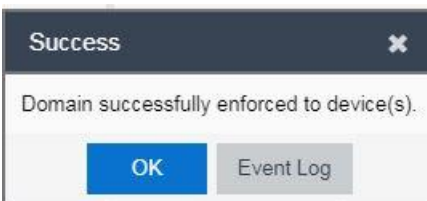
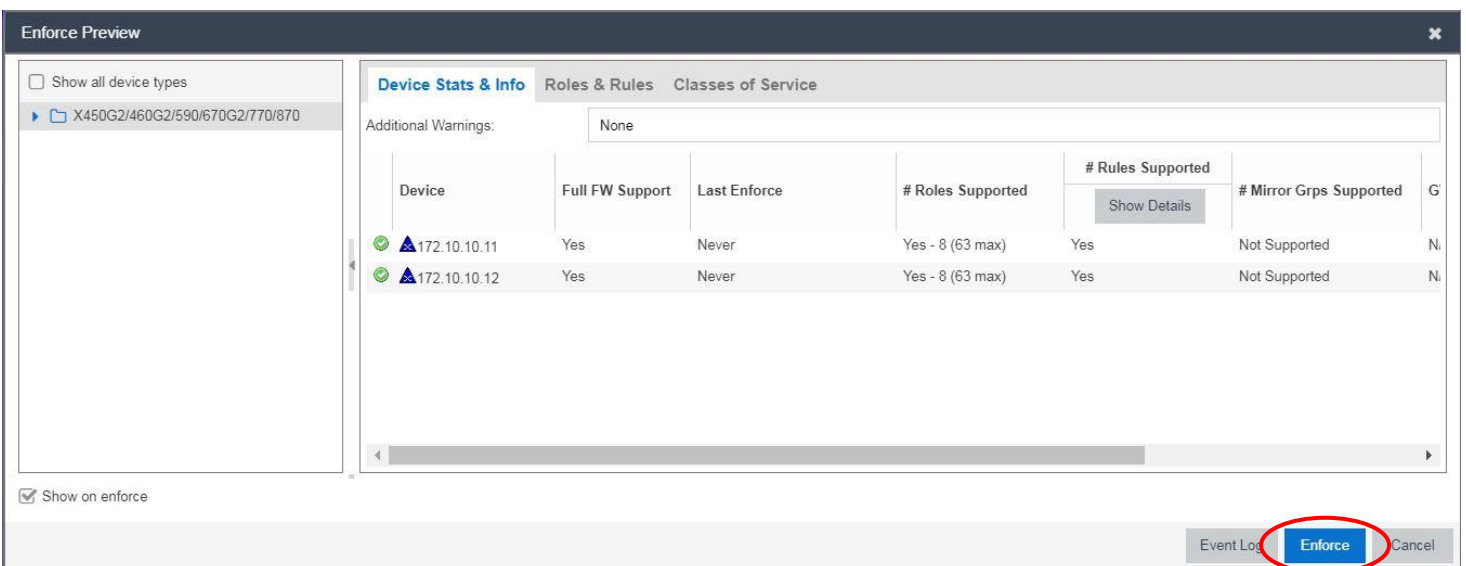
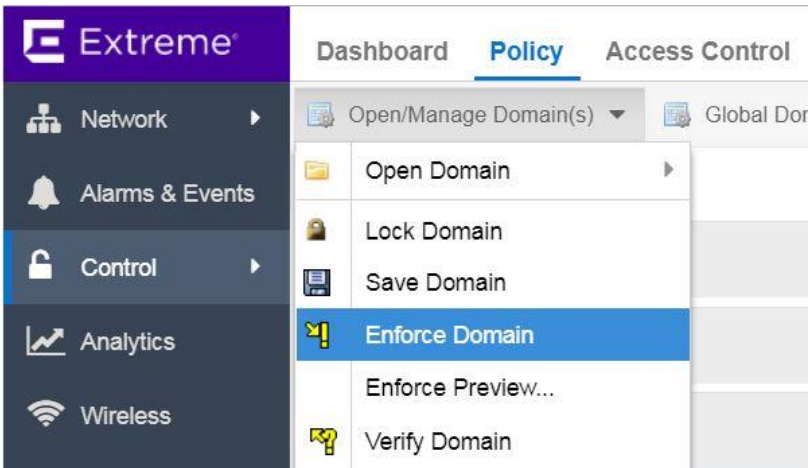
Assign Device(s) to Domain...

- Add the access switch(s) provisioned in Campus 1 from the left column to the policy domain, and click **OK**:



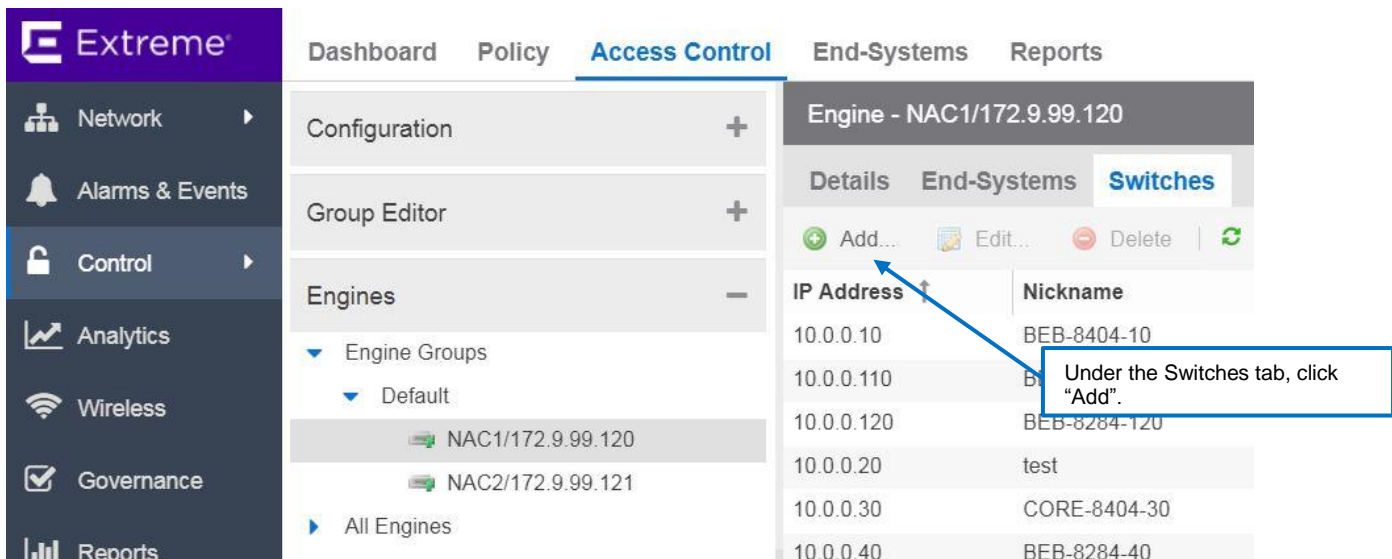
- Once added, **Save Domain**, and then enforce/sync the current policy profiles to the switches in this wired policy domain:



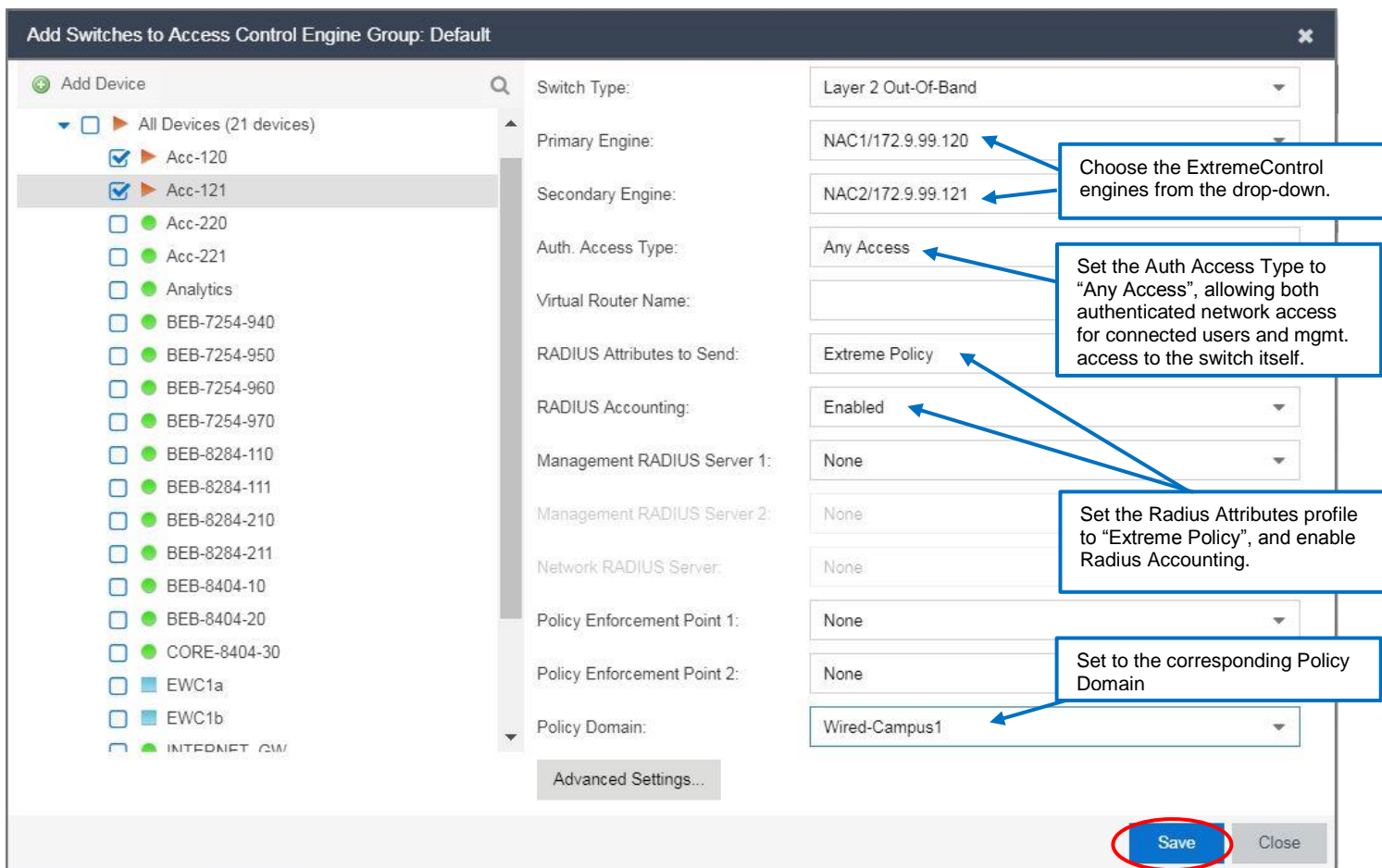


- Repeat the previous steps to add newly deployed Summit switches to other Campus Policy Domain(s).

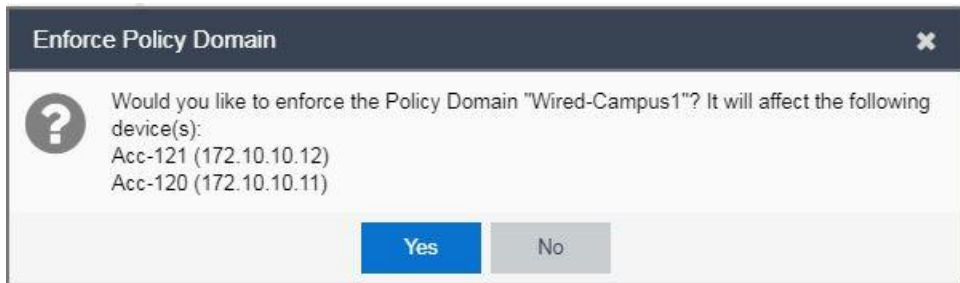
- Click on the **Access Control** tab and add the switch to the ExtremeControl engines:



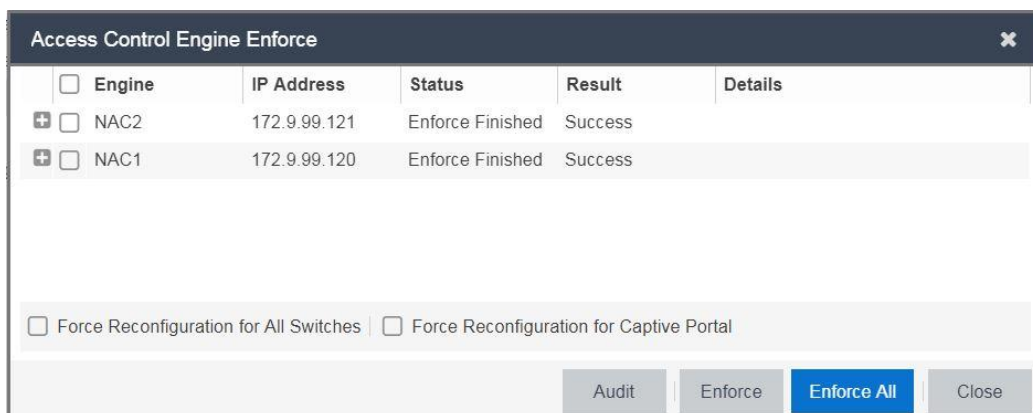
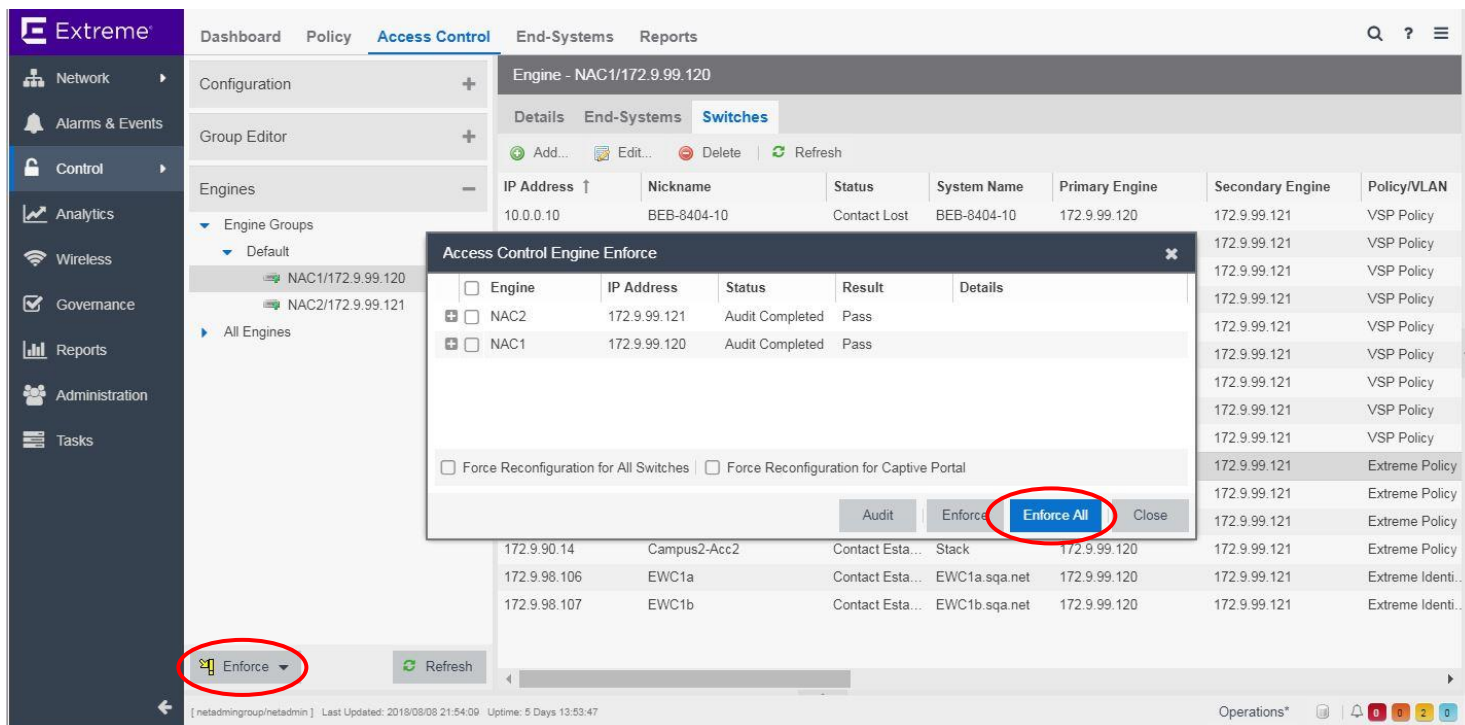
- Enter the ExtremeControl parameters for the switch, and click **Save**:



- Upon prompt to enforce the domain to the new switch(es), click **Yes**:



- Click **“Enforce”** at the bottom left of the screen to enforce the current rule base to the ExtremeControl Engine:



- Verify that the Fabric Attach Mgmt VLAN (from the FA Server) was assigned to the access switch:

```
(Private) Slot-1 Stack.2 # show fabric attach element
Fabric Attach Mode: Proxy
```

System Id	Port	Type	Mgmt VLAN	Auto Tag	Provision
00-bb-00-01-10-11-30-02-00-02	1:50	Server (No Auth)	100	Mix	Disabled
00-bb-00-01-10-11-30-02-00-02	2:50	Server (No Auth)	100	Mix	Disabled

```
(Private) Slot-1 Stack.3 #
```

- Upon connection, wired user traffic will be authenticated via ExtremeControl, and the corresponding Role will be sent to the access switch. The access switch will assign that role to the end user via netlogin:

```
(Private) Slot-1 Stack.4 # show netlogin session port 1:3
Multiple authentication session entries
```

Port	: 1:3	Station address	: 00:41:01:00:01:cd
Auth status	: success	Last attempt	: Wed Aug 22 20:53:04 2018
Agent type	: mac	Session applied	: true
Server type	: radius	VLAN-Tunnel-Attr	: None
Policy index	: 1	Policy name	: IoT Campus (active)
Session timeout	: 0	Session duration	: 0:03:37
Idle timeout	: 300	Idle time	: 0:00:00
Auth-Override	: disabled	Termination time	: Not Terminated

- The policy profile is assigned, along with its corresponding parameters:

```
Slot-1 Stack.10 # show policy profile 1
Profile Index :1
Profile Name :IoT Campus
Row Status :active
Port VID Status :enabled
Port VID Override :101
CoS Status :enabled
CoS :0
Web Redirect Index :0
Disable ingress port :disabled
Replace TCI Status :disabled
Auth Override Status :disabled
NSI :1010101
Tagged Egress :
Untagged Egress :101
Forbidden Egress :
Rule Precedence :1-2,10,12-19,23,20-22,25,31
:MACSource (1), MACDest (2), IPv6Dest (10),
:IPSource (12), IPDest (13), IPFrag (14),
:UDPSrcPort (15), UDPDestPort (16), TCPSrcPort (17),
:TCPDestPort (18), ICMPType (19), ICMP6Type (23),
:TTL (20), IPTOS (21), IPProto (22), Ether (25),
:Port (31)
Admin Profile Usage :none
Oper Profile Usage :1:3
Dynamic Profile Usage :1:3
```

- Verification via ExtremeControl: **Navigate to Control → End Systems**

...	Last Seen ↓	IP Ad...	MAC Address	MAC ...	Host Na...	Devi...	Device...	User...	Switch IP	Switch Nickn...	Switch Port	Policy	Authorization	Risk	Profile
✓	2018/08/22 20:55:16		00:41:01:00:01:CD						172.10.10.11	Acc-120	1:3	IoT Campus	Filter-Id='Ent...		IoT Campus Pro...

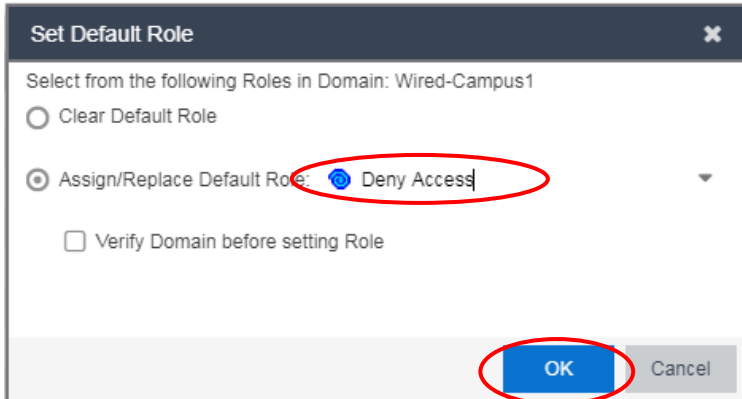
Default Role

A Default Policy role can be applied to wired ports. This can be useful if the authenticated user is assigned an unknown or invalid role, the NAC is unreachable during authentication, or a user fails authentication to an assigned Accept Policy. A Default Role is generally restrictive in nature, but will vary depending on the security requirements of the network.

A Default Role can be applied at the port or switch level on Summit access switches:

ExtremeControl interface showing the configuration page for a domain. The 'Ports' tab is selected, and a list of ports is shown. A red circle highlights the 'Set Default Role...' button next to the 'Acc-120' device.

Policy Manager will prompt to skip applying this role to interswitch ports and ports where Access Points are detected. This is recommended.



Policy Manager will prompt to skip applying this role to interswitch ports and ports where Access Points are detected. This is recommended.



ERS Access Switch

The ERS access switches were used in two separate stack formations in Campus 3. These are both 3-switch stacks connected to form a ring within each stack. Combining the switches in stack formation allowed for easier administration of the switches.

The stack operates as if it were a single switch with a single IP address and a single point of authentication. One switch – called the Base switch – is responsible for running network protocols and managing the stack. The Base runs BOSS software and maintains all the software tables for all the switches in the stack. All switches in the stack, including the Base switch, are also referred to as units.

The procedure for creating an ERS access stack is outside the scope of this document. This information can be found in existing GTAC knowledgebase articles and other CLI documentation. The ERS documentation can be found at the following link below.

[How to Create a Stack with ERS Switches](#)

The resulting stack should appear similar to the output below.

```
5900_STACK#show stack health
```

```
-----
UNIT#           Switch Model      Cascade Up      Cascade Down
-----
1 (Base)        5928GTS-uPWR      OK              OK
2               5928GTS-uPWR      OK              OK
3               5928GTS-uPWR      OK              OK
-----
```

```
Switch Units Found = 3
Stack Health Check = OK - RESILIENT
Stack Diagnosis = Stack in full resilient mode.
```

A successfully configured stack will assign each switch within the stack a unique unit number and one will be given one of three assignments: master, backup, or standby. Each stack only has one master and one backup but can have more than one standby. The backup node will take the place of the master node if the master node fails. A standby node will take the place of the backup node if the backup node becomes the master node.

In this EVD, the access switches are managed in-band via a static IP configured on the FA Management VLAN for each campus.

ERS Access Switch Provisioning/Fabric Attach

After the stacking configuration is complete, it is provisioned for user network access.

Warning

To avoid potential network issues, it's recommended to enter the base configuration below before connecting to the network.

Note

For more information on the commands used below, including configuring an SNMPv3 profile in XMC, refer to [Design Considerations](#)

- Before deploying, configure the access switch to establish initial IP connectivity and FA functionality to the XMC and allow network provisioning.

```

ip default-gateway 172.30.10.1
ip address stack 172.30.10.12
ip address source configured-address
telnet-access disable
ssh

mlt 1 name "Trunk #1" enable member 1/25,2/25

no fa message-authentication 1/ALL,2/ALL,3/ALL
fa zero-touch-option auto-port-mode-fa-client client-type 6-7
fa zero-touch-option auto-trusted-mode-fa-client client-type 6-7

interface ethernet 2/22
spanning-tree mstp edge-port true
exit

vlacp enable
interface Ethernet ALL
vlacp port 1/25,2/25 timeout short
vlacp port 1/25,2/25 timeout-scale 5
exit

logging remote address 172.9.99.119
logging remote enable
logging remote facility local4

snmp server primary address 134.141.79.190
snmp server secondary address 134.141.79.191
snmp enable
snmp sync-interval 1
clock source snmp
clock time-zone EST -5

```

Configure the IP, and default gateway. Disable Telnet and enable SSH.

Configure the MLT trunk ports connecting to the BEBs.

Configure FA options to allow APs to connect as trusted clients (wap-type 1 / 2).

Configure interfaces APs will be connected to with the "edge-port" option set to "true", indicating MSTP edge-port status.

Enable VLACP to allow for fast failover, and configure the MLT trunk ports

Configure syslog commands pointed to XMC, and SNMP configuration.

- Enter RADIUS configuration:

```

radius server host 172.9.99.120 key acct-enable
<shared secret>
<shared secret>
radius server host 172.9.99.121 secondary
radius server host 172.9.99.120 key used-by eapol acct-enable
<shared secret>
<shared secret>
radius server host 172.9.99.121 secondary used-by eapol
radius server host 172.9.99.120 key used-by non-eapol acct-enable
<shared secret>
<shared secret>
radius server host 172.9.99.121 secondary used-by non-eapol
radius-server encapsulation ms-chap-v2
radius-server password fallback

cli password telnet radius
cli password serial radius

```

Configure RADIUS host for mgmt. access login, specifying ExtremeControl IP addresses. When prompted, enter/confirm the RADIUS shared secret.

Configure the same parameters for dot1x (eapol) and MACauth (non-eapol).

Enable encryption of RADIUS packets.

Enable password authentication for telnet/SSH/serial.

- Configure the SNMPv3 configuration:

```
snmp-server name "Acc-321"
snmp-server view snmpView +1.3
snmp-server view adminView +1.3
snmp-server user xmc_v3 sha aes read-view adminView write-view adminView notify-view adminView
<SHA password>
<SHA password>
<AES password>
<AES password>

snmp-server user engine-id 80:00:1f:88:80:c5:04:f2:24:d6:ac:d0:5a xmc_v3 sha aes
<SHA password>
<SHA password>
<AES password>
<AES password>

snmp-server host 172.9.99.119 port 162 v3 auth-priv "xmc_v3" inform
```

Use the SHA and AES passphrases to match XMC's SNMP profile.

Configure the SNMP engine-id, providing the SHA and AES passphrases. See SNMP Design Considerations on where to retrieve the engine-id.

Set the SNMP Trap target to the XMC.

- Configure Extensible Authentication Protocol over LAN (EAPOL) settings:

```
eapol multivlan auto-config port 1/3,3/1,3/3,3/16
interface Ethernet ALL
eapol multihost eap-mac-max 32 non-eap-mac-max 32 mac-max 64
exit
eapol enable
save config
```

Enable authentication for eap and non-eap users on desired ports.

Save the configuration.

- In XMC, under **Network**→**Devices**, right-click the **Campus Access Site** and choose **Add Device**:

The screenshot shows the Extreme XMC interface. The left sidebar contains navigation menus for Network, Alarms & Events, Control, Analytics, Wireless, Governance, Reports, Administration, and Tasks. The main area displays a 'Devices' table with columns for Status, Name, Site, IP Address, Poll Status, and Poll De. A table with 6 rows is visible, showing devices like Acc-120, Acc-121, Acc-220, and others. An 'Add Device' dialog box is open, showing the following fields:

- IP Address: 172.30.10.12
- Profile: ACsnmpv3
- Nickname: Acc-321

The 'OK' button is circled in red. A callout box points to the IP Address field with the text: "Enter IP address, choose the snmpv3 profile, and a switch 'Nickname'. Click OK."

- Repeat this for any other deployed access switches in this campus.

- To discover multiple access switches at once, an address range can be specified. Navigate to **Network**→**Devices**→**Sites**→**Campus Access**→**Discover**. Under **Addresses**, click **Add**:
- Choose **Address Range** from the drop-down, and fill in parameters. Click **OK**:

Add Address
✕

Discover Type:

Start Address:

End Address:

OK
Cancel

- Under **Profiles**, check the desired SNMP profile to apply. Click Save, then Discover:

The screenshot shows the Extreme Networks GUI with the following configuration:

Addresses Table:

Enabled	Discover Type	Address
<input checked="" type="checkbox"/>	Address Range	172.30.10.11 - 172.30.10.15
<input checked="" type="checkbox"/>	Address Range	172.10.10.11 - 172.10.10.15
<input checked="" type="checkbox"/>	Address Range	172.20.10.11 - 172.20.10.15

Profiles Table:

Accept	Name	Reject
<input type="checkbox"/>	BOSS_ESM_v2_Profile	<input type="checkbox"/>
<input type="checkbox"/>	BOSS_4800_v2_Profile	<input type="checkbox"/>
<input type="checkbox"/>	BOSS_v2_Profile	<input type="checkbox"/>
<input type="checkbox"/>	v3_wireless	<input type="checkbox"/>
<input type="checkbox"/>	v3_analytics	<input type="checkbox"/>
<input type="checkbox"/>	snmpv3_ssh_Profile	<input type="checkbox"/>
<input type="checkbox"/>	v2_nac	<input type="checkbox"/>
<input checked="" type="checkbox"/>	ACsnmpv3	<input type="checkbox"/>
<input type="checkbox"/>	v3_test	<input type="checkbox"/>

Buttons at the bottom: Discover, Configure Devices..., Scheduler..., Save

- When Discover complete, click **Configure Devices**. Highlight each of the newly discovered switches, and give each a System Name and (under Device Annotation tab) a Nickname:

Configure Device

Device ID ↑	System Name	Device Nickname	Device Type	Poll Type	Site	Firmware
172.30.10.11	ERS-4900	Acc-320	ERS4950GTS-PWR+	SNMP	/World/Campus Access	v7.6.1.0:
172.30.10.12	ERS-5900	Acc-321	ERS5928GTS-UPWR	SNMP	/World/Campus Access	v7.6.1.0:

Device Annotation

System Name: **ERS-4900** Default Site: /World/Campus Acce

Contact: Poll Group: Default

Location: Poll Type: SNMP

Administration Profile: ACsnmpv3 SNMP Timeout: 5

Replacement Serial Number: SNMP Retries: 3

Remove from Service: Topology Layer: L2 Access

Reload Device Sync from Site Enforce Preview... Cancel

Configure Device

Device ID ↑	System Name	Device Nickname	Device Type	Poll Type	Site	Firmware
172.30.10.11	4900_STACK	4900_STACK	ERS4950GTS-PWR+	SNMP	/World/Campus Access	v7.6.1.033
172.30.10.12	5900_STACK	5900_STACK	ERS5928GTS-UPWR	SNMP	/World/Campus Access	v7.6.1.033

Device Annotation

Nickname: **Acc-320**

Asset Tag: <Different>

User Data 1: <Different>

User Data 2: <Different>

- Click **Enforce Preview**, then **Enforce** to apply these settings:

Compare Device Configuration

Enabled	IP Address	Site	Match				Status	
			System	VLAN Definition	Port Alias	Port VLAN	Action	Progress
<input checked="" type="checkbox"/>	172.30.10.12	/World/Campus Access	✓	✗	✓	✗	Enforce Success	100
<input checked="" type="checkbox"/>	172.30.10.11	/World/Campus Access	✓	✓	✓	✓	Enforce Success	100

Enforce Options: System VLAN Definition Port Alias Port VLAN

Device VLAN Definitions Ports

	Desired		Current
sysName	ERS-5900	✓	ERS-5900
sysContact		✓	
sysLocation		✓	

- Click on the **Access Control** tab and add the switch to the ExtremeControl engines:

The screenshot shows the Extreme Networks interface with the 'Access Control' tab selected. The 'Engines' section is expanded to show 'Default' engine groups, with 'NAC1/172.9.99.120' selected. The 'Switches' sub-tab is active, displaying a table of switches. A blue callout box points to the 'Add...' button in the top left of the switches table, with the text 'Under the Switches tab, click "Add".'

IP Address	Nickname
10.0.0.10	BEB-8404-10
10.0.0.110	BEB-8404-110
10.0.0.120	BEB-8284-120
10.0.0.20	test
10.0.0.30	CORE-8404-30
10.0.0.40	BEB-8284-40

- As the ERS access switches use RADIUS Attributes instead of Extreme Policy, an Attributes configuration file needs to be created that can be applied to all future-deployed ERS switches. Enter the ExtremeControl parameters for the switch, and click **Save**:

The screenshot shows the 'Add Switches to Access Control Engine Group: Default' dialog box. The 'Switch Type' is set to 'Layer 2 Out-Of-Band'. The 'Primary Engine' is 'NAC1/172.9.99.120' and the 'Secondary Engine' is 'NAC2/172.9.99.121'. The 'RADIUS Attributes to Send' dropdown is open, showing 'New...' selected. A blue callout box points to the 'New...' option with the text 'Choose New under the RADIUS Attributes to Send.'

Choose the ExtremeControl engines from the drop-down.

Choose **New** under the **RADIUS Attributes to Send**.

- Configure a name for the Attributes Configuration file.

The screenshot shows the 'Add RADIUS Attribute Configuration' dialog box. The 'Name' field contains 'Extreme ERS - Fabric Attach'. The 'Enable Port Link Control' checkbox is unchecked. The 'Attributes' dropdown menu is open, displaying three options: 'FA-VLAN-Create' (highlighted in blue), 'FA-VLAN-ISID', and 'FA-VLAN-PVID'. The 'Substitutions' dropdown is currently empty. A blue callout box with an arrow pointing to the 'FA-VLAN-Create' option contains the following text: 'Choose the FA-VLAN-Create attribute from the drop-down. Then under Substitutions, choose Custom 1. This attribute will instruct the ERS to create VLANs upon successful authentication.'

- Choose **FA-VLAN-ISID** for the next attribute. Under Substitutions, choose **VLAN_ID**. Enter a colon (":"), then choose the **CUSTOM2** substitution (%VLAN_ID%:%CUSTOM2%):

The screenshot shows the 'Add RADIUS Attribute Configuration' dialog box. The 'Name' field contains 'Extreme ERS - Fabric Attach'. The 'Enable Port Link Control' checkbox is unchecked. The 'Attributes' dropdown is set to 'FA-VLAN-ISID'. The 'Substitutions' dropdown is set to 'VLAN_ID'. The 'Attributes' field contains the text: 'FA-VLAN-Create=%CUSTOM1%' and 'FA-VLAN-ISID=%VLAN_ID%:'. The 'Substitutions' dropdown menu is open, displaying several options: 'CLI_AUTH', 'CUSTOM1', 'CUSTOM2' (highlighted in blue), 'CUSTOM3', 'CUSTOM4', 'CUSTOM5', 'Per-User ACL Cisco', 'Per-User ACL HP', and 'Per-User ACL Generic'. A blue callout box with an arrow pointing to the 'CUSTOM2' option contains the following text: 'This attribute will allow the corresponding VLAN id and I-SID value to be assigned upon successful authentication.'

- Choose **FA-Client-Trust**, then **CUSTOM3** for the Substitution:

Add RADIUS Attribute Configuration

Name: Extreme ERS - Fabric Attach

Enable Port Link Control:

Attributes : FA-Client-Trust Substitutions : CUSTOM3

FA-VLAN-Create=%CUSTOM1%
FA-VLAN-ISID=%VLAN_ID%:%CUSTOM2%
FA-Client-Trust=%CUSTOM3%

Save Close

- Finally, add the **Service_Type** attribute, with the **MGMT_SERV_TYPE** substitution. Click **Save**:

Edit RADIUS Attribute Configuration

Name: Extreme ERS - Fabric Attach

Enable Port Link Control:

Attributes : Substitutions :

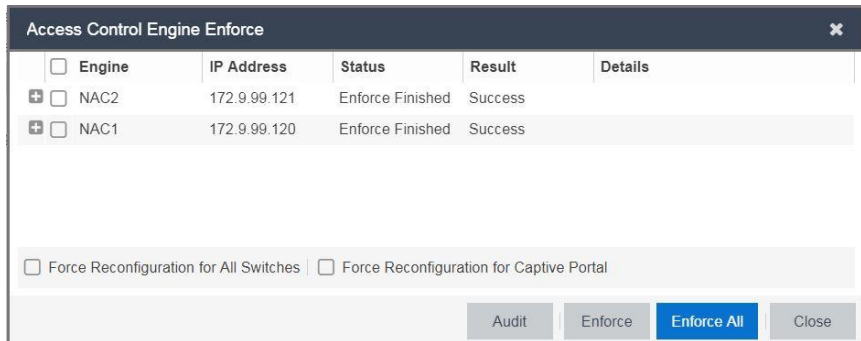
FA-VLAN-Create=%CUSTOM1%
FA-VLAN-ISID=%VLAN_ID%:%CUSTOM2%
FA-Client-Trust=%CUSTOM3%
Service-Type=%MGMT_SERV_TYPE%

Save Close

- Finish the remaining config parameters for adding the switch to ExtremeControl:

- Click **“Enforce”** at the bottom left of the screen to enforce the current rule base to the ExtremeControl Engine:

IP Address	Nickname	Status	System Name	Primary Engine	Secondary Engine	Policy/VLAN
10.0.0.10	BEB-8404-10	Contact Lost	BEB-8404-10	172.9.99.120	172.9.99.121	VSP Policy
172.9.99.121				172.9.99.121	172.9.99.121	VSP Policy
172.9.99.121				172.9.99.121	172.9.99.121	VSP Policy
172.9.99.121				172.9.99.121	172.9.99.121	VSP Policy
172.9.99.121				172.9.99.121	172.9.99.121	VSP Policy
172.9.99.121				172.9.99.121	172.9.99.121	VSP Policy
172.9.99.121				172.9.99.121	172.9.99.121	VSP Policy
172.9.99.121				172.9.99.121	172.9.99.121	VSP Policy
172.9.99.121				172.9.99.121	172.9.99.121	VSP Policy
172.9.99.121				172.9.99.121	172.9.99.121	Extreme Policy
172.9.99.121				172.9.99.121	172.9.99.121	Extreme Policy
172.9.99.121				172.9.99.121	172.9.99.121	Extreme Policy
172.9.90.14	Campus2-Acc2	Contact Esta...	Stack	172.9.99.120	172.9.99.121	Extreme Policy
172.9.98.106	EWC1a	Contact Esta...	EWC1a.sqa.net	172.9.99.120	172.9.99.121	Extreme Identi...
172.9.98.107	EWC1b	Contact Esta...	EWC1b.sqa.net	172.9.99.120	172.9.99.121	Extreme Identi...



- Verify that the Fabric Attach Mgmt VLAN (from the FA Server) was assigned to the access switch:

```
Acc-320(config)#show fa element
=====
Fabric Attach Discovered Elements
=====
UNIT/          MGMT          ELEM ASGN
PORT   TYPE      VLAN  STATE  SYSTEM ID      AUTH  AUTH
-----
MLT1   Server    300   T / S  00:bb:00:03:10:11:30:01:00:01  NA   NA
```

- Upon connection, wired user traffic will be authenticated via ExtremeControl, and the corresponding Accept Policy will be sent to the access switch. The access switch will assign that role to the end user via netlogin:

```
Acc-321#show eapol session port 1/3
----- Non-EAP Clients -----
Unit/Port Client MAC Address State Vid Pri
-----
1/3      00:32:01:00:00:19  Authenticated By RADIUS 302 0
Total number of DHCP phones: 0
Total number of EAP clients: 0
Total number of non-EAP clients: 1
Total number of unauthenticated clients: 0
```

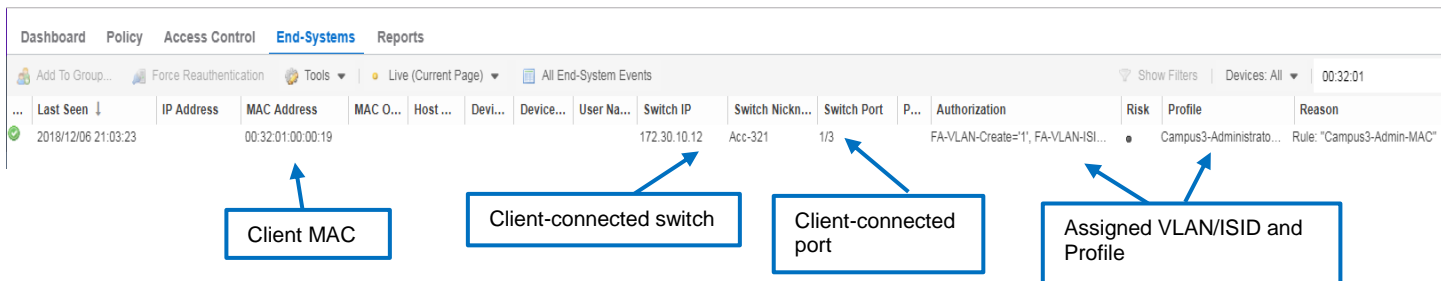
The end user authenticated MAC.

- The corresponding VLAN and ISID are assigned:

```
Acc-321#show fa ass
I-SID   VLAN   Source   Status
-----
1030302 302    Radius   Active
Binding Count: 1
```

The VLAN/ISID mapping

- Verification via ExtremeControl: **Navigate to Control → End Systems**



Authentication – Netlogin & RADIUS

Network login is a security feature that controls admission of user packets and access rights, preventing unauthorized access into the network. Netlogin offers three authentication types: MAC-based, dot1x and web-based. MAC-based authentication can be done locally or using a RADIUS server. MAC-based with RADIUS server and dot1x methods are implemented for this solution.

By itself, netlogin actions consist of allowing or filtering traffic on the ports it is enabled on. Its functionality can be further enhanced by using policies, which offer a greater variety of actions and granular control of user packets access to the network.

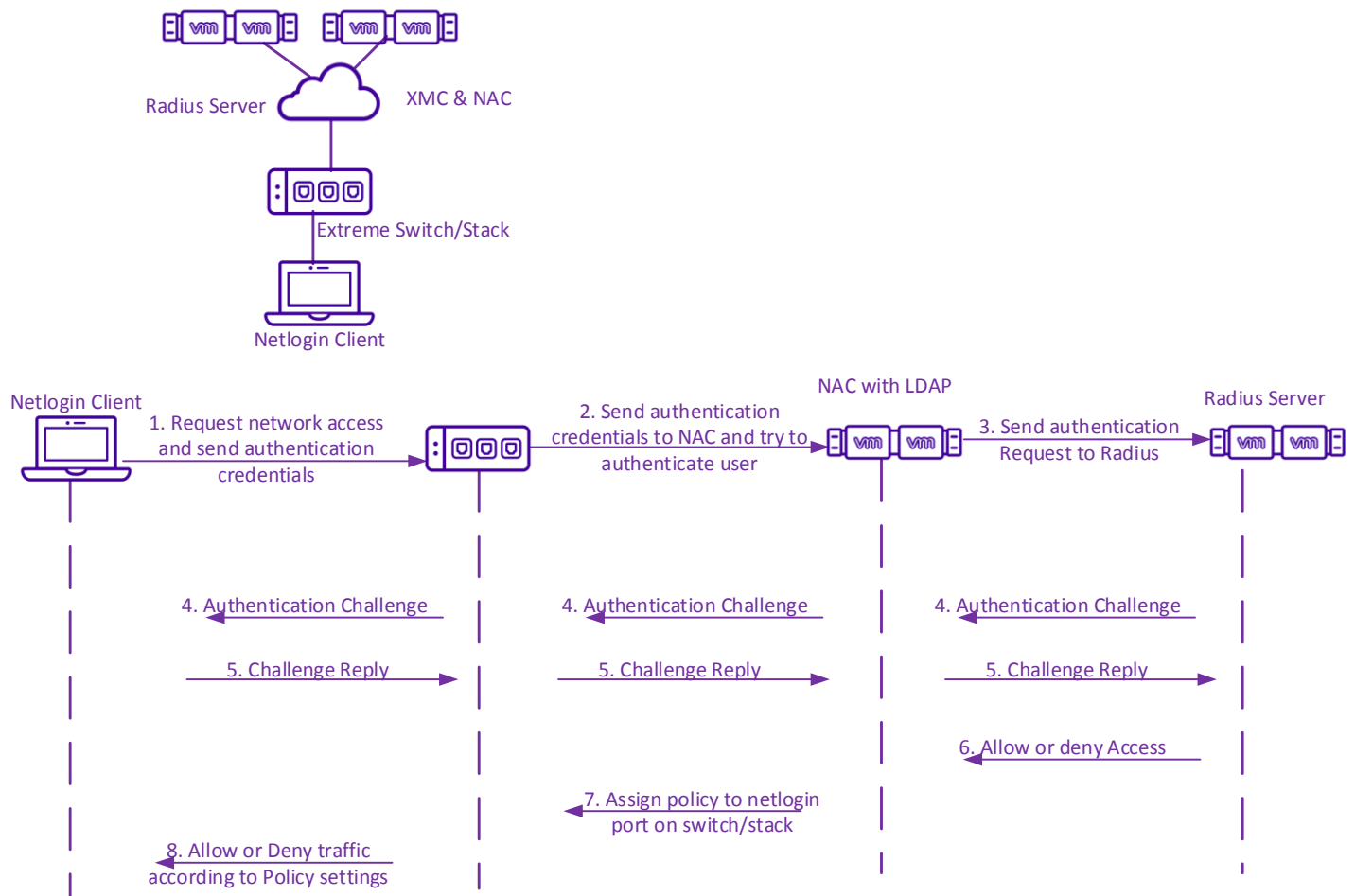
Netlogin dot1x authentication involves three parties: supplicant, authenticator and authentication server. The supplicant is the client machine, capable of running 802.1X authentication software. The authenticator is the network device the client is connected to, configured with netlogin. The authentication server is usually a third-party RADIUS server.

For clients that can't run authentication software – like printers, APs, and other wired devices connected to the network – MAC-based authentication can be used. In this case the supplicant is unaware that the authentication is taking place. The authenticator will use the device's MAC address to authenticate the user.

For a user to authenticate, the following conditions must be met:

1. The Extreme device is added to Extreme Management Center.
2. Controllers are added to Extreme Management Center and are configured.
3. LDAP configurations are made.
4. The device is added to the correct Control Domain.
5. Policies are created – roles and corresponding services are defined.
6. Policies are enforced on Extreme switches.
7. Access control rules and accept policies are defined.
8. Network devices are added as trusted RADIUS clients for ExtremeControl.
9. Access control settings are enforced on the controllers.

Authentication Process



Authentication Steps

1. A user connecting to the switch and requesting network access sends login credentials to the switch.
2. The switch sends the credentials in a RADIUS Request message to the ExtremeControl. Upon seeing the request, the ExtremeControl verifies its RADIUS server configuration. If a server is present, the authentication request is sent to it. If no server is found, the LDAP configuration conditions are verified. If the conditions are all met, the authentication request is sent to the RADIUS server. At this point ExtremeControl/LDAP is acting as authenticator.
3. When the RADIUS server receives an authentication request it first verifies that the authenticator is in its trusted client list and that the shared secret received matches the locally configured one, to determine if it can accept an authentication request from the client. Next, if the client verification passes, the RADIUS server searches for a Network Access policy whose access conditions are passed by the Request packet. If an access policy is found, the authentication process can continue. If not, the user's login attempt is rejected.
4. For PEAP and TLS authentication, a RADIUS Challenge message is sent to the user.
5. The user must respond to the challenge in order to complete the authentication process.

6. The RADIUS server either allows or denies the user access and sends the response to the ExtremeControl server.
7. If the user passes authentication, ExtremeControl starts verifying the LDAP attributes and Access Control Rules one by one until the conditions of one of them are met. A Profile and an Accept Policy for the matched rule are returned for the authenticated user and applied on the switch port to which the user is connected.
8. All traffic generated by the user will be treated according to the services configured for the Role corresponding to the Accept policy the user matched.

RADIUS Configuration

When user access control is done using policy and netlogin, at least one RADIUS server must be configured on the access switches. At the access layer of the Automated Campus solution, two RADIUS servers are configured—one primary and one secondary – for redundancy. If the primary server fails, the authentication requests will be sent to the second RADIUS server. On the switches, the ExtremeControl engines are configured as RADIUS servers.

When the access switch is added as a Switch to ExtremeControl, the resulting auto-configuration should look similar to the one below:

Summit Access switches:

```
Slot-1 Stack.1 # show config aaa
#
# Module aaa configuration.
#
configure radius 1 server 172.9.99.120 1812 client-ip 172.9.90.11 vr VR-Default
configure radius 1 shared-secret encrypted "$PRLoiBq3oT81gwfTQRzSQhR8yaZhYQ=="
configure radius 2 server 172.9.99.121 1812 client-ip 172.9.90.11 vr VR-Default
configure radius 2 shared-secret encrypted "$1XDtAvhCUB7v5akv9X97TG0r1VDK+Q=="
configure radius-accounting 1 server 172.9.99.120 1813 client-ip 172.9.90.11 vr VR-Default
configure radius-accounting 1 shared-secret encrypted "$UriT+Zu2oRu4Yj6PA1Ss81U/b/9a3Q=="
configure radius-accounting 1 timeout 10
configure radius-accounting 2 server 172.9.99.121 1813 client-ip 172.9.90.11 vr VR-Default
configure radius-accounting 2 shared-secret encrypted "$t4+vv1g0kNXIq2X39Fmv5ONPXUP3RQ=="
configure radius-accounting 2 timeout 10
enable radius
enable radius mgmt-access
enable radius netlogin
configure radius timeout 10
configure radius mgmt-access timeout 15
configure radius netlogin timeout 15
enable radius-accounting
enable radius-accounting mgmt-access
enable radius-accounting netlogin
```

ERS Access switches: When the ERS is configured with the commands from the provisioning section, the resulting configuration should look similar to the one below:

```
Acc-321(config)#show run module radius
!
! *** RADIUS ***
!
radius-server encapsulation ms-chap-v2
no radius use-management-ip
radius server host 172.9.99.120 acct-enable
radius server host 172.9.99.121 secondary
radius server host 172.9.99.120 used-by eapol acct-enable
radius server host 172.9.99.121 secondary used-by eapol
radius server host 172.9.99.120 used-by non-eapol acct-enable
radius server host 172.9.99.121 secondary used-by non-eapol
!
! *** RADIUS Dynamic Server ***
!
```

Netlogin Configuration (Summit)

Authentication with netlogin dot1x and MAC is enabled on all Summit ports except for the uplink and server ports. The authentication order is dot1x MAC.

When complete, the configuration should look similar to the one below:

Summit Access switches

```
Slot-1 Stack.2 # show config netlogin
#
# Module netLogin configuration.
#
enable netlogin dot1x mac
configure netlogin authentication protocol-order dot1x mac web-based
enable netlogin ports 1:1-49,2:1-49,3:1-49 dot1x
enable netlogin ports 1:1-49,2:1-49,3:1-49 mac
configure netlogin add mac-list ff:ff:ff:ff:ff:ff 48
```

EAPOL Configuration (ERS)

Authentication with EAPOL dot1x and MAC can be enabled on all ERS ports except for the uplink and server ports.

When complete, the configuration should look similar to the one below:

```
Acc-321(config)#show run module EAP
! *** EAP ***
eapol multihost radius-non-eap-enable
eapol multihost auto-non-eap-mhsa-enable
interface Ethernet ALL
eapol multihost port 1/1-2,1/4-28,2/ALL eap-mac-max 32 non-eap-mac-max 32 mac-max 64
eapol multihost port 3/1 eap-mac-max 32 non-eap-mac-max 32 radius-non-eap-enable mac-max 64
eapol multihost port 3/2 eap-mac-max 32 non-eap-mac-max 32 mac-max 64
eapol multihost port 3/3 eap-mac-max 32 non-eap-mac-max 32 radius-non-eap-enable mac-max 64
eapol multihost port 3/4-15 eap-mac-max 32 non-eap-mac-max 32 mac-max 64
eapol multihost port 3/16 eap-mac-max 32 non-eap-mac-max 32 radius-non-eap-enable mac-max 64
eapol multihost port 3/17-28 eap-mac-max 32 non-eap-mac-max 32 mac-max 64
exit
interface Ethernet ALL
eapol port 3/1,3/3,3/16 status auto
exit
```

Wireless User Access

Once the Wireless Controllers have been configured and the access switches have been provisioned in XMC, the deployment of Extreme Wireless Access Points for user access is fairly simple.

AP Provisioning / Fabric Attach

1. Connect a new AP to an access switch port.
2. Once the AP boots up, LLDP is exchanged between the AP and the access switch, discovering each other as Fabric Attach elements. The AP will automatically reboot in FA mode.
3. The access switch, acting as the FA proxy, will advertise (via LLDP) the FA management VLAN to the AP: To verify this, enter the following:

Summits in Campus 1:

```
Slot-1 Stack.1 # show fabric attach elements
Fabric Attach Mode: Proxy
```

System Id	Port	Type	Mgmt VLAN	Auto Tag	Provision
00-bb-00-01-10-11-30-02-00-02	1:50	Server (No Auth)	100	Mix	Disabled
d8-84-66-e3-25-b8-00-00-00-00	2:20	WAP Type 1	100	Mix	Disabled
d8-84-66-57-aa-58-00-00-00-00	2:22	WAP Type 1	100	Mix	Disabled
00-bb-00-01-10-11-30-02-00-02	2:50	Server (No Auth)	100	Mix	Disabled

FA Mgmt VLAN 100 is received from FA Server port and advertised to all detected FA element ports (APs).

ERS in Campus 3:

```
ERS-4900(config)#show fa elements
```

```
=====
Fabric Attach Discovered Elements
=====
```

UNIT/ PORT	TYPE	MGMT VLAN	STATE	SYSTEM ID	ELEM AUTH	ASGN AUTH
MLT1 2/22	Server Client	300 0	T / S T / D	00:bb:00:03:10:11:30:01:00:01 d8:84:66:4f:a9:bc:00:00:00:00	NA NA	NA N

FA Mgmt VLAN 300 is received from FA Server port and advertised to all detected FA element ports (APs).

4. The AP will acquire an IP address (via DHCP) from the network server, along with DHCP scope option 78, which provides the IP addresses for the EWCs.

5. The AP will then register with the EWCs, and its serial number will appear in its list:

The screenshot shows the 'APs' management page. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS, WIPS, and Help. A search bar is present with the text 'Search for AP Name, Site, Model ...'. A 'Show / hide columns' button is also visible. The main table lists APs with columns for Name, Model, IP Address, SW Version, Location, and Site. The first row, with serial number 1608Y-1176300000, is circled in red. Below the table, it says 'Showing: 7 rows, Local: 6, Foreign: 1'.

Name	Model	IP Address	SW Version	Location	Site
1608Y-1176300000	AP3935e-FCC	172.30.10.21	10.41.11.0009		
Acc120-57aa58	AP3935i-FCC	172.10.10.22	10.41.11.0009	Campus1	Campus1
Acc121-31D79A	AP3935e-FCC	172.10.10.21	10.41.11.0009	Campus1	Campus1
Acc220-4FA926	AP3935e-FCC	172.20.10.20	10.41.11.0009		Campus2
Acc220-4FA9B6	AP3935e-FCC	172.20.10.24	10.41.11.0009	Campus3	Campus2
Acc221-7A04B7	AP3916ic-FCC	172.20.10.21	10.41.11.0009	Campus2	Campus2
Acc321-E325B8	AP3935i-FCC	172.30.10.22	10.41.11.0009	Campus3	Campus3

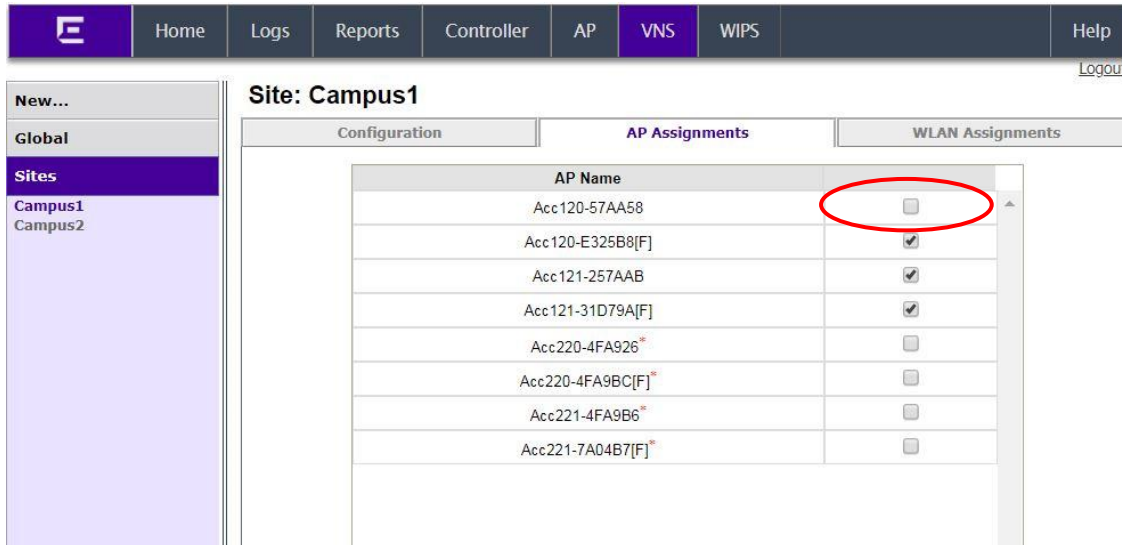
6. Click on the new AP, then **Configure**:

The screenshot shows the 'Edit AP' configuration page. The 'AP Properties' tab is active. The 'Name' field is highlighted with a blue box and an arrow pointing to a callout box that says 'Optional: Enter a User-friendly name for the AP, and a Location description.' The 'Apply' button is circled in red. The 'Country' field is set to 'United States'.

AP Properties updated successfully

Copy to Defaults Reset to Defaults **Apply** Close

- On the EWC (**VNS**→**Sites**), add the AP to the appropriate site. This AP will inherit all the configuration parameters (Roles, WLAN assignments, etc) associated with the Site. Click **Save**:



- The “Access Point” Policy Role enforced to the Summit access switches identifies the port the AP is connected to based on its MAC OUI and applies the “AP Aware” rule, instructing the access switch to forego any authentication of end users ingressing that port. The AP will process authentication requests with ExtremeControl for connecting wireless users. The access switch will only have a netlogin authentication entry for the AP off that port:

```
Slot-1 Stack.15 # show netlogin session port 2:22
Multiple authentication session entries
-----
Port           : 2:20           Station address   : d8:84:66:57:aa:58
Auth status    : success        Last attempt     : Tue Sep 11 14:45:50 2018
Agent type     : mac           Session applied  : true
Server type    : radius       VLAN-Tunnel-Attr : None
Policy index   : 7            Policy name      : Access Point (active)
Session timeout : 0           Session duration : 0:16:00
Idle timeout   : 300        Idle time        : 0:00:00
Auth-Override  : enabled       Termination time : Not Terminated
```

AP MAC address, and the Role assigned.

Auth-Override indicates the access switch will not authenticate end-users ingressing this port.

9. With the ERS, the EAPOL and FA configuration will identify the AP as a connected FA client, foregoing any authentication of end users on that port. The RADIUS attributes for AP-connected ERS ports will also be applied from ExtremeControl to instruct the ERS to accept any FA requests from the connected client. The access switch will only have an EAPOL authentication entry for the AP off that port, with wireless clients showing as non-authenticated:

```
Acc-321(config)#sh eapol session port 2/22
```

----- Non-EAP Clients -----					
Unit/Port	Client MAC Address	State		Vid	Pri
2/22	D8:84:66:E3:25:B8	Authenticated By RADIUS		300	0

----- Unauthorized Clients -----					
Unit/Port	Client MAC Address	Type		Radius Status	
2/22	00:1B:77:15:46:09	MHSA Auth		No request	
2/22	C0:BD:D1:AA:7E:35	MHSA Auth		No request	
2/22	E8:4E:06:50:5D:1D	MHSA Auth		No request	

10. The AP (FA Client) will request to the access switch (FA Proxy) the required I-SID assignments based on the configured wireless topologies:

- **Summit:**

```
Slot-1 Acc-120.1 # show vlan fab att ass
```

Port	VLAN	VLAN Name	Type	ISID/NSI	Status
	101	VLAN_101	Dynamic	1010101	Active
	104	VLAN_104	Dynamic	1010104	Active
2:20	100	VLAN_100	Dynamic	1010100	Active
2:20	200	SYS_VLAN_0200	Dynamic	1020200	Active
2:20	1050	SYS_VLAN_1050	Dynamic	1501050	Active
2:20	1051	SYS_VLAN_1051	Dynamic	1501051	Active
2:20	1052	SYS_VLAN_1052	Dynamic	1501052	Active

VLAN and associated I-SID requested

AP-connected port

- **ERS:**

```
ERS-4900(config)#show fa assignment
```

I-SID	VLAN	Source	Status
1010100	100	Client	Active
1020200	200	Client	Active
1030300	300	Radius	Active
1030301	301	Radius	Active
1030303	303	Radius	Active
1090907	907	Radius	Active
1501050	1050	Client	Active
1501051	1051	Client	Active
1501052	1052	Client	Active


Binding Count: 9

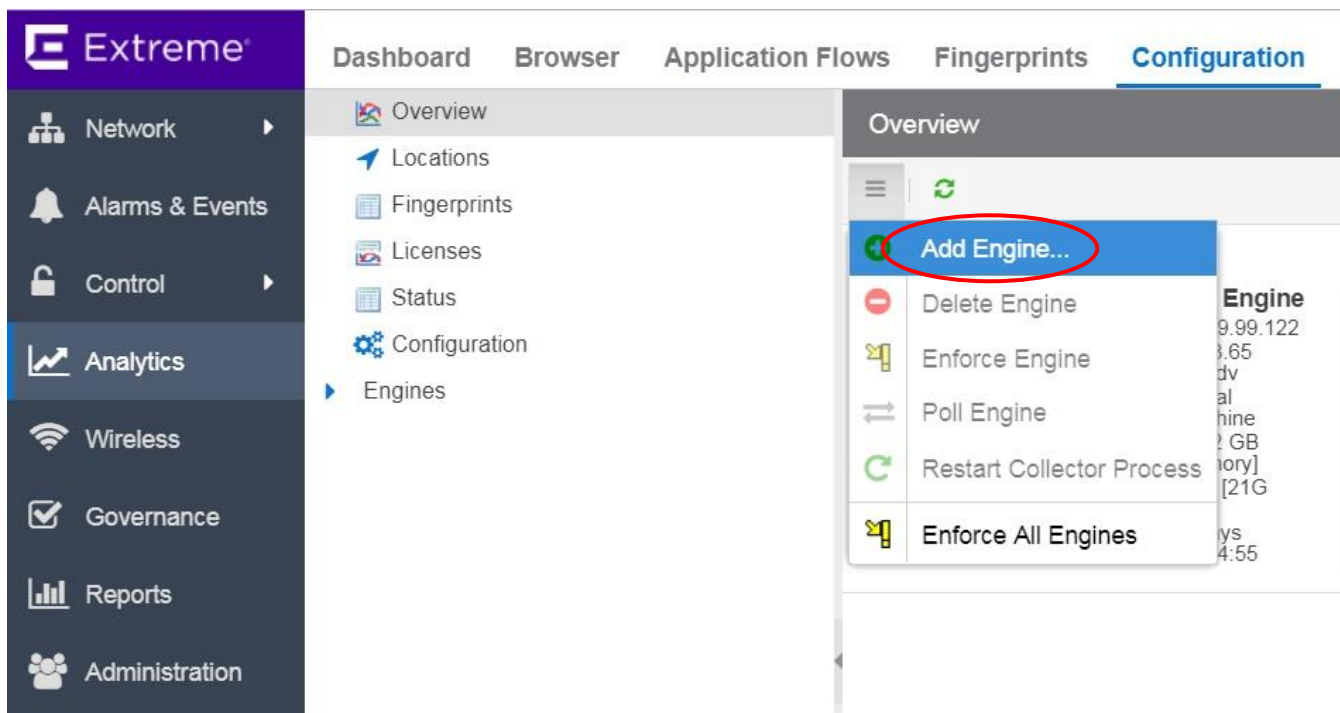
VLAN and associated I-SID requested

ExtremeAnalytics Configuration

Adding Analytics to Extreme Management Center

From Extreme Management Center, navigate to:

Extreme Management → Analytics → Overview →  → Add Engine



- Provide the IP address of the ExtremeAnalytics Engine, a user-friendly name, and configured SNMP profile. Click **OK**

Add Application Analytics Engine ✕

IP Address:

Name:

Profile:

After adding an engine, go to the engine's Configuration panel to add a wireless controller flow source, enable Access Control integration, or change the default web credentials.

- The ExtremeAnalytics engine will appear in the Overview Pane. Locate the green indicator, confirming that the engine is operational. You should also see basic engine processing data.

The screenshot shows the 'Overview' section of a management interface. A green dot next to the 'Analytics' label is circled in red. Below it, three columns of data are displayed:

Application Analytics Engine	Sensor Process	Collector Process
IP: 172.9.99.122 Version: 8.1.3.65 Serial Number: appidv virtual machine Number of CPUs: 8 [12 GB [Memory]: memory] Disk Info: 28G [21G free] Last Enforce: 4 Days 01:43:52	In Packets: 7,153/s [peaks: day 8,313/s, week 8,415/s] Dropped Packets: 0/s [peaks: day 0/s, week 0/s] Out Records: 3,016/s [peaks: day 3,431/s, week 3,431/s] Sensor Up Time: 7 Days 21:23:58 Process CPU:	NetFlow Records: 3,189/s [peaks: day 3,427/s, week 3,427/s] Identification Rate: 100% [average: day 95%, week 81%] Number of Clients: 813 [peaks: day 860, week 860] Collector Up Time: 17 Days 17:58:35 Process CPU:

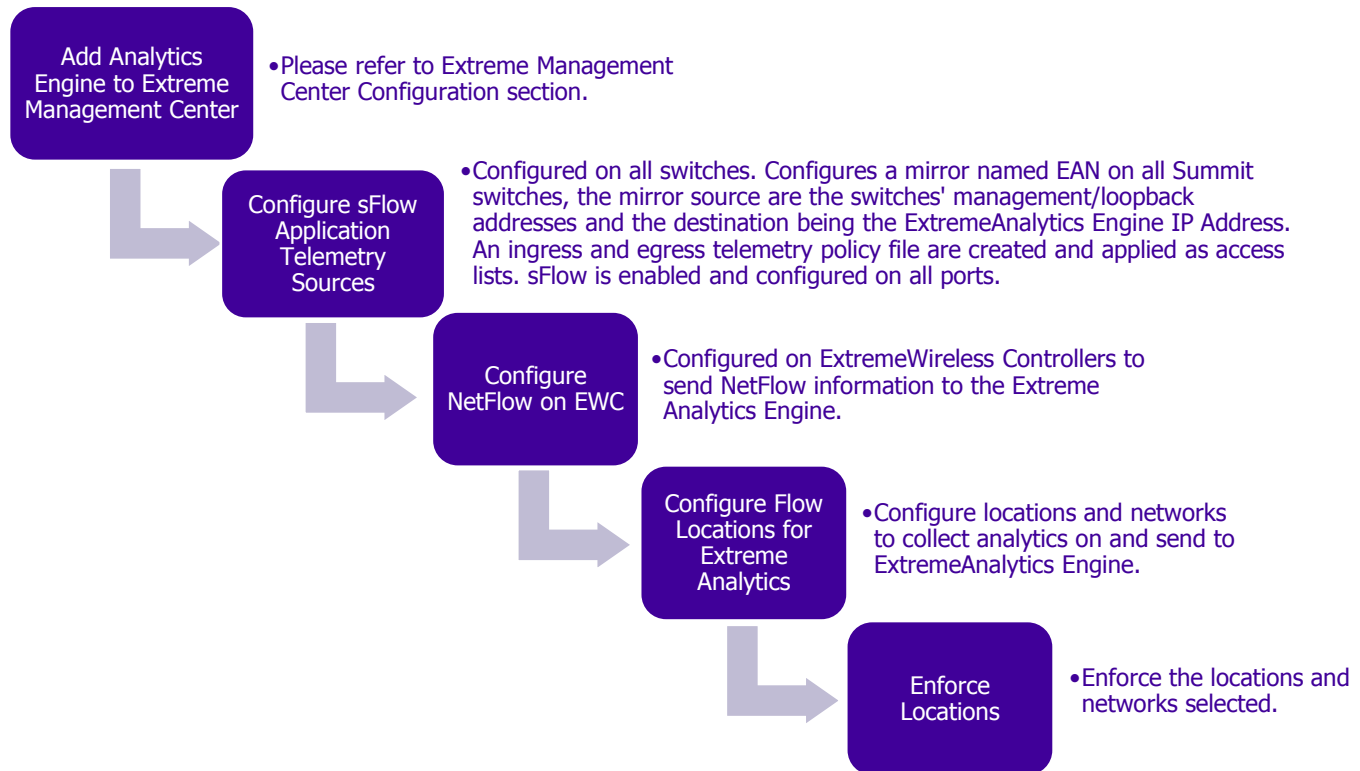
- Click the enforce button at the bottom of the web page to fully deploy the ExtremeAnalytics Engine.

The screenshot shows the 'Operations*' toolbar. A yellow icon with a hammer and a red 'X' (the 'Enforce' button) is circled in red, with the number '1' next to it. Other icons include a trash can, a bell, and several colored status indicators.

The screenshot shows a dialog box titled 'Enforce All Engines'. The text inside asks: 'Are you sure you want to enforce all Application Analytics engines?'. At the bottom, there are two buttons: 'Yes' (highlighted with a red circle) and 'No'.

ExtremeAnalytics Configuration

Extreme Analytics will be configured to provide detailed flow information. Refer to the flow chart below:



Flow collection in this topology is handled by the uplink ports to the Analytics engine. If an ExtremeSwitching access switch is utilized, the ability to collect analytics at the stack or standalone switch are dependent on the models utilized. Please refer to product documents to determine hardware capabilities of the access switches.

Warning

The following sections detail how to configure Analytics on both access devices (Summits and APs) and on core devices (Fabric Connect switches), however only ONE option should be chosen to avoid duplicate reporting.

Note

The lower the sampling rate is set to, the more accurate the reporting will be. However, keep in mind that low sampling rate will increase CPU usage to some degree.

Extreme Analytics SFLOW Configuration (Summit Access Switches)

In this section, the user will add Summit access switches as Mirror Sources for sending the flow information to the Extreme Analytics Engine.

- Navigate to this menu location and enter the following information.

Analytics → Configuration → Engines → Analytics → Configuration

Configuration - 172.9.99.122

Flow Collection Type:	App Telemetry ▼	Max End-Systems in Hourly Details:	25000 ▲▼
Collection Privacy Level:	Maximum Access ▼	Store Slow Client Data:	<input type="checkbox"/>
Client Aggregation:	IP Address ▼	Store Application Location Data:	<input type="checkbox"/>
Sensor Log Level:	Informational ▼		

- Each Access switch will be added as the mirror source. The source IP address will be the switch management address, and the destination of the mirror will be the ExtremeAnalytics Engine. The Access switch does not have the resources necessary to collect flow data for ExtremeAnalytics. However, the flow data will be aggregated at the switch's uplink ports.

Analytics → Configuration → Engines → Analytics → Configuration → Application Telemetry Sources → Add

Application Telemetry Sources

Name	IP	Device Fa...	Sample Rate	ERSPAN VL...	ERSPAN IP
<div style="display: flex; justify-content: space-between; align-items: center;"> + Add - Remove ✎ Edit </div>					

- Under **Source** field, click the ellipsis icon “...” to bring up **Source Device** view:

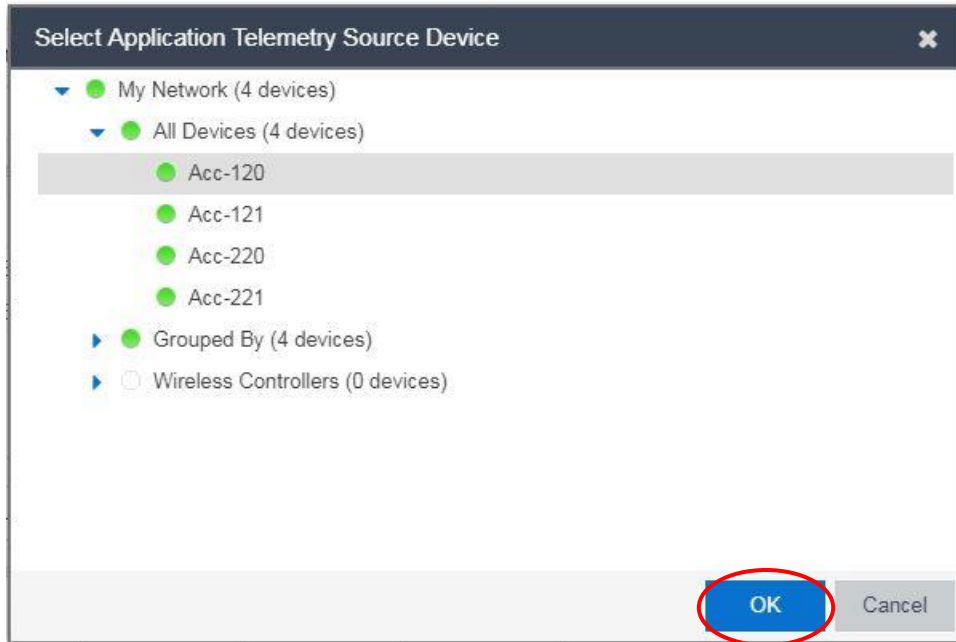
Add Application Telemetry Source ✕

Source: ...

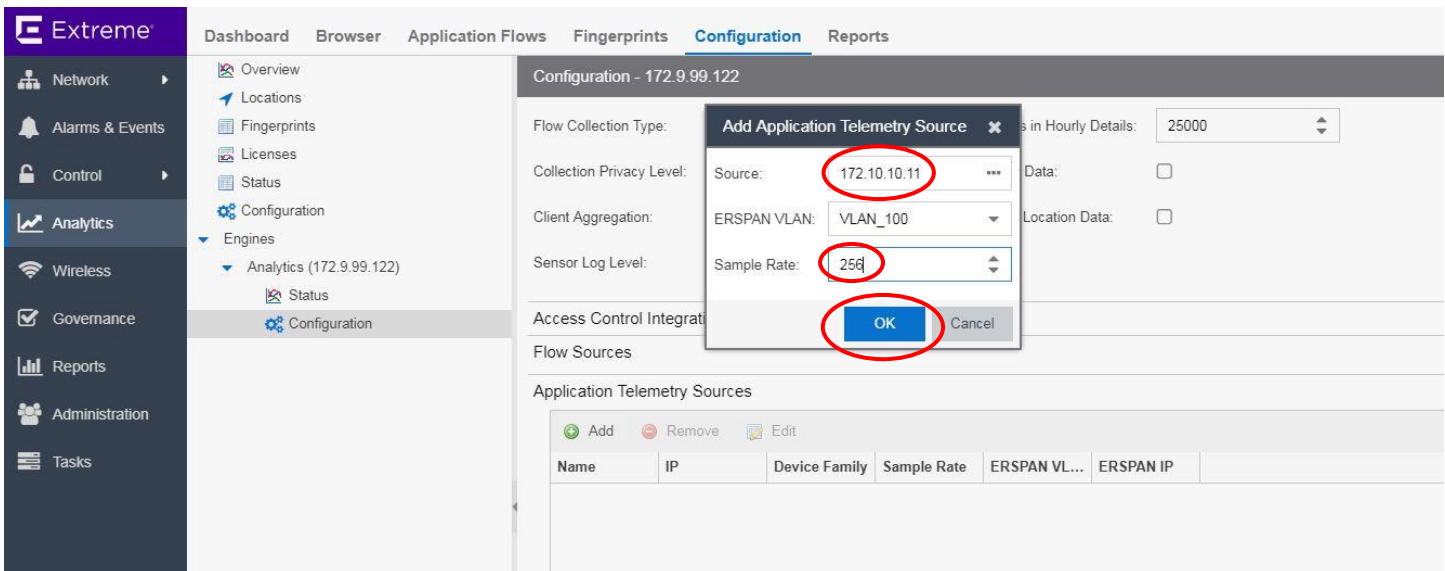
ERSPAN VLAN:

Sample Rate:

- Select All Devices → **Acc-120** → Click **OK**:



- Verify that **Source** IP address is the device management address. Optionally you can set **Sample Rate** to a different setting, minimum rate is **256**. Click **OK**:



- Depending on port density, this process can take several minutes. After adding all Access switches, Application Telemetry Sources should be configured. Final output should look something like below:

Application Telemetry Sources

Name	IP	Device Family	Sample Rate	ERSPAN VL...	ERSPAN IP
Acc-121	172.10.10.12	Summit Series	256	VLAN_100	172.10.10.12
Acc-120	172.10.10.11	Summit Series	256	VLAN_100	172.10.10.11
Acc-220	172.20.10.11	Summit Series	256	VLAN_200	172.20.10.11
Acc-221	172.20.10.12	Summit Series	256	VLAN_200	172.20.10.12

Extreme Analytics SFLOW Configuration (Fabric Connect Switches)

Configuring Analytics for Fabric Connect switches will be a future feature of XMC. However, support can be configured via the switch cli. This will enable flow-sample information to be forwarded to the Analytics engine so that data can be compiled and displayed in XMC. This document will not describe all of the variables for adding Analytics to a Fabric Connect switch. This information can be found in existing GTAC knowledge base articles and other CLI documentation.

Note

This illustrates how to enable SFLOW on BEB-910. This configuration should also be executed on any core BEBs with links to the access layer.

Some useful points to keep in mind:

- App-telemetry is enabled and SFlow is used as the flow type.
- The switch supports only ingress sampling.
- The switch does not support enabling sFlow on a link aggregation group (LAG) interface. However, you can enable sFlow on the member interfaces of a LAG.
- Order of Operations: Enable sFlow globally, add the sFlow collector; then enable app-telemetry.

Note that up to two collectors can be configured. SFlow configurations can be verified with **show sflow**; **show sflow collector**; and **show sflow interface enabled**. App-telemetry can be verified with **show app-telemetry status**, while **show app-telemetry counters** will show packet/byte statistics of protocol types.

BEB-910

```

BEB-8404-910:1>enable
BEB-8404-910:1#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
BEB-8404-910:1(config)#sflow agent-ip 10.0.0.10
INFO: Please be aware that sFlow agent IP address is only supported in MGMT or GRT VRF.
BEB-8404-910:1(config)#sflow enable
BEB-8404-910:1(config)#show sflow

```

- Enter Global Configuration mode
- Configure agent IP address (switch management)
- Enable sFlow

```

=====
sFlow Global Configuration
=====

```

```

Global State           : Enabled
Agent IP               : 10.0.0.10

```

BEB-910

```
BEB-8404-910:1(config)#sflow collector 1 address 172.9.99.122
BEB-8404-910:1#show sflow collector
```

- Configure collector IP address

```
=====
sFlow Collector Configuration Info
=====
Id      Owner      Collector-IP      Port      Timeout (secs)
-----
1       -          172.9.99.122     6343     0
2       -          0.0.0.0          6343     0
-----
```

```
All 2 out of 2 Total Num of sflow collector entries displayed
BEB-8404-910:1#
```

- Configure the interfaces with the sampling rate (range of 8192-1000000):

BEB-910

```
BEB-8404-910:1(config)#int gigabitEthernet 2/10
BEB-8404-910:1(config-if)#sflow collector 1
BEB-8404-910:1(config-if)#sflow sampling-rate 8192
BEB-8404-910:1(config-if)#exit
BEB-8404-910:1(config)#int gigabitEthernet 2/17
BEB-8404-910:1(config-if)#sflow collector 1
BEB-8404-910:1(config-if)#sflow sampling-rate 8192
BEB-8404-910:1(config-if)#exit
BEB-8404-910:1(config)#int gigabitEthernet 2/18
BEB-8404-910:1(config-if)#sflow collector 1
BEB-8404-910:1(config-if)#sflow sampling-rate 8192
BEB-8404-910:1(config-if)#exit
BEB-8404-910:1(config)#int gigabitEthernet 3/10
BEB-8404-910:1(config-if)#sflow collector 1
BEB-8404-910:1(config-if)#sflow sampling-rate 8192
BEB-8404-910:1(config-if)#exit
BEB-8404-910:1(config)#int gigabitEthernet 3/17
BEB-8404-910:1(config-if)#sflow collector 1
BEB-8404-910:1(config-if)#sflow sampling-rate 8192
BEB-8404-910:1(config-if)#exit
BEB-8404-910:1(config)#int gigabitEthernet 4/17
BEB-8404-910:1(config-if)#sflow collector 1
BEB-8404-910:1(config-if)#sflow sampling-rate 8192
BEB-8404-910:1(config-if)#exit
```

- Enter Interface Configuration mode
- Configure collector ID
- Configure sampling-rate

- Verification:

BEB-910

```
BEB-8404-910:1(config)#show sflow interface enabled
```

```
=====
sFlow Port Configuration Info
=====
Packet-Sample-Rate  Max-Header-Size  Counter-interval  Collector-list  Port
                    (in secs)
-----
2/10    8192             128               0               1
2/17    8192             128               0               1
2/18    8192             128               0               1
3/10    8192             128               0               1
3/17    8192             128               0               1
4/17    8192             128               0               1
-----
```

```
All 6 out of 6 Total Num of sflow port entries displayed
BEB-8404-910:1(config)#
```

BEB-910

```
BEB-8404-910:1(config)#app-telemetry enable
BEB-8404-910:1#show app-telemetry status
Application Telemetry is enabled
Collector is reachable via 172.9.99.122
BEB-8404-910:1#show app-telemetry counter
```

Enable app-telemetry in Configuration mode

```
=====
Application Telemetry Counter
=====
```

EntryId	Name	Packets	Bytes
1	dhcpv4	14754	6810146
2	dhcpv6	2435	416385
3	dnstcp	0	0
4	dnstcp1	0	0
5	dnsudp	2404	303631
6	dnsudp1	7302	751554
7	tcpsyn	131704200	10272927656
8	tcpsynack	131714232	10273710096
9	tcpfinack	263419495	19493036890
10	bjnp	0	0
11	quicd	0	0
12	radius1	6709	1207152
13	radius4	7634	1277650
...			
126	ZOOM-TCP1	4	4440
127	ZOOM-TCP2	9158	679988
128	ZOOM-UDP1	0	0
129	ZOOM-UDP2	0	0
130	RADIUS-5	10717	750190
131	RADIUS-2	6626	766460
132	RADIUS-3	256624	34515226
133	RADIUS-11	2477	242746

```

Displayed 133 of 133 entries
BEB-8404-910:1(config)#

```

Extreme Analytics NetFlow Configuration (Wireless)

Extreme Analytics can also be configured for the ExtremeWireless controllers. In this case NetFlow is utilized rather than sFlow. In order to support both sFlow and NetFlow simultaneously the Flow Collection Type will need to be changed to **Both**.

Analytics → Configuration → Engines → Analytics → Configuration

Configuration - 172.9.99.122





Flow Collection Type:	Both	Max End-Systems in Hourly Details:	25000
Collection Privacy Level:	NetFlow	Store Slow Client Data:	<input type="checkbox"/>
Client Aggregation:	Both	Store Application Location Data:	<input type="checkbox"/>
Sensor Log Level:	Informational		

- After changing the Flow Sources Dialog should open within the Access Control Integration pane. Select **Add**.

Analytics → Configuration → Engines → Analytics → Configuration → Application Telemetry Sources → Add

Access Control Integration

Flow Sources

Name	IP	Device Family	Port	Source Ports
<div style="border: 1px solid #ccc; padding: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center; border-bottom: 1px solid #ccc;">  Add  Remove  Edit  Test </div> </div>				

- Under **Flow Source** click “...” and navigate to **My Network → All Devices → EWC1a**, then click **OK**.

Add Flow Source
✕

Flow Source: ⋮

OK
Cancel

Select Flow Source Device
✕

- ▶ ● My Network (2 devices)
 - ▶ ● All Devices (2 devices)
 - EWC1a
 - EWC1b
 - ▶ ● Grouped By (2 devices)
 - ▶ ● Wireless Controllers (2 devices)

OK
Cancel

- Select all the WLANs and click **OK**. Notice that if a controller is paired to another controller it will perform the configuration in one step. There will be no need to perform this step for the second controller.

The screenshot shows a dialog box titled "Add Flow Source". It has a close button (X) in the top right corner. The "Flow Source:" field contains the IP address "172.9.98.106". The "Paired Controller:" field contains the IP address "172.9.98.107". Under the "WLANs:" section, there are three checked checkboxes: "AC-Campus", "AC-Guest", and "AC-Open". At the bottom, there are two buttons: "OK" (highlighted with a red circle) and "Cancel".

- Once controllers are added, the Access Control Integration | Flow Sources pane should look like the one below.

Flow Sources

➕ Add ➖ Remove 📄 Edit 🔄 Test					
Name	IP	Device Family	Port	Source Ports	WLANs
EWC1a	172.9.98.106	Wireless Co...	none		AC-Campus,AC-Guest,AC-Open
EWC1b	172.9.98.107	Wireless Co...	none		AC-Campus,AC-Guest,AC-Open

Extreme Analytics Location Configuration

Finally, select the networks from which flow information will be collected. This can be quite broad or narrow depending on your administrative requirements.

- Select a location. This is just a label and there is no requirement that it be a Role. Below it is identified as **Campus1 analytics**.

Analytics → Configuration → Locations

The screenshot shows the Extreme Networks configuration interface. The left sidebar contains navigation options: Network, Alarms & Events, Control, Analytics, Wireless, Governance, Reports, and Administration. The main content area is titled 'Locations' and includes a table with the following columns: Location, Address/Mask, Role, Home Engine, and Description. The table contains one entry for 'Campus1' with a role of 'Access' and a home engine of 'Analytics'. Below the table, there are three subnets listed under 'PrivateAddressSpace': 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. An 'Update' button is visible at the bottom right of the table area.

Location	Address/Mask	Role	Home Engine	Description
Campus1		Access	Analytics	Campus1 analytics

- Add the subnets which flow collection should monitor.

Analytics → Configuration → Locations → Highlight created Location → Right Click → Add Address

The screenshot shows a context menu opened over the 'Campus1' location in the table. The menu options are: Add 'Campus1' to Tracked Locations, Add Address (highlighted with a red circle), Edit, and Remove. The 'Add Address' option is the one to be selected according to the instructions.

Location	Address/Mask	Role	Home Engine	Description
Campus1		Access	Analytics	Campus1 analytics

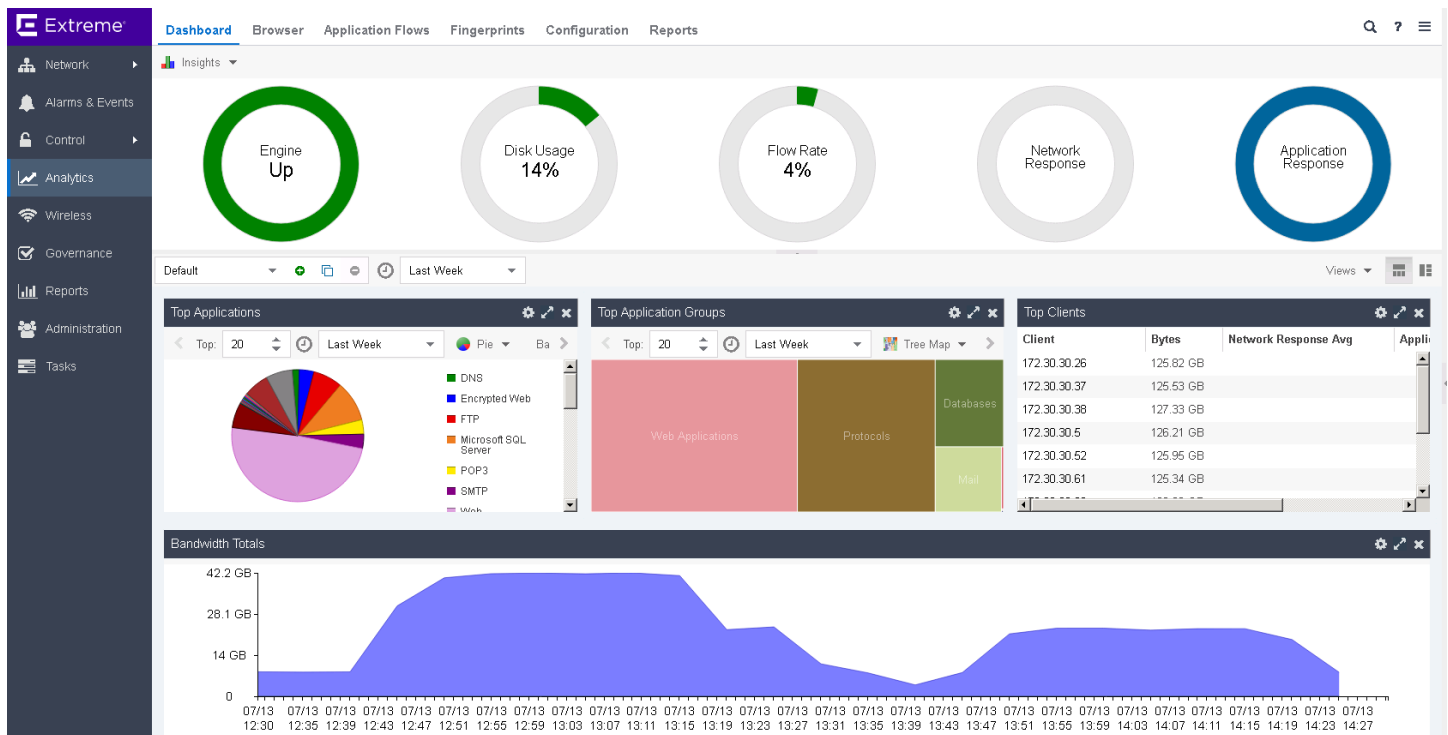
- After locations and subnets are added, user may have something that resembles below. Locations are based off of roles. User could have created locations based on physical locations. The important thing to remember is that locations are just a group of subnets, not an actual physical location.

Locations				
+ Add Location + Add Address Edit - Remove				
Location	Address/Mask	Role	Home Engine	Description
▶ PrivateAddressSpace		Core	Analytics	RFC 1918 private address space id
▼ Campus1		Access	Analytics	Campus1 analytics
	172.10.10.0/22			
	172.10.32.0/22			
	172.10.24.0/22			
	172.10.20.0/22			
	172.10.28.0/22			
▼ Central servers		Data Center	Analytics	Central servers analytics
	172.90.14.0/24			
	172.90.20.0/24			
	172.9.98.0/24			
	172.9.99.0/24			
	172.90.5.0/24			
	172.90.4.0/24			
	172.90.3.0/24			
	172.90.2.0/24			
	172.90.1.0/24			
▼ Campus2		Access	Analytics	Campus2 analytics
	172.20.32.0/22			
	172.20.28.0/22			
	172.20.24.0/22			
	172.20.20.0/22			
	172.20.0.0/22			
▼ Wireless		Access	Analytics	Wireless analytics
	172.90.40.0/22			
	172.105.2.0/24			
	172.105.1.0/24			
	172.105.0.0/24			

Extreme Analytics Verification

The Analytics will start collecting information. The polling interval is every 5 minutes. Be sure to give the dashboard enough time to begin populating information.

Analytics → Dashboard

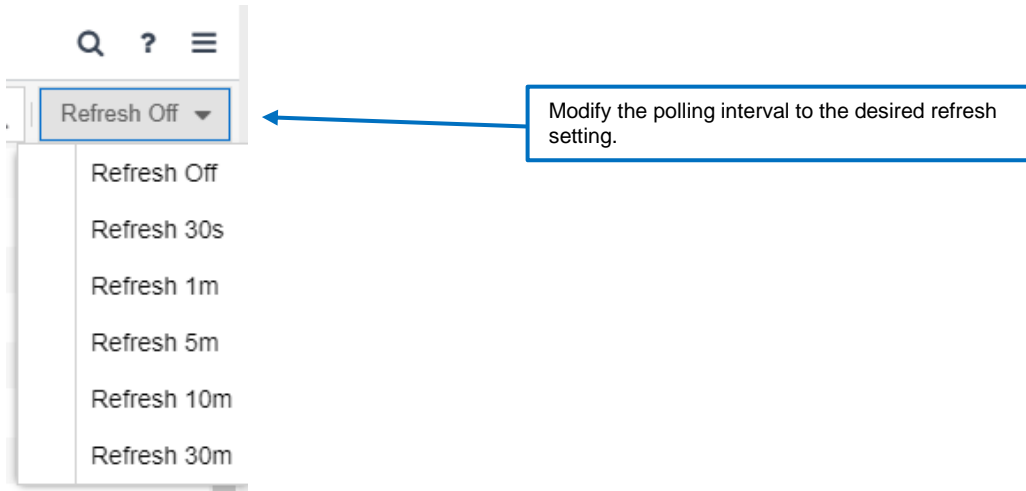


- Even though the dashboard might not be collecting information, the Application Flows window should begin to collect information. You can change the polling interval if you want to see updates in real time.

Analytics → Application Flows

The screenshot shows the 'Application Flows' window in the Extreme Analytics interface. The table displays network flows with columns for Flows, Client Address, Server Address, Server Port, Application, Application Group, and Application Info.

Flows	Client Address	Server Address	Server Port	Application	Application Group	Application Info
13	172.10.32.59	226.1.1.20	rtsp	rtsp port	Protocols	PerSwitchData=((172.1...
1738	172.20.29.146	172.90.1.163	urd	urd port	Protocols	PerSwitchData=((172.2...
12	172.20.32.76	226.1.1.17	rtsp	rtsp port	Protocols	PerSwitchData=((172.2...
744...	172.20.31.179	172.90.1.220	https	Encrypted Web	Web Applications	ServerIP=172.90.1.220...
1729	172.20.29.220	172.90.1.137	msft-gc-ssl	msft-gc-ssl port	Protocols	PerSwitchData=((172.2...
564...	172.20.31.167	172.90.1.228	http	Web	Web Applications	ServerIP=172.90.1.228...
13	172.10.32.55	226.1.1.36	rtsp	rtsp port	Protocols	PerSwitchData=((172.1...



- From the switch CLI the App Telemetry mirror can be observed with the `show mirror` command. Verify the IP addresses for the Analytics Engine and the Switch Management and that the Status = Up.

Summit Access Switch

```
Slot-1 Stack.1 # show mirror
```

```
DefaultMirror (Disabled)
  Description: Default Mirror Instance, created automatically
  Mirror to port: -

EAN (Enabled)
  Description:
  Mirror to remote IP: 172.9.99.122
  From IP : 172.20.10.11
  Status : Up
  VR : VR-Default
  Ping check: On
```

- Tunnel EAN is enabled.
- Mirror to Remote IP = Analytic Engine IP
- From IP = Management address of the switch
- Status = Up

```
Mirrors defined: 2
Mirrors enabled: 1 (Maximum 4)
HW filter instances used: 0 (Maximum 128)
HW mirror instances used: 0 ingress, 0 egress (Maximum 4 total, 2 egress)
```

- Below is an example of an sflow configuration. Issue `show conf etmon` to display sflow configuration.

Summit Access Switch

```
Slot-1 Stack.5 # show config etmon
#
# Module etmon configuration.
#
configure sflow sample-rate 256
configure sflow poll-interval 60
enable sflow
configure sflow collector 172.9.99.122 port 6343 vr "VR-Default"
configure sflow agent ipaddress 172.20.10.11
configure sflow ports 1:1 sample-rate 256
enable sflow ports 1:1 ingress
configure sflow ports 1:2 sample-rate 256
enable sflow ports 1:2 ingress
configure sflow ports 1:3 sample-rate 256
enable sflow ports 1:3 ingress
configure sflow ports 1:4 sample-rate 256
enable sflow ports 1:4 ingress
```

```

configure sflow ports 1:5 sample-rate 256
enable sflow ports 1:5 ingress
...
configure sflow ports 2:49 sample-rate 256
enable sflow ports 2:49 ingress
configure sflow ports 2:50 sample-rate 256
enable sflow ports 2:50 ingress
configure sflow ports 2:51 sample-rate 256
enable sflow ports 2:51 ingress
configure sflow ports 2:52 sample-rate 256
enable sflow ports 2:52 ingress
configure sflow ports 2:53 sample-rate 256
enable sflow ports 2:53 ingress
configure sflow ports 2:54 sample-rate 256
enable sflow ports 2:54 ingress

```

- When SFLOW App Telemetry is configured in XMC, two ACLs are configured and applied. Issue `show config acl` and verify the two access-lists are applied. Also, user can verify the access-lists by issuing an `ls` at the prompt to list present file.

Summit Access Switch

```

configure access-list telemetry any ingress
configure access-list telemetryegress any egress

-rw-r--r-- 1 admin 33450 Jul 13 11:02 telemetry.pol
-rw-r--r-- 1 admin 125 Jul 13 11:02 telemetryegress.pol

```

- User can also SSH into the Extreme Analytics and verify that SFLOW and GRE packets are being sent to the Analytics Engine. User should see both SFLOW and GRE packets being sent from all configured SFLOW sources.

Extreme Analytics Appliance

```

root@purviewnew813:~$ tcpdump -i eth0 proto gre -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:36:01.021962 IP 172.20.10.11 > 172.9.99.122: GREv0, length 64: gre-proto-0x88be

root@purviewnew813:~$ tcpdump -i eth0 port 6343 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:40:38.049317 IP 172.20.10.11.35586 > 172.9.99.122.6343: sFlowv5, IPv4 agent 172.9.90.13,
agent-id 0, length 1372

```

- Netflow configuration can be verified from the ExtremeWireless Controller graphical user interface. Within the wireless controller navigate to;

VNS → Global → Netflow/MirrorN

- Verify: Netflow Export-Destination IP Address = Extreme Analytics Engine.

The screenshot shows the ExtremeWireless Controller GUI. The navigation menu at the top includes Home, Logs, Reports, Controller, AP, VNS, WIPS, and Help. The VNS menu is selected. On the left, a sidebar menu shows 'Global' selected, with sub-items: Authentication, DAS, Wireless QoS, Bandwidth Control, Default Role, Filtering Mode, Sync Summary, NAC Integration, Client Autologin, Topology Group, Algorithm, Netflow/MirrorN, and Redirection URL. The main content area is titled 'Netflow/MirrorN Configuration' and contains the following fields:

- Netflow Export-Destination IP Address: 172.9.99.122 (highlighted with a red circle)
- Netflow Export Interval: 60 (30-360 seconds)
- Mirror first N: 15 (1-31 packets/flow)
- Traffic Mirror L2 Port: None

- User can also SSH into the Extreme Analytics and verify that IPFIX packets are being sent to the Analytics Engine from the EWC controllers.

Extreme Analytics Appliance

```
root@purviewnew813:~$ tcpdump -i eth0 port 2095 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:17:52.222947 IP 172.9.98.107.2095 > 172.9.99.122.2095: UDP, length 388
13:18:20.075153 IP 172.9.98.106.2095 > 172.9.99.122.2095: UDP, length 388
```

RF-Planning

When designing a wireless network, a thorough RF plan is vital to the success of the deployment. This process involves an extensive site survey and use of the Extreme Networks™ Planning Tool. Extreme Wireless RF-Planning can further be enhanced with the use of the Ekahau Site Survey tool and hardware.

Site Survey

Site Survey is perhaps the most important step in RF design. It validates the wireless deployment's expected coverage experience. A thorough site survey analyzes sufficient signal strength throughout the covered area and allows for channel planning to reduce co-channel interference.

Site Surveys are extremely important to new wireless deployments and when replacing or upgrading installed wireless gear. Products from different vendors or even across product generations of the same vendor often have different transmission characteristics. These changes can include; technological advances, the number of transmit and receive chains, and differences in radiation pattern. Never assume that replacing one piece of equipment for another, at the same installation points, will result in the same experience as the previous install.

An AP-on-a-stick physical site survey is the preferred method to thoroughly assess a site's RF design requirements. Testing an AP's proposed location provides true measurement and representation of the signal propagation and coverage to be expected. This method considers actual site characteristics such as obstructions to the RF signal, absorption by walls, and impact of any other architectural materials.

If a physical site survey is not possible, at minimum, a predictive survey should be performed. The predictive model often provides a first-pass view of the number of APs required to cover a site or a first-pass validation of whether installing a target AP family in pre-existing spots will provide the required coverage. The predictive model also provides greater insight into proper channel configuration, to obtain a performance optimized experience.

ExtremeWireless RF Planning Tool

The ExtremeWireless RF Planning Tool is a predictive survey tool made available to Extreme Network customers. The RF Planning tool is available online at <https://wirelessplanner.extremenetworks.com>.

Access to the tool is free, but user registration is required. Users can create a set of access credentials for the tool. Registration provides storage of saved models for later reference.

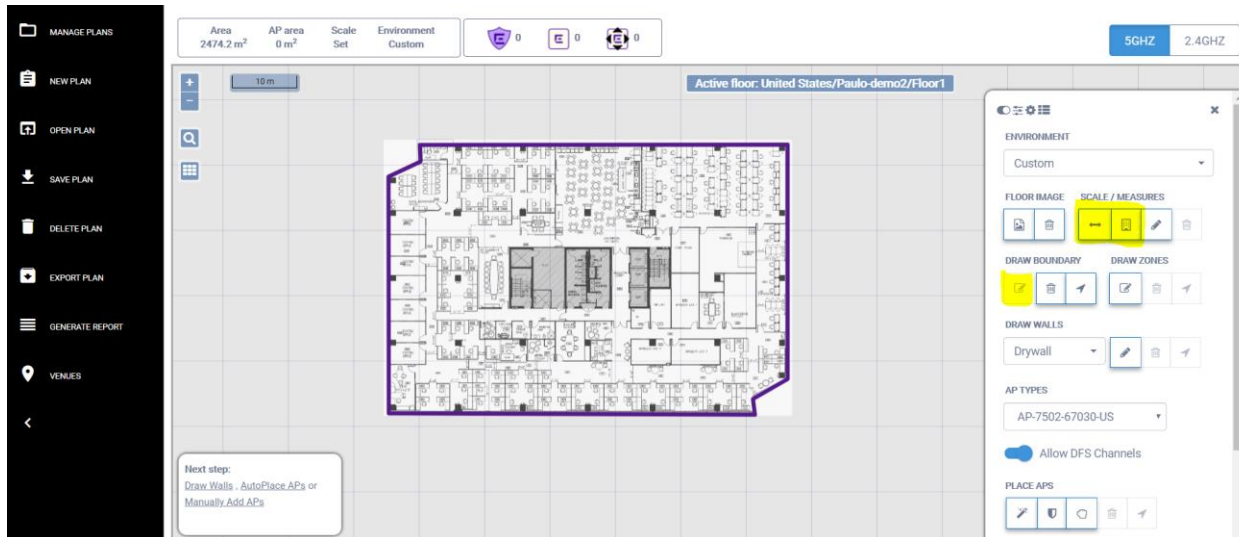
Once registered, the user is directed to provide the country of installation. Country selection is very important because the tool can customize requirements to applicable regulatory restrictions of the country identified. Regulatory restrictions can apply to channel availability, power levels, or even equipment availability. If country certification is required but not yet available for a device, it may not be available for selection.

The screenshot shows the user interface of the ExtremeWireless RF Planning Tool. At the top, there are two tabs: 'Plan settings' (active) and 'Account settings'. Below the tabs, there is a 'Country' selection field with a dropdown arrow and a red border, containing the text 'Please Enter a Country'. To the right of this field is a blue 'START' button with a right-pointing arrow. Below the 'Country' field, there is a 'New Plan' section with a blue 'START' button. Underneath, there is a 'Manage plans' section showing two plan entries: 'Untitled-1' and 'Untitled-2'. To the right of these entries is a set of four blue icons: a pencil (edit), a document (copy), a folder (share), and a trash can (delete).

After providing a few more details, you are provided with the working Canvas. Modeling steps include;

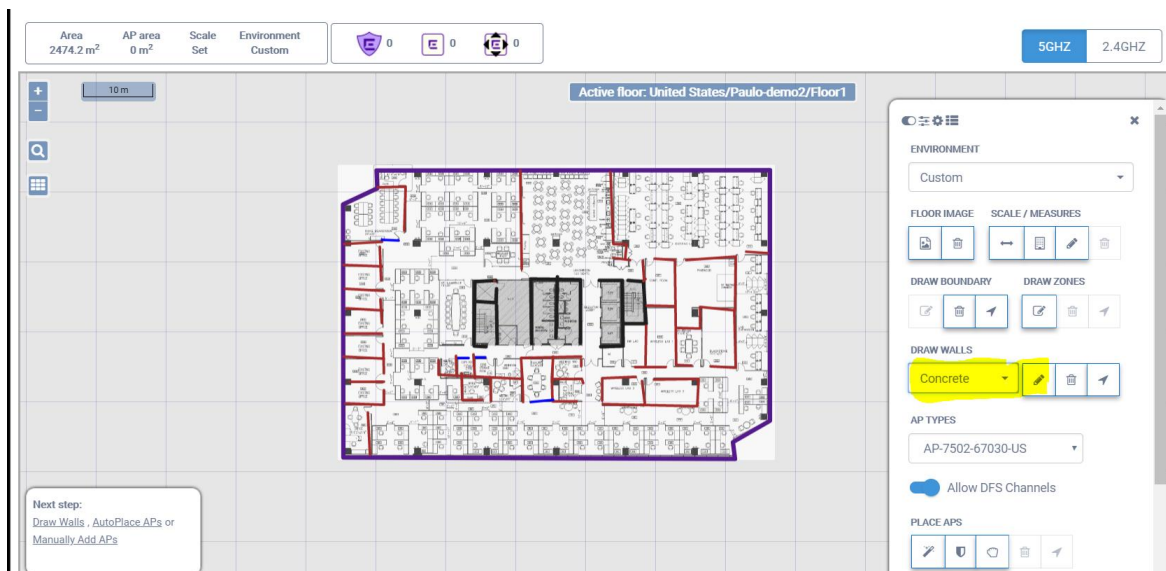
1. Floor Plan Outline and Scale

- You can either design a floor plan outline or upload a floor plan image representative of the site being designed.
- The tool allows for multi-floor designs within the same project, but note that it only considers one floor at a time. It does not consider or model cross-floor propagation.
- Scale can be defined by mapping a line of pixels into a corresponding distance. A simple way to determine an approximate scale is to determine the width of a doorway. In the United States the typical width of doorway is 3 feet, which can be used as reference for a 1-meter (3 ft.) line.



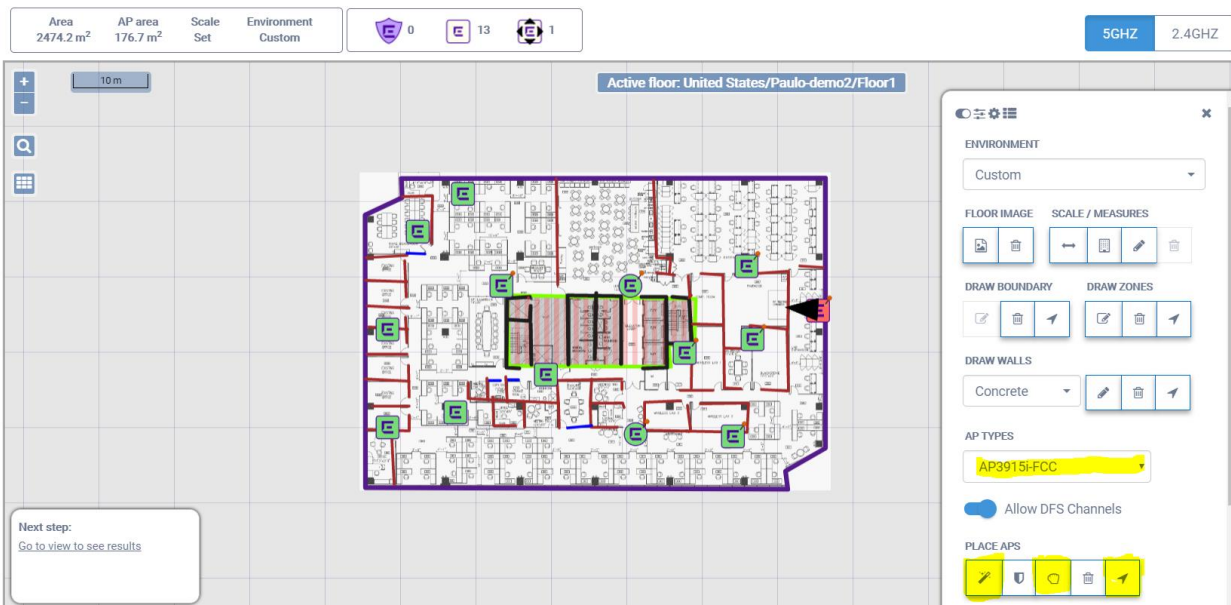
2. Identify and map any known RF obstructions.

- Consider include wall materials, escape routes (stairways), and restrooms (washrooms).
- The more detailed your model is, the more accurate the predictive model will be.
- Do not assume free-space (no walls) unless you are in fact planning for a true open area.



3. Access Point Placement

- a. The tool support for the entire portfolio of Wave 1 and Wave 2 access points from ExtremeWireless and ExtremeWireless WiNG is available. (Due to regulatory restrictions, not all APs are available in all regions.)
- b. Placement is primarily assessed based on a coverage objective.
- c. Automatic AP placement is available for a set of devices, primarily internal-antenna models, using a set of heuristic algorithms to determine the best placement for the APs from an RF coverage perspective. Only one AP model type at a time can be selected for auto-placement, but models can share with other available AP models that already pre-determined (pinned). This method provides the simplest way to determine how many APs will be required to cover a floor-plan area. After the automatic wizard runs, APs locations can be manually adjusted to a more correct installation location. When this is done, the AP is pinned to the selected location.
- d. Manual placement provides a more fine-controlled method for AP placements: you individually place each AP into its corresponding installation point. This can be the starting step for a model that starts from an existing installation design. You can manually select from the available models to complete the coverage to the desired targets.
- e. Automatic AP placement can be rerun after APs are manually placed or pinned. This ensures that the proposed installation model does not require any additional devices for fine tuning. Alternatively, you can also define exclusion areas in which to the algorithm will not attempt to place APs.

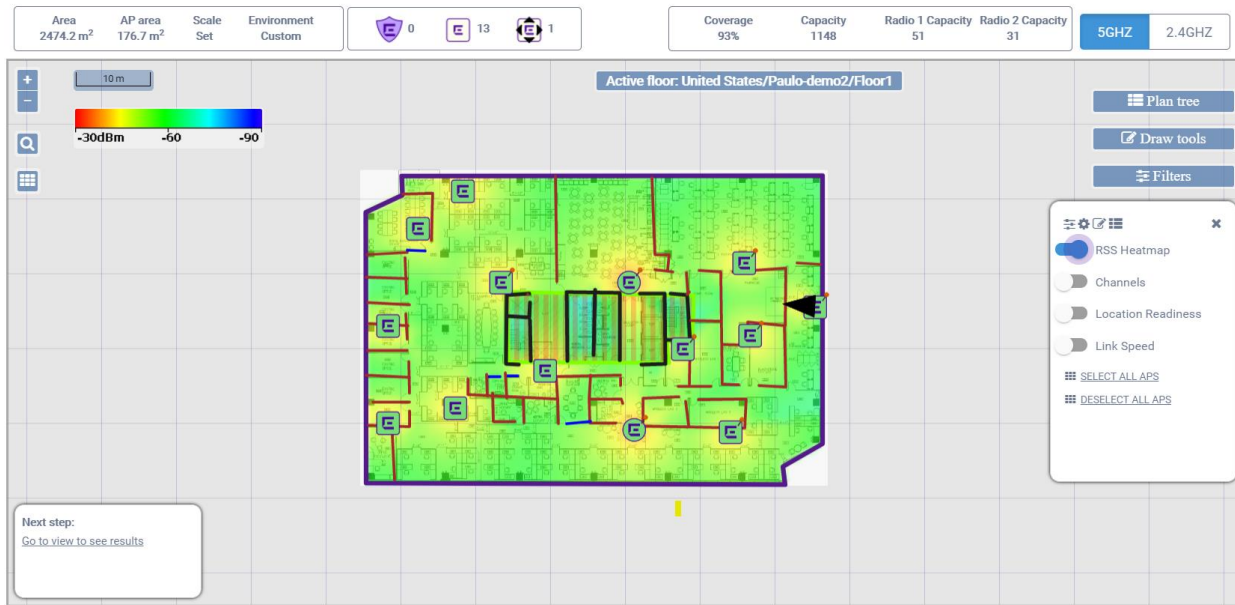


Visualization

Several visualization tools are available to help you visualize the resulting coverage on both 2.4GHz and 5.0Ghz frequencies:

1. RF Coverage Heat map – provides assessment of signal strength coverage of the floor plan.
2. Channel Plan – provides an optimized view of a representative channel plan to reduce co-channel interference.

3. Location Visualization – provides an assessment of the deployment’s readiness to support fidelity in triangulation. The tool provides the ability to recommend where to install full-size sensors to improve location fidelity, augmenting without impacting the current deployment for coverage. The additional added benefit of full-time sensors is that they can perform double-duty by complementing optional Wireless Intrusion Detection and Prevention integration solutions.
4. Link Speed – provides a generalized link speed estimate for typical clients based on the signal coverage metrics.



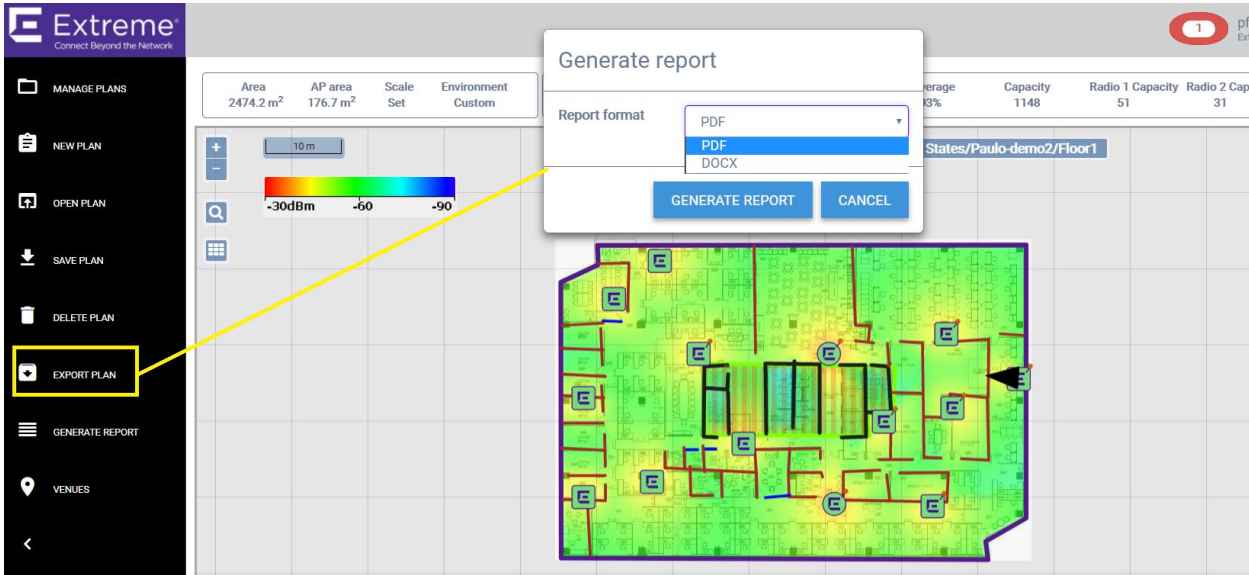
5. Provides visualization of the angle of orientation for the AP-Camera model (AP3916i).
6. Provides an assessment of Bluetooth Low Energy coverage for models that support iBeacon transmit functions (for example, AP391xx and AP7632/62).

Sharing and Exporting

After the model provides your desired coverage characteristics, installed devices, and placement suggestions, you can conveniently share this information – with a partner or customer, or for placing orders – by exporting the model as a PDF or as a Microsoft Word document.

The resulting document includes all of the details provided in the model: the criteria used as input for the model, the representative floor plan of installation locations, the snapshot of RF coverage, and Channel Plan heat maps.

More important, these documents provide a summarized Bill of Materials (BOM) listing the corresponding types and number of APs determined for site coverage. The PDF document is Extreme Networks branded and can be shared directly with the customer or partner. The Microsoft Word document allows for editing, re-arranging, or even branding of the final report.



APs by Country, Building and Floor

United States - Paulo-demo2

Floor	Product Name	Product Part Number	Quantity
Floor1	WS-AP3915i-FCC	31028	11
Floor1	WS-AP3916ic-FCC	31034	2
Floor1	WS-AP3935e-FCC	31014	1
Total APs for 'Paulo-demo2':			14
Total APs in Plan:			14

Product Lifecycle – Exporting into Other Products

The model representation can be directly exported for use by ExtremeWireless management tools such as ExtremeCloud, ExtremeCloud Appliance, and Extreme Management Center. This capability allows reuse of a predictive model into an actual deployed model. This allows users to map actual deployed equipment into the predicted installation instances. The details of the floor plans are preserved – saving time in getting visibility of the actual installation deployment.

RF Survey Tools

Conducting a site survey with the ExtremeWireless™ RF Planning Tool can be enhanced with the use of third-party survey tools. The key part to a new deployment is providing a predictive or active survey assessment as part of the design.

Predictive and active site surveys can be done using a variety of third-party tools such as Ekahau, Netscout's AirMagnet tool, and others. Attributes from an Ekahau survey can be imported directly into the ExtremeWireless and ExtremeCloud products.

Design Considerations

Network Time Protocol (NTP)

Deploying the Extreme Networks' Automated Campus solution requires time synchronization between Extreme's applications, switches, and other network components to function properly and communicate efficiently. Log and syslog events also benefit when all network applications and components are synchronized, along with synchronization of alarm events generated within Extreme Management Center.

Effective synchronization often means faster and easier resolution of network problems.

To maintain optimal synchronization within the ecosystem of Extreme's Automated Campus Solution, we recommend the use of NTP for Extreme Management Center, Extreme Access Control, ExtremeAnalytics, ExtremeWireless Controllers, Extreme switches, and any third-party servers (such as RADIUS servers).

Note

Configuration for third-party RADIUS servers is not documented in this section.

Extreme Management Center

Extreme Management Center NTP configuration is executed during installation using the command-line interface. Once the appliance is installed, log in to the console as root. The install process starts with a series of configuration questions. The administrator is prompted for NTP configuration under the **<Configure Date And Time Settings>** section of the install. If the administrator chooses to change the settings after install, a simple run of the **dateconfig** script can be executed. The **dateconfig** script is located in `/usr/postinstall`.

```
Please enter a NTP Server IP Address (Required): <ntp_ip_address_2>

Would you like to add another server (y/n) [n]?
=====
NTP Servers
=====
These are the currently specified NTP servers:

<ntp_ip_address_1>
<ntp_ip_address_2>

Enter 0 or any key other than a valid selection to complete NTP configuration and continue.
If you need to make a change, enter the appropriate number from the
choices listed below.

0. Accept the current settings and continue
1. Restart NTP server selection
2. Set date and time manually
=====

Enter selection [0]:
=====
Set Time Zone
=====
You will now be asked to enter the time zone information for this system.
Available time zones are stored in files in the /usr/share/zoneinfo directory.
Please select from one of the following example time zones:

1. US Eastern
```

```

2. US Central
3. US Mountain
4. US Pacific
5. Other - Shows a graphical list
=====

```

```
Enter selection [1]:
```

```

Current default time zone: 'America/New_York'
Local time is now:      Thu Jun 21 15:30:00 EDT 2018.
Universal Time is now:  Thu Jun 21 19:30:00 UTC 2018.

```

- Print the following to the console if synchronization is successful after the selection of the timezone with the post install script <dateconfig>:

```

The time was successfully synchronized to the server at <ntp_ip_address_1>
rsyslog start/running, process 21801
* Starting NTP server ntpd                                     [ OK ]

```

The command <ntpq -np> will also display pertinent information about NTP daemon operation and performance – including statistics about delay, offset, and jitter.

```

root@XMC:/# ntpq -np
  remote                       refid                      st t when poll reach  delay  offset  jitter
=====
0.ubuntu.pool.n .POOL.                    16 p   - 64    0   0.000  0.000  0.000
1.ubuntu.pool.n .POOL.                    16 p   - 64    0   0.000  0.000  0.000
2.ubuntu.pool.n .POOL.                    16 p   - 64    0   0.000  0.000  0.000
3.ubuntu.pool.n .POOL.                    16 p   - 64    0   0.000  0.000  0.000
ntp.ubuntu.com  .POOL.                    16 p   - 64    0   0.000  0.000  0.000
*<ntp_ip_address_1> 129.6.15.29              2 u   45 64   377   2.867  1.833  0.751
+<ntp_ip_address_2> 129.6.15.29              2 u   37 64   377   2.669  2.899  3.512
                                     [ OK ]

```

ExtremeControl

ExtremeControl NTP configuration is executed during installation within the command-line interface. Once the appliance is installed, log in to the console as root. The install process starts with a series of configuration questions. The administrator is prompted for NTP configuration under the **<Configure Date And Time Settings>** section of the install. If the administrator chooses to change the settings after install, a simple run of the dateconfig script can be executed. The dateconfig script is located in /usr/postinstall.

```

=====
Configure Date And Time Settings
=====

```

```

The engine date and time can be set manually or using an external
Network Time Protocol (NTP) server. It is strongly recommended that
NTP is used to configure the date and time to ensure accuracy of time
values for SNMP communications and logged events. Up to 5
server IP addresses may be entered if NTP is used.
=====

```

```
Do you want to use NTP (y/n) [y]? y
```

```
Please enter a NTP Server IP Address [<ntp_ip_address_1>]: <ntp_ip_address_1>
```

```
Would you like to add another server (y/n) [y]?
```

```
Please enter a NTP Server IP Address [<ntp_ip_address_2>]: <ntp_ip_address_2>
```

```
Would you like to add another server (y/n) [n]?
```

```
=====
NTP Servers
=====
```

```
These are the currently specified NTP servers:
```

```
<ntp_ip_address_1>
```

```
<ntp_ip_address_2>
```

```
Enter 0 or any key other than a valid selection to complete NTP configuration and continue.
If you need to make a change, enter the appropriate number from the
choices listed below.
```

- ```
0. Accept the current settings and continue
1. Restart NTP server selection
2. Set date and time manually
=====
```

```
Enter selection [0]:
```

```
=====
Set Time Zone
=====
```

```
You will now be asked to enter the time zone information for this system.
Available time zones are stored in files in the /usr/share/zoneinfo directory.
Please select from one of the following example time zones:
```

- ```
1. US Eastern
2. US Central
3. US Mountain
4. US Pacific
5. Other - Shows a graphical list
=====
```

```
Enter selection [1]:
```

```
Current default time zone: 'America/New_York'
```

```
Local time is now: Thu Jun 21 19:38:04 EDT 2018.
```

```
Universal Time is now: Thu Jun 21 23:38:04 UTC 2018.d
```

Print the following to the console if synchronization is successful after the selection of the timezone with the post install script <dateconfig>:

```
The time was successfully synchronized to the server at <ntp_ip_address_1>
rsyslog start/running, process 2123
```

```
* Starting NTP server ntpd
```

```
[ OK ]
```

The command <ntpq -np> will also display pertinent information about the NTP daemon operation and performance – including statistics about delay, offset, and jitter.

```
root@NAC:/# ntpq -np
      remote           refid      st t when poll reach  delay  offset  jitter
=====
0.ubuntu.pool.n .POOL.    16 p   - 64    0   0.000  0.000  0.000
1.ubuntu.pool.n .POOL.    16 p   - 64    0   0.000  0.000  0.000
2.ubuntu.pool.n .POOL.    16 p   - 64    0   0.000  0.000  0.000
3.ubuntu.pool.n .POOL.    16 p   - 64    0   0.000  0.000  0.000
ntp.ubuntu.com .POOL.    16 p   - 64    0   0.000  0.000  0.000
#<ntp_ip_address_1> 129.6.15.29  2 u   48   64  377   2.445 -11.077  0.910
#<ntp_ip_address_2> 129.6.15.29  2 u   42   64  377   2.715  -2.139  2.747
```

ExtremeAnalytics

ExtremeAnalytics NTP configuration is executed during installation within the command-line interface. Once the appliance is installed, log in to the console as root. The install process starts with a series of configuration questions. The administrator is prompted for the NTP configuration under the **<Configure Date And Time Settings>** section of the install. If the administrator chooses to change the settings after install, a simple run of the dateconfig script can be executed. The dateconfig script is located in /usr/postinstall.

```

Configure Date And Time Settings
=====
The engine date and time can be set manually or using an external
Network Time Protocol (NTP) server. It is strongly recommended that
NTP is used to configure the date and time to ensure accuracy of time
values for SNMP communications and logged events. Up to 5
server IP addresses may be entered if NTP is used.
=====

Do you want to use NTP (y/n) [n]? y

Please enter a NTP Server IP Address (Required): <ntp_ip_address_1>

Would you like to add another server (y/n) [n]? y

Please enter a NTP Server IP Address (Required): <ntp_ip_address_2>

Would you like to add another server (y/n) [n]?
=====
NTP Servers
=====
These are the currently specified NTP servers:

<ntp_ip_address_1>
<ntp_ip_address_2>

Enter 0 or any key other than a valid selection to complete NTP configuration and continue.
If you need to make a change, enter the appropriate number from the
choices listed below.

0. Accept the current settings and continue
1. Restart NTP server selection
2. Set date and time manually
=====
Enter selection [0]:
=====
Set Time Zone
=====
You will now be asked to enter the time zone information for this system.
Available time zones are stored in files in the /usr/share/zoneinfo directory.
Please select from one of the following example time zones:

1. US Eastern
2. US Central
3. US Mountain
4. US Pacific
5. Other - Shows a graphical list
=====
Enter selection [1]:

Current default time zone: 'America/New_York'
Local time is now:      Thu Jun 21 21:10:23 EDT 2018.
Universal Time is now:  Fri Jun 22 01:10:23 UTC 2018.
=====

```

Print the following to the console if synchronization is successful after the selection of the timezone with the post install script <dateconfig>:

```
The time was successfully synchronized to the server at <ntp_ip_address_1>
rsyslog start/running, process 27186

* Starting NTP server ntpd                                     [ OK ]
```

The command <ntpq -np> will also display pertinent information about the NTP daemon operation and performance – including statistics about delay, offset, and jitter.

```
root@EA:/# ntpq -np
      remote           refid      st t when poll reach   delay   offset  jitter
=====
0.ubuntu.pool.n .POOL.        16 p   - 64    0    0.000   0.000   0.000
1.ubuntu.pool.n .POOL.        16 p   - 64    0    0.000   0.000   0.000
2.ubuntu.pool.n .POOL.        16 p   - 64    0    0.000   0.000   0.000
3.ubuntu.pool.n .POOL.        16 p   - 64    0    0.000   0.000   0.000
ntp.ubuntu.com  .POOL.        16 p   - 64    0    0.000   0.000   0.000
+<ntp_ip_address_1> 132.163.96.2  2 u   48  64  377   2.359  -26.569   8.534
*<ntp_ip_address_2> 132.163.96.2  2 u   37  64  377   2.530  -27.124  28.495
```

ExtremeWireless Controllers

ExtremeWireless Controller NTP configuration is accessed through the User Interface located at **Controller → Network → Network Time**. In the Network Time panel, the timezone and up to 3 NTP servers can be added. After filling in the fields, click **Apply**.

The screenshot displays the 'Network Time' configuration page in the ExtremeWireless Controller UI. The page is divided into several sections:

- Time Zone Settings:** Includes dropdown menus for 'Continent or Ocean' (set to America) and 'Time Zone Region' (set to New_York - Eastern (most areas)). An 'Apply Time Zone' button is present.
- System Time:** Shows the current system time as 07-29-2018 15:35 with a 'Set Clock' button.
- NTP Configuration:** This section is highlighted with a red box. It features a checked checkbox for 'NTP', three input fields for 'Time Server 1', 'Time Server 2', and 'Time Server 3'. The first two fields contain the placeholder text 'x.x.x.x'. Below these fields is an unchecked checkbox for 'Run local NTP Server' and an 'Apply' button.

The bottom status bar of the UI shows: [EWC1a | V2110 Small | 19 days, 07:20] User: netadmin [M] [1] [2] [L] Software: 10.41.07.0014 | Admin Users: 3 © 2006-2018 Extreme Networks. All Rights Reserved.

To verify NTP server settings, log in to the console and enter the command <time>. Then enter the command <show ntpip>. The following output should be displayed:

```
EWCl1a.SQA.net:time# show ntpip
ntpip 1 <ntp_ip_address_1>
ntpip 2 <ntp_ip_address_2>
```

Extreme Switches

Extreme Switch SNTP configuration is executed through the command-line-interface. SNTP is enabled on the VR level. The following are examples of the SNTP configuration within this Validated Design:

Summit Access Switches

```
config timezone name EST -300 autodst
configure sntp-client primary <ntp_ip_address_1> vr VR-Default
configure sntp-client secondary <ntp_ip_address_2> vr VR-Default
configure sntp-client update-interval 60
enable sntp-client
```

To verify the SNTP daemon is synched with the NTP server, enter the command <show sntp>:

```
(Private) Slot-1 Stack.1 # show sntp
SNTP client is enabled
SNTP time is valid
Primary server: <ntp_ip_address_1> VR-Default
Secondary server: tp_ip_adderss_2> VR-Default
Broadcasts: VR-Mgmt
Query interval:60
Last valid SNTP update: From server:<ntp_ip_address_1>, on Mon Jul 30 08:53:57 2018

SNTPC Statistics:
Packets transmitted:
  to primary server:          4923
  to secondary server:        9
Packets received with valid time:
  from Primary server:       4914
  from Secondary server:      8
  from Broadcast server:     0
Packets received without valid time:
  from Primary server:        0
  from Secondary server:      0
  from Broadcast server:      0
Replies not received to requests:
  from Primary server:        9
  from Secondary server:      1
```

ERS Access Switches

```
sntp server primary address 134.141.79.190
sntp server secondary address 134.141.79.191
sntp enable
sntp sync-interval 1
clock source sntp
clock time-zone EST -5
```

To verify the SNTP daemon is synched with the NTP server, enter the command `<show sntp>`:

```
ERS-4900(config)#show sntp
SNTP Status:                Enabled
Primary server address:     134.141.79.190
Secondary server address:  134.141.79.191
Sync interval:              1 hours
Last sync source:          134.141.79.190
Primary server sync failures: 0
Secondary server sync failures: 0
Last sync time:            2018-12-08 19:30:48 GMT-05:00
Next sync time:            2018-12-08 20:30:48 GMT-05:00
Current time:              2018-12-08 20:24:33 GMT-05:00
```

Fabric Connect Switches

```
clock time-zone EST
no ntp
ntp server <ntp_ip_address_1>
ntp server <ntp_ip_address_2>
ntp interval 60
ntp
```

To verify the NTP daemon is synched with the NTP server, enter the command `<show ntp>`:

```
BEB-8284-50:1(config)#show ntp

=====
                                NTP
=====
Version   Enabled      Interval    Last Update Time                Synchronized To
-----
3         True         60         Mon Jul 30 07:47:33 2018 EST    <ntp_ip_address_1>
```

DHCP/BOOTP Relay Agent

A DHCP Relay agent relays DHCP requests from the client to the DHCP server, and relays the DHCP replies from the server to the client. It acts as a proxy and can reduce the number of DHCP servers required in the network. The DHCP relay agent inserts its own IP address in the giaddr field (gateway address) of the DHCP request. The DHCP server looks into this IP address, identifies the DHCP client's subnet, and assigns an IP address accordingly.

DHCP Relay is configured in the domain the IP interface was created (GRT or VRF) and must also be enabled on the IP interface. Redundant DHCP servers are present in this design. The following is the DHCP Relay configuration for this Validated Design:

Fabric Connect Switches (BEB-110):

- Global configuration:

```
ip dhcp-relay fwd-path 172.10.10.1 172.9.99.105
ip dhcp-relay fwd-path 172.10.10.1 172.9.99.105 enable
ip dhcp-relay fwd-path 172.10.10.1 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.10.10.1 172.9.99.115
ip dhcp-relay fwd-path 172.10.10.1 172.9.99.115 enable
ip dhcp-relay fwd-path 172.10.10.1 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.10.24.1 172.9.99.105
ip dhcp-relay fwd-path 172.10.24.1 172.9.99.105 enable
ip dhcp-relay fwd-path 172.10.24.1 172.9.99.105 mode bootp_dhcp
```

```

ip dhcp-relay fwd-path 172.10.24.1 172.9.99.115
ip dhcp-relay fwd-path 172.10.24.1 172.9.99.115 enable
ip dhcp-relay fwd-path 172.10.24.1 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.10.28.1 172.9.99.105
ip dhcp-relay fwd-path 172.10.28.1 172.9.99.105 enable
ip dhcp-relay fwd-path 172.10.28.1 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.10.28.1 172.9.99.115
ip dhcp-relay fwd-path 172.10.28.1 172.9.99.115 enable
ip dhcp-relay fwd-path 172.10.28.1 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.0.2 172.9.99.105
ip dhcp-relay fwd-path 172.105.0.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.0.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.0.2 172.9.99.115
ip dhcp-relay fwd-path 172.105.0.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.0.2 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.1.2 172.9.99.105
ip dhcp-relay fwd-path 172.105.1.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.1.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.1.2 172.9.99.115
ip dhcp-relay fwd-path 172.105.1.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.1.2 172.9.99.115 mode bootp_dhcp

router vrf iot
ip dhcp-relay fwd-path 172.10.20.1 172.9.99.105
ip dhcp-relay fwd-path 172.10.20.1 172.9.99.105 enable
ip dhcp-relay fwd-path 172.10.20.1 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.10.20.1 172.9.99.115
ip dhcp-relay fwd-path 172.10.20.1 172.9.99.115 enable
ip dhcp-relay fwd-path 172.10.20.1 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.2.2 172.9.99.105
ip dhcp-relay fwd-path 172.105.2.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.2.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.2.2 172.9.99.115
ip dhcp-relay fwd-path 172.105.2.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.2.2 172.9.99.115 mode bootp_dhcp
exit

router vrf surveillance
ip dhcp-relay fwd-path 172.10.32.1 172.9.99.105
ip dhcp-relay fwd-path 172.10.32.1 172.9.99.105 enable
ip dhcp-relay fwd-path 172.10.32.1 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.10.32.1 172.9.99.115
ip dhcp-relay fwd-path 172.10.32.1 172.9.99.115 enable
ip dhcp-relay fwd-path 172.10.32.1 172.9.99.115 mode bootp_dhcp
exit

```

- Interface configuration:

```

interface vlan 100
ip dhcp-relay
exit

interface vlan 102
ip dhcp-relay
exit

interface vlan 103
ip dhcp-relay
exit

interface vlan 1050
ip dhcp-relay
exit

interface vlan 1051

```

```

ip dhcp-relay
exit

interface vlan 1052
vrf iot
ip dhcp-relay
exit

interface vlan 101
vrf iot
ip dhcp-relay
exit

interface vlan 104
vrf surveillance
ip dhcp-relay
exit

```

Fabric Connect Switches (BEB-111):

- Global configuration:

```

ip dhcp-relay fwd-path 172.10.10.2 172.9.99.105
ip dhcp-relay fwd-path 172.10.10.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.10.10.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.10.10.2 172.9.99.115
ip dhcp-relay fwd-path 172.10.10.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.10.10.2 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.10.24.2 172.9.99.105
ip dhcp-relay fwd-path 172.10.24.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.10.24.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.10.24.2 172.9.99.115
ip dhcp-relay fwd-path 172.10.24.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.10.24.2 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.10.28.2 172.9.99.105
ip dhcp-relay fwd-path 172.10.28.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.10.28.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.10.28.2 172.9.99.115
ip dhcp-relay fwd-path 172.10.28.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.10.28.2 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.0.3 172.9.99.105
ip dhcp-relay fwd-path 172.105.0.3 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.0.3 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.0.3 172.9.99.115
ip dhcp-relay fwd-path 172.105.0.3 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.0.3 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.1.3 172.9.99.105
ip dhcp-relay fwd-path 172.105.1.3 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.1.3 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.1.3 172.9.99.115
ip dhcp-relay fwd-path 172.105.1.3 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.1.3 172.9.99.115 mode bootp_dhcp

router vrf iot
ip dhcp-relay fwd-path 172.10.20.2 172.9.99.105
ip dhcp-relay fwd-path 172.10.20.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.10.20.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.10.20.2 172.9.99.115
ip dhcp-relay fwd-path 172.10.20.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.10.20.2 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.2.3 172.9.99.105
ip dhcp-relay fwd-path 172.105.2.3 172.9.99.105 enable

```

```
ip dhcp-relay fwd-path 172.105.2.3 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.2.3 172.9.99.115
ip dhcp-relay fwd-path 172.105.2.3 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.2.3 172.9.99.115 mode bootp_dhcp
exit
router vrf surveillance
ip dhcp-relay fwd-path 172.10.32.2 172.9.99.105
ip dhcp-relay fwd-path 172.10.32.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.10.32.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.10.32.2 172.9.99.115
ip dhcp-relay fwd-path 172.10.32.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.10.32.2 172.9.99.115 mode bootp_dhcp
exit
```

- Interface configuration:

```
interface vlan 100
ip dhcp-relay
exit

interface vlan 102
ip dhcp-relay
exit

interface vlan 103
ip dhcp-relay
exit

interface vlan 1050
ip dhcp-relay
exit

interface vlan 1051
ip dhcp-relay
exit

interface vlan 1052
vrf iot
ip dhcp-relay
exit

interface vlan 101
vrf iot
ip dhcp-relay
exit

interface vlan 104
vrf surveillance
ip dhcp-relay
exit
```

Fabric Connect Switches (BEB-210):

- Global configuration:

```

ip dhcp-relay fwd-path 172.20.10.1 172.9.99.105
ip dhcp-relay fwd-path 172.20.10.1 172.9.99.105 enable
ip dhcp-relay fwd-path 172.20.10.1 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.20.10.1 172.9.99.115
ip dhcp-relay fwd-path 172.20.10.1 172.9.99.115 enable
ip dhcp-relay fwd-path 172.20.10.1 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.20.24.1 172.9.99.105
ip dhcp-relay fwd-path 172.20.24.1 172.9.99.105 enable
ip dhcp-relay fwd-path 172.20.24.1 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.20.24.1 172.9.99.115
ip dhcp-relay fwd-path 172.20.24.1 172.9.99.115 enable
ip dhcp-relay fwd-path 172.20.24.1 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.20.28.1 172.9.99.105
ip dhcp-relay fwd-path 172.20.28.1 172.9.99.105 enable
ip dhcp-relay fwd-path 172.20.28.1 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.20.28.1 172.9.99.115
ip dhcp-relay fwd-path 172.20.28.1 172.9.99.115 enable
ip dhcp-relay fwd-path 172.20.28.1 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.0.4 172.9.99.105
ip dhcp-relay fwd-path 172.105.0.4 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.0.4 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.0.4 172.9.99.115
ip dhcp-relay fwd-path 172.105.0.4 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.0.4 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.1.4 172.9.99.105
ip dhcp-relay fwd-path 172.105.1.4 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.1.4 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.1.4 172.9.99.115
ip dhcp-relay fwd-path 172.105.1.4 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.1.4 172.9.99.115 mode bootp_dhcp

```

DHCP relay configured on each VLAN interface in the GRT, pointed to both DHCP servers.

router vrf iot

```

ip dhcp-relay fwd-path 172.20.20.1 172.9.99.105
ip dhcp-relay fwd-path 172.20.20.1 172.9.99.105 enable
ip dhcp-relay fwd-path 172.20.20.1 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.20.20.1 172.9.99.115
ip dhcp-relay fwd-path 172.20.20.1 172.9.99.115 enable
ip dhcp-relay fwd-path 172.20.20.1 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.2.4 172.9.99.105
ip dhcp-relay fwd-path 172.105.2.4 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.2.4 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.2.4 172.9.99.115
ip dhcp-relay fwd-path 172.105.2.4 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.2.4 172.9.99.115 mode bootp_dhcp
exit

```

router vrf surveillance

```

ip dhcp-relay fwd-path 172.20.32.1 172.9.99.105
ip dhcp-relay fwd-path 172.20.32.1 172.9.99.105 enable
ip dhcp-relay fwd-path 172.20.32.1 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.20.32.1 172.9.99.115
ip dhcp-relay fwd-path 172.20.32.1 172.9.99.115 enable
ip dhcp-relay fwd-path 172.20.32.1 172.9.99.115 mode bootp_dhcp
exit

```

- Interface configuration:

```

interface vlan 200
ip dhcp-relay
exit

interface vlan 202
ip dhcp-relay
exit

interface vlan 203
ip dhcp-relay
exit

interface vlan 1050
ip dhcp-relay
exit

interface vlan 1051
ip dhcp-relay
exit

interface vlan 1052
vrf iot
ip dhcp-relay
exit

interface vlan 201
vrf iot
ip dhcp-relay
exit

interface vlan 204
vrf surveillance
ip dhcp-relay
exit

```

DHCP relay enabled on
VLAN interfaces in the GRT.

DHCP relay enabled on
VLAN interfaces in the VRFs.

Fabric Connect Switches (BEB-211):

- Global configuration:

```

ip dhcp-relay fwd-path 172.20.10.2 172.9.99.105
ip dhcp-relay fwd-path 172.20.10.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.20.10.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.20.10.2 172.9.99.115
ip dhcp-relay fwd-path 172.20.10.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.20.10.2 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.20.24.2 172.9.99.105
ip dhcp-relay fwd-path 172.20.24.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.20.24.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.20.24.2 172.9.99.115
ip dhcp-relay fwd-path 172.20.24.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.20.24.2 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.20.28.2 172.9.99.105
ip dhcp-relay fwd-path 172.20.28.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.20.28.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.20.28.2 172.9.99.115
ip dhcp-relay fwd-path 172.20.28.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.20.28.2 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.0.5 172.9.99.105
ip dhcp-relay fwd-path 172.105.0.5 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.0.5 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.0.5 172.9.99.115
ip dhcp-relay fwd-path 172.105.0.5 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.0.5 172.9.99.115 mode bootp_dhcp

```

```

ip dhcp-relay fwd-path 172.105.1.5 172.9.99.105
ip dhcp-relay fwd-path 172.105.1.5 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.1.5 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.1.5 172.9.99.115
ip dhcp-relay fwd-path 172.105.1.5 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.1.5 172.9.99.115 mode bootp_dhcp

router vrf iot
ip dhcp-relay fwd-path 172.20.20.2 172.9.99.105
ip dhcp-relay fwd-path 172.20.20.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.20.20.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.20.20.2 172.9.99.115
ip dhcp-relay fwd-path 172.20.20.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.20.20.2 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.2.5 172.9.99.105
ip dhcp-relay fwd-path 172.105.2.5 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.2.5 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.2.5 172.9.99.115
ip dhcp-relay fwd-path 172.105.2.5 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.2.5 172.9.99.115 mode bootp_dhcp
exit

router vrf surveillance
ip dhcp-relay fwd-path 172.20.32.2 172.9.99.105
ip dhcp-relay fwd-path 172.20.32.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.20.32.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.20.32.2 172.9.99.115
ip dhcp-relay fwd-path 172.20.32.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.20.32.2 172.9.99.115 mode bootp_dhcp
exit

```

- Interface configuration:

```

interface vlan 200
ip dhcp-relay
exit

interface vlan 202
ip dhcp-relay
exit

interface vlan 203
ip dhcp-relay
exit

interface vlan 1050
ip dhcp-relay
exit

interface vlan 1051
ip dhcp-relay
exit

interface vlan 1052
vrf iot
ip dhcp-relay
exit

interface vlan 201
vrf iot
ip dhcp-relay
exit
interface vlan 204
vrf surveillance
ip dhcp-relay
exit

```


Fabric Connect Switches (BEB-310):

- Global configuration:

```

ip dhcp-relay fwd-path 172.30.10.1 172.9.99.105
ip dhcp-relay fwd-path 172.30.10.1 172.9.99.105 enable
ip dhcp-relay fwd-path 172.30.10.1 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.30.10.1 172.9.99.115
ip dhcp-relay fwd-path 172.30.10.1 172.9.99.115 enable
ip dhcp-relay fwd-path 172.30.10.1 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.30.24.1 172.9.99.105
ip dhcp-relay fwd-path 172.30.24.1 172.9.99.105 enable
ip dhcp-relay fwd-path 172.30.24.1 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.30.24.1 172.9.99.115
ip dhcp-relay fwd-path 172.30.24.1 172.9.99.115 enable
ip dhcp-relay fwd-path 172.30.24.1 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.30.28.1 172.9.99.105
ip dhcp-relay fwd-path 172.30.28.1 172.9.99.105 enable
ip dhcp-relay fwd-path 172.30.28.1 172.9.99.105 mode bootp_dhcp

ip dhcp-relay fwd-path 172.30.28.1 172.9.99.115
ip dhcp-relay fwd-path 172.30.28.1 172.9.99.115 enable
ip dhcp-relay fwd-path 172.30.28.1 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.0.6 172.9.99.105
ip dhcp-relay fwd-path 172.105.0.6 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.0.6 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.0.6 172.9.99.115
ip dhcp-relay fwd-path 172.105.0.6 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.0.6 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.1.6 172.9.99.105
ip dhcp-relay fwd-path 172.105.1.6 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.1.6 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.1.6 172.9.99.115
ip dhcp-relay fwd-path 172.105.1.6 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.1.6 172.9.99.115 mode bootp_dhcp

router vrf iot
ip dhcp-relay fwd-path 172.30.20.1 172.9.99.105
ip dhcp-relay fwd-path 172.30.20.1 172.9.99.105 enable
ip dhcp-relay fwd-path 172.30.20.1 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.30.20.1 172.9.99.115
ip dhcp-relay fwd-path 172.30.20.1 172.9.99.115 enable
ip dhcp-relay fwd-path 172.30.20.1 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.2.6 172.9.99.105
ip dhcp-relay fwd-path 172.105.2.6 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.2.6 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.2.6 172.9.99.115
ip dhcp-relay fwd-path 172.105.2.6 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.2.6 172.9.99.115 mode bootp_dhcp
exit

router vrf surveillance
ip dhcp-relay fwd-path 172.30.32.1 172.9.99.105
ip dhcp-relay fwd-path 172.30.32.1 172.9.99.105 enable
ip dhcp-relay fwd-path 172.30.32.1 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.30.32.1 172.9.99.115
ip dhcp-relay fwd-path 172.30.32.1 172.9.99.115 enable
ip dhcp-relay fwd-path 172.30.32.1 172.9.99.115 mode bootp_dhcp
exit

```

- Interface configuration:

```

interface vlan 300
ip dhcp-relay
exit

interface vlan 302
ip dhcp-relay
exit

interface vlan 303
ip dhcp-relay
exit

interface vlan 1050
ip dhcp-relay
exit

interface vlan 1051
ip dhcp-relay
exit

interface vlan 1052
vrf iot
ip dhcp-relay
exit

interface vlan 301
vrf iot
ip dhcp-relay
exit

interface vlan 304
vrf surveillance
ip dhcp-relay
exit

```

Fabric Connect Switches (BEB-311):

- Global configuration:

```

ip dhcp-relay fwd-path 172.30.10.2 172.9.99.105
ip dhcp-relay fwd-path 172.30.10.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.30.10.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.30.10.2 172.9.99.115
ip dhcp-relay fwd-path 172.30.10.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.30.10.2 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.30.24.2 172.9.99.105
ip dhcp-relay fwd-path 172.30.24.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.30.24.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.30.24.2 172.9.99.115
ip dhcp-relay fwd-path 172.30.24.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.30.24.2 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.30.28.2 172.9.99.105
ip dhcp-relay fwd-path 172.30.28.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.30.28.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.30.28.2 172.9.99.115
ip dhcp-relay fwd-path 172.30.28.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.30.28.2 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.0.7 172.9.99.105
ip dhcp-relay fwd-path 172.105.0.7 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.0.7 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.0.7 172.9.99.115
ip dhcp-relay fwd-path 172.105.0.7 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.0.7 172.9.99.115 mode bootp_dhcp

```

```

ip dhcp-relay fwd-path 172.105.1.7 172.9.99.105
ip dhcp-relay fwd-path 172.105.1.7 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.1.7 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.1.7 172.9.99.115
ip dhcp-relay fwd-path 172.105.1.7 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.1.7 172.9.99.115 mode bootp_dhcp

router vrf iot
ip dhcp-relay fwd-path 172.30.20.2 172.9.99.105
ip dhcp-relay fwd-path 172.30.20.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.30.20.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.30.20.2 172.9.99.115
ip dhcp-relay fwd-path 172.30.20.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.30.20.2 172.9.99.115 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.2.7 172.9.99.105
ip dhcp-relay fwd-path 172.105.2.7 172.9.99.105 enable
ip dhcp-relay fwd-path 172.105.2.7 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.105.2.7 172.9.99.115
ip dhcp-relay fwd-path 172.105.2.7 172.9.99.115 enable
ip dhcp-relay fwd-path 172.105.2.7 172.9.99.115 mode bootp_dhcp
exit

router vrf surveillance
ip dhcp-relay fwd-path 172.30.32.2 172.9.99.105
ip dhcp-relay fwd-path 172.30.32.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.30.32.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.30.32.2 172.9.99.115
ip dhcp-relay fwd-path 172.30.32.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.30.32.2 172.9.99.115 mode bootp_dhcp
exit

```

- Interface configuration:

```

interface vlan 300
ip dhcp-relay
exit

interface vlan 302
ip dhcp-relay
exit

interface vlan 303
ip dhcp-relay
exit

interface vlan 1050
ip dhcp-relay
exit

interface vlan 1051
ip dhcp-relay
exit

interface vlan 1052
vrf iot
ip dhcp-relay
exit

interface vlan 301
vrf iot
ip dhcp-relay
exit
  interface vlan 304
vrf surveillance
ip dhcp-relay
exit

```

Fabric Connect switches (BEB-910):

- **Global Configuration:** As Guest traffic from the campuses egresses the EWC, the DVR controllers need to be configured to relay the DHCP requests to the DHCP server:

```
ip dhcp-relay fwd-path 172.90.40.2 172.9.99.105
ip dhcp-relay fwd-path 172.90.40.2 172.9.99.105 enable
ip dhcp-relay fwd-path 172.90.40.2 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.90.40.2 172.9.99.115
ip dhcp-relay fwd-path 172.90.40.2 172.9.99.115 enable
ip dhcp-relay fwd-path 172.90.40.2 172.9.99.115 mode bootp_dhcp
```

- **Interface Configuration:**

```
interface Vlan 906
ip dhcp-relay
exit
```

Fabric Connect switches (BEB-920):

- **Global Configuration:** As Guest traffic from the campuses egresses the EWC, the DVR controllers need to be configured to relay the DHCP requests to the DHCP server:

```
ip dhcp-relay fwd-path 172.90.40.3 172.9.99.105
ip dhcp-relay fwd-path 172.90.40.3 172.9.99.105 enable
ip dhcp-relay fwd-path 172.90.40.3 172.9.99.105 mode bootp_dhcp
ip dhcp-relay fwd-path 172.90.40.3 172.9.99.115
ip dhcp-relay fwd-path 172.90.40.3 172.9.99.115 enable
ip dhcp-relay fwd-path 172.90.40.3 172.9.99.115 mode bootp_dhcp
```

- **Interface Configuration:**

```
interface Vlan 906
ip dhcp-relay
exit
```

- **Verification:** To view statistics on requests relayed, enter the command `<show ip dhcp-relay counters>`:

```
Slot-BEB-8284-210:1(config)#show ip dhcp-relay counters
```

```
=====
                        DHCP Counters - GlobalRouter
=====
INTERFACE          IP_ADDRESS          REQUESTS          REPLIES
-----
Vlan200            172.20.10.1          86                161
Vlan202            172.20.24.1          6                 12
Vlan203            172.20.28.1          0                 0
Vlan1050           172.105.0.4          0                 0
Vlan1051           172.105.1.4          47                0
```

Link Layer Discover Protocol (LLDP)

LLDP is enabled by default in Summit and Fabric Connect and is an integral part of the process for the initial discovery of Fabric Attach elements. Fabric Attach uses the IEEE802.1ab LLDP (Link Layer Discovery Protocol) extensions to automatically attach network devices to individual services in a Fabric Connect network.

The Link Layer Discovery Protocol (LLDP), defined by IEEE standard 802.1ab, provides a standard method for discovering physical network devices and their capabilities within a given network management domain. Upon connection and detection of an FA Client, the FA Server (BEB) will advertise (via LLDP) the management I-SID/VLAN to the FA Client.

- The FA client component on the access switches communicates directly with the FA server on the BEB to request VLAN-to-I-SID mappings for user traffic.
- Access switches also support FA Proxy, allowing other FA clients (such as APs) to connect to the FA server through it.
- Both FA client and FA proxy functionality is enabled by default on the access switches.

To view LLDP neighbors on VSP, enter the command `<show lldp neighbor summary>`:

```
BEB-8284-50:1(config)#show lldp neighbor summ
=====
LLDP Neighbor Summary
=====
LOCAL          IP          CHASSIS      REMOTE
PORT          PROT  ADDR          ID          PORT          SYSNAME      SYSDESCR
-----
1/1           LLDP  0.0.0.0       02:04:96:a1:bf:74  2:50          Campus1-Acc2  ExtremeXOS (Stack) version 22~
1/2           LLDP  0.0.0.0       02:04:96:a0:ad:fe  1:50          Stack         ExtremeXOS (Stack) version 22~
1/10          LLDP  160.10.100.52 e4:5d:52:3c:bc:00  1/10         IP_CLOUD_1   VSP-8284XSQ (6.1.50.0)
1/41          LLDP  10.0.0.40     e4:5d:52:43:b8:00  1/41         BEB-8284-40  VSP-8284XSQ (7.1.0.0_B034) (P~
=====
Total Neighbors : 4
```

To view LLDP neighbors on Summit switches, enter the command `<show lldp neighbor>`:

```
Slot-1 Stack.1 # show lldp neighbor

Port      Neighbor      Neighbor
Chassis ID  Port ID      TTL    Age    Neighbor
System Name
=====
1:50      B0:AD:AA:48:18:00  1/2      120    20    BEB-8284-50
2:20      D8:84:66:E3:25:B8  eth0     120    17    C1A1-E325B8
2:22      D8:84:66:57:AA:58  eth0     120    16    C1A1-57AA58
2:50      E4:5D:52:43:B8:00  1/2      120    3     BEB-8284-40
=====
NOTE: The Chassis ID and/or Port ID might be truncated to fit the screen.
```

To view the LLDP neighbors on ERS switches, enter the command `<show lldp neighbor>`:

```
4900_STACK(config)#show lldp neighbor
=====
LLDP neighbor
=====
Port: 2/22  Index: 3          Time: 5 days, 16:14:02
ChassisId: MAC address      d8:84:66:e3:25:b8
PortId:    Interface alias  eth0
SysName:   Acc321-E325B8
SysCap:    W / W           (Supported/Enabled)
```

```

Port: 1/50 Index: 2 Time: 5 days, 16:14:21
ChassisId: MAC address 64:6a:52:ce:0c:00
PortId: Interface name 2/1
SysName: BEB-8404-310
SysCap: rB / rB (Supported/Enabled)
PortDesc: Extreme Networks Virtual Services Platform 8404C Module 8418XSQ - 10GbCX Port
2/1
SysDescr: VSP-8404C (7.1.0.0)

```

Simple Network Management Protocol (SNMPv3)

SNMPv3 is an enhanced standard for SNMP that improves the security and privacy of SNMP access to managed devices and provides sophisticated control of access to the device MIB. The prior standard versions of SNMP, SNMPv1, and SNMPv2c, provided no privacy and little security.

SNMPv3 is designed to be secure against:

- Modification of information, where an in-transit message is altered.
- Masquerades, where an unauthorized entity assumes the identity of an authorized entity.
- Message stream modification, where packets are delayed and/or replayed.
- Disclosure, where packet exchanges are sniffed (examined) and information is learned about the contents.

You can use the access control subsystem to configure whether access to a managed object in a local MIB is allowed for a remote principal. The access control scheme allows you to define access policies based on MIB views, groups, and multiple security levels. In addition, the SNMPv3 target and notification MIBs provide a more procedural approach for generating and filtering of notifications. SNMPv3 objects are stored in non-volatile memory unless specifically assigned to volatile storage. Objects defined as permanent cannot be deleted.

SNMP is disabled by default. If you choose to enable SNMP, the switch follows the interactive script asking you if you want to enable SNMPv1/v2c and/or SNMPv3. SNMP access for a VR has global SNMP status that includes all SNMPv1v2c, SNMPv3 default users and default group status. However, trap receiver configuration and trap enabling/disabling are independent of global SNMP access and are still forwarded on a VR that is disabled for SNMP access.

In order for Extreme Management Center to take advantage of the more secure and robust SNMPv3 XMC, the switches and wireless controllers must be configured for the proper matching credentials and user name. On Extreme Management Center, administration profiles are required to communicate to the network devices and wireless controllers. Following are the steps required to create an Administration Profile (CLI **Credentials** → **Profiles** → **SNMP Credentials**).

Extreme Management Center Profile Configuration - Switching

Profiles are used to define access to the devices in the network by creating identities used for authentication when performing SNMP queries and sets and identities for CLI operations.

A profile can be configured with the SNMP version to be used and the read and write user and security level. It also points to a set of CLI credentials.

In the Automated Campus EVD, a profile that uses SNMPv3 was created and is used by all network devices. For CLI, SSH access is enabled. Authentication for CLI is done via LDAP/RADIUS server. A different SNMPv3 profile is used by the wireless controllers.

- To create new CLI credentials, go to **Administration** → **Profiles** → **CLI Credentials** and click **Add**.

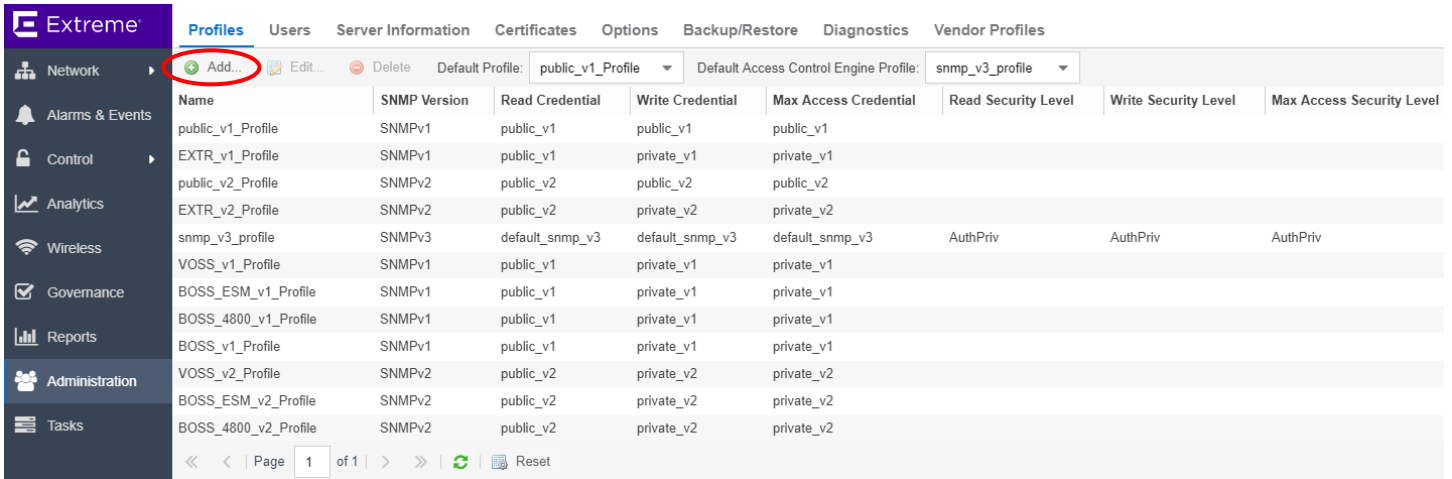
Name	SNMP Version	Read Credential	Write Credential	Max Access Credential	Read Security Level	Write Security Level	Max Access Security Level
public_v1_Profile	SNMPv1	public_v1	public_v1	public_v1			
EXTR_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
public_v2_Profile	SNMPv2	public_v2	public_v2	public_v2			
EXTR_v2_Profile	SNMPv2	public_v2	private_v2	private_v2			
snmp_v3_profile	SNMPv3	default_snmp_v3	default_snmp_v3	default_snmp_v3	AuthPriv	AuthPriv	AuthPriv
VOSS_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
BOSS_ESM_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
BOSS_4800_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
BOSS_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
VOSS_v2_Profile	SNMPv2	public_v2	private_v2	private_v2			
BOSS_ESM_v2_Profile	SNMPv2	public_v2	private_v2	private_v2			
BOSS_4800_v2_Profile	SNMPv2	public_v2	private_v2	private_v2			

Description	User Name	Type	Login Password	Enable Password	Configuration Password
Default	admin	Telnet			
< No Access >					
Default RWA	rwa	Telnet	***		
Default BOSS ESM	admin	SSH	*****		
Default BOSS 4800	RW	Telnet	*****		
Default BOSS	RW	Telnet	*****		
Wireless Controller	admin	SSH	*****	*****	*****
radiusmgmt	xmc	SSH	*****	*****	*****

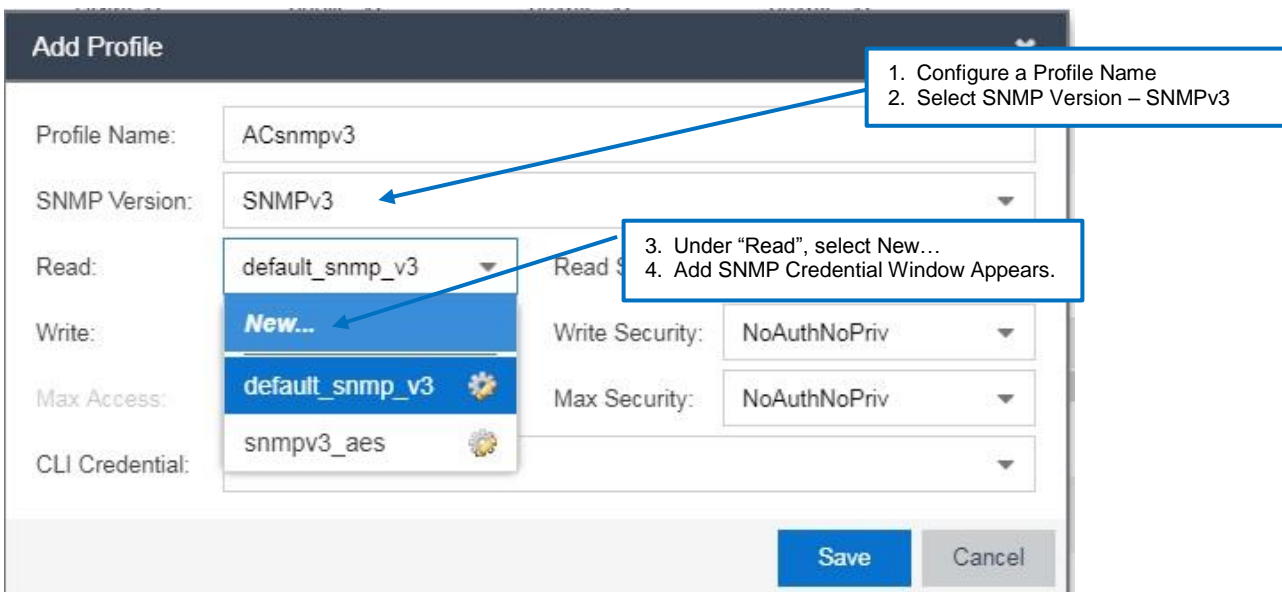
- Only SSH is permitted for management connections to the network devices. Telnet access is disabled.

1. Configure a Description
2. Configure a User Name
3. Configure SSH as the Type.
4. Configure a Login Password.
5. Configure an Enable Password.
6. Configure a Configuration Password.
7. Click Save

- To create a new profile, go to **Administration** → **Profiles** and select **Add** to create a custom SNMP profile:



Name	SNMP Version	Read Credential	Write Credential	Max Access Credential	Read Security Level	Write Security Level	Max Access Security Level
public_v1_Profile	SNMPv1	public_v1	public_v1	public_v1			
EXTR_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
public_v2_Profile	SNMPv2	public_v2	public_v2	public_v2			
EXTR_v2_Profile	SNMPv2	public_v2	private_v2	private_v2			
snmp_v3_profile	SNMPv3	default_snmp_v3	default_snmp_v3	default_snmp_v3	AuthPriv	AuthPriv	AuthPriv
VOSS_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
BOSS_ESM_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
BOSS_4800_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
BOSS_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
VOSS_v2_Profile	SNMPv2	public_v2	private_v2	private_v2			
BOSS_ESM_v2_Profile	SNMPv2	public_v2	private_v2	private_v2			
BOSS_4800_v2_Profile	SNMPv2	public_v2	private_v2	private_v2			



Add Profile

Profile Name: ACsnmpv3

SNMP Version: SNMPv3

Read: default_snmp_v3 (dropdown menu open showing: New..., default_snmp_v3, snmpv3_aes)

Write: NoAuthNoPriv

Max Access: default_snmp_v3

Max Security: NoAuthNoPriv

CLI Credential: snmpv3_aes

Buttons: Save, Cancel

1. Configure a Profile Name
2. Select SNMP Version – SNMPv3
3. Under "Read", select New...
4. Add SNMP Credential Window Appears.

Add SNMP Credential

Credential Name:	snmpv3_aes
SNMP Version:	SNMPv3
User Name:	xmc_v3
Authentication Type:	SHA
Authentication Password:	extreme11
Privacy Type:	AES
Privacy Password:	extreme12extreme

1. Configure a Credential Name.
 2. Select from SNMP Version: SNMPv3.
 3. Configure a User Name.
 4. Select from Authentication Type: MD5.
 5. Configure an Authentication Password.
 6. Select form Privacy Type: AES.
 7. Configure a Privacy Password.
 8. Click Save.

Save Cancel

- The same SNMPv3 user with the same authentication protocol and password and the same privacy protocol and password must be created on the network device.
- Configure the created profile with the new SNMP and CLI credentials:

Add Profile

Profile Name:	ACsnmpv3		
SNMP Version:	SNMPv3		
Read:	snmpv3_aes	Read Security:	AuthPriv
Write:	snmpv3_aes	Write Security:	AuthPriv
Max Access:	snmpv3_aes	Max Security:	AuthPriv
CLI Credential:	ssh		

Use the newly created snmpv3_aes for Read/Write/Max Access.

Use AuthPriv for Read Security/Write Security/Max Security.

Use the newly created ssh CLI credentials.

Save Cancel

Switch Configuration – Extreme Management Center Administration Profile

After the administration profile is configured in Extreme Management Center, the same credentials must be configured on the device in order for Extreme Management Center to manage and configure the device.

Summit Access Switch:

- By default, the SNMPv3 engine-ID is present within the <snmpMaster configuration> module. To match the credentials configured within the Extreme Management Center administrative profile, enter the command <configure snmpv3 add user xmc_v3 authentication sha privacy aes 128>. You will be prompted with a series of password entries that must match the passwords within the administrator profile for Authentication and Privacy.

```
Slot-1 Stack.3 #configure snmpv3 add user xmc_v3 authentication sha privacy aes 128
Authentication password: extreme11
Reenter authentication password: extreme11
Privacy password: extreme12extreme
Reenter privacy password: extreme12extreme
```

- After executing the above command, you should receive output similar to the following when you issue the command <show configuration snmp>:

```
Slot-1 Stack.3 # show config snmp
#
# Module snmpMaster configuration.
#
configure snmpv3 engine-id 03:02:04:96:a1:bf:74
configure snmpv3 add user "xmc_v3" engine-id 80:00:07:7c:03:02:04:96:a1:bf:74 authentication sha
auth-encrypted localized-key
23:24:70:53:44:6f:42:4c:66:74:31:74:4b:35:68:7a:6a:63:39:42:56:58:4c:4a:61:56:6d:68:49:2f:47:42:
74:75:36:6c:31:4a:59:38:37:4d:78:33:4b:45:30:4c:6c:4a:54:6e:51:3d privacy aes 128 privacy-
encrypted localized-key
23:24:67:64:65:6f:79:41:45:2b:59:68:66:63:34:61:67:6a:67:33:44:62:78:6a:37:4e:4d:49:4f:6f:7a:46:
31:34:53:43:79:36:6b:79:44:71:52:71:33:30:4b:41:50:51:56:78:49:3d
```

- Enter the following commands to complete the SNMPv3 configuration for this Validated Design. The following shows the commands and their output.

```
config snmpv3 add group snmpv3group user xmc_v3 sec-model usm
config snmpv3 add access snmpv3group sec-model usm sec-level priv read-view defaultAdminView
write-view defaultAdminView notify-view defaultAdminView
configure snmpv3 add community "private" name "private" user "v1v2c_rw"
configure snmpv3 add community "public" name "public" user "v1v2c_ro"
enable snmp acc snmpv3
disable snmp access snmp-v1v2c
disable snmpv3 default-group
```

- To show SNMP configuration, enter the command `<show configuration snmp>`:

```
Slot-1 Stack.5 # show config snmp
#
# Module snmpMaster configuration.
#
configure snmpv3 engine-id 03:02:04:96:a1:bf:74
configure snmpv3 add user "xmc_v3" engine-id 80:00:07:7c:03:02:04:96:a1:bf:74 authentication sha
auth-encrypted localized-key
23:24:70:53:44:6f:42:4c:66:74:31:74:4b:35:68:7a:6a:63:39:42:56:58:4c:4a:61:56:6d:68:49:2f:47:42:
74:75:36:6c:31:4a:59:38:37:4d:78:33:4b:45:30:4c:6c:4a:54:6e:51:3d privacy aes 128 privacy-
encrypted localized-key
23:24:67:64:65:6f:79:41:45:2b:59:68:66:63:34:61:67:6a:67:33:44:62:78:6a:37:4e:4d:49:4f:6f:7a:46:
31:34:53:43:79:36:6b:79:44:71:52:71:33:30:4b:41:50:51:56:78:49:3d
configure snmpv3 add group "snmpv3group" user "xmc_v3" sec-model usm
configure snmpv3 add access "snmpv3group" sec-model usm sec-level priv read-view
"defaultAdminView" write-view "defaultAdminView" notify-view "defaultAdminView"
configure snmpv3 add community "private" name "private" user "v1v2c_rw"
configure snmpv3 add community "public" name "public" user "v1v2c_ro"
enable snmp access
disable snmp access snmp-v1v2c
enable snmp access snmpv3
disable snmpv3 default-group
```

- Configure parameters for SNMP traps:

```
configure snmpv3 add target-addr "v3AdminAddr" param "v3adminParam" ipaddress 172.9.99.119
transport-port 162 tag-list "TVTrapTag"
configure snmpv3 add target-params "v3adminParam" user "xmc_v3" mp-model snmpv3 sec-model usm
sec-level priv
```

ERS Access Switch:

- Enter SNMPv3 configuration parameters:

```
5928GTS-uPWR(config)#snmp-server name "5900_STACK"
5900_STACK(config)#snmp-server view snmpView +1.3
5900_STACK(config)#snmp-server view adminView +1.3
5900_STACK(config)#snmp-server user xmc_v3 sha aes read-view adminView write-view adminView
notify-view adminView
Enter SHA pass-phrase: *****
Confirm SHA pass-phrase: *****
Enter Aes pass-phrase: *****
Confirm Aes pass-phrase: *****
```

When prompted, enter the SHA and AES passphrases to match XMC's SNMP profile.

To configure the XMC as a trap target:

```
5900_STACK(config)#snmp-server user engine-id 80:00:1f:88:80:c5:04:f2:24:d6:ac:d0:5a xmc_v3 sha
aes
Enter SHA pass-phrase: *****
Confirm SHA pass-phrase: *****
Enter Aes pass-phrase: *****
Confirm Aes pass-phrase: *****
```

Specify the XMC engine-id

When prompted, enter the SHA and AES passphrases to match XMC's SNMP profile.

Note

The ERS requires the engine id be entered into the CLI. This value can be retrieved from the XMC file:

`/usr/local/Extreme_Networks/NetSight/services/snmptrapd.conf`

- To show SNMP configuration, enter the command `<show snmp user>`:

```

Acc-321(config)#show snmp user
-----
User Name: xmc_v3
SNMP Engine ID: 80:00:1F:88:80:C5:04:F2:24:D6:AC:D0:5A
Authentication Protocol: SHA
Privacy Protocol: AES
Storage Type: Non Volatile (NVRAM)
Status: Active
-----
User Name: xmc_v3
SNMP Engine ID: 80:00:02:32:80:02:00:57:58:4C:49:52:37:32:34:50:35:33:30:30:30:32
Authentication Protocol: SHA
Privacy Protocol: AES
Storage Type: Non Volatile (NVRAM)
Status: Active
Views for Unauthenticated Access:
  Read View:
  Write View:
  Notify View:
Views for Authenticated Access:
  Read View:
  Write View:
  Notify View:
Views for Authenticated and Encrypted Access:
  Read View: adminView
  Write View: adminView
  Notify View: adminView
-----
Acc-321(config)#

```

Fabric Connect Switch:

- Enter the following commands to remove the default SNMP settings:

```

no snmp-server community public
no snmp-server community private
no snmp-server user initial
yes
no snmp-server group initial

```

Command will prompt for a **yes/no** confirmation.

- SNMPv3 Configuration:

```

snmp-server view adminView 1.3
snmp-server host 172.9.99.119 v3 authpriv xmc_v3
snmp-server user xmc_v3 group snmpv3group sha extreme11 aes extreme12extreme
snmp-server group snmpv3group "" auth-priv read-view adminView write-view adminView notify-view
adminView
snmp-server authentication-trap enable

```

Set the SNMPv3 Authentication and Privacy passwords.

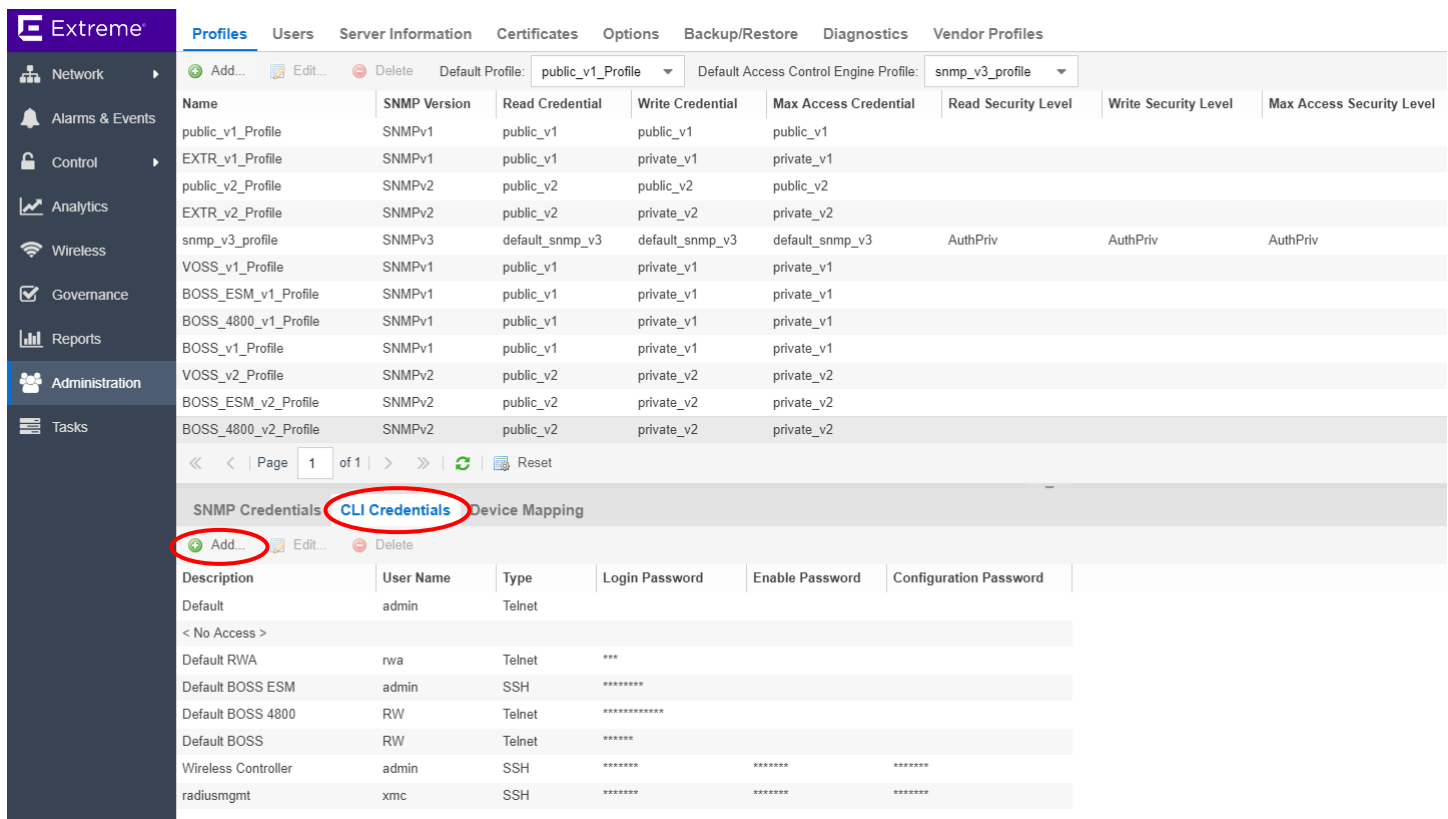
Extreme Management Center Profile Configuration - Wireless Controllers

Profiles are used to define access to the wireless controllers in the network by creating identities used for authentication when performing SNMP queries and sets and identities for CLI operations.

A profile can be configured with the SNMP version to be used for the read and write user and security level. It also points to a set of CLI credentials for the wireless controllers.

In the Automated Campus EVD, a profile that uses SNMPv3 was created and is used by Extreme Management Center for the wireless controllers. For CLI, SSH access is enabled. Authentication for CLI is done via RADIUS server.

- To create new CLI credentials, go to **Administration** → **Profiles** → **CLI Credentials** and click **Add**.



The screenshot shows the Extreme Management Center interface. The left sidebar contains navigation options: Network, Alarms & Events, Control, Analytics, Wireless, Governance, Reports, Administration (selected), and Tasks. The main content area is titled 'Profiles' and includes tabs for Users, Server Information, Certificates, Options, Backup/Restore, Diagnostics, and Vendor Profiles. Below these tabs is a table of profiles with columns: Name, SNMP Version, Read Credential, Write Credential, Max Access Credential, Read Security Level, Write Security Level, and Max Access Security Level. The 'snmp_v3_profile' is highlighted. Below the table are navigation controls (Page 1 of 1) and a 'Reset' button. The 'CLI Credentials' tab is selected and circled in red. Below this tab is an 'Add...' button, also circled in red, and a table of credentials with columns: Description, User Name, Type, Login Password, Enable Password, and Configuration Password. The table lists various default profiles and wireless controller credentials.

Name	SNMP Version	Read Credential	Write Credential	Max Access Credential	Read Security Level	Write Security Level	Max Access Security Level
public_v1_Profile	SNMPv1	public_v1	public_v1	public_v1			
EXTR_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
public_v2_Profile	SNMPv2	public_v2	public_v2	public_v2			
EXTR_v2_Profile	SNMPv2	public_v2	private_v2	private_v2			
snmp_v3_profile	SNMPv3	default_snmp_v3	default_snmp_v3	default_snmp_v3	AuthPriv	AuthPriv	AuthPriv
VOSS_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
BOSS_ESM_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
BOSS_4800_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
BOSS_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
VOSS_v2_Profile	SNMPv2	public_v2	private_v2	private_v2			
BOSS_ESM_v2_Profile	SNMPv2	public_v2	private_v2	private_v2			
BOSS_4800_v2_Profile	SNMPv2	public_v2	private_v2	private_v2			

Description	User Name	Type	Login Password	Enable Password	Configuration Password
Default	admin	Telnet			
< No Access >					
Default RWA	rwa	Telnet	***		
Default BOSS ESM	admin	SSH	*****		
Default BOSS 4800	RW	Telnet	*****		
Default BOSS	RW	Telnet	*****		
Wireless Controller	admin	SSH	*****	*****	*****
radiusmgmt	xmc	SSH	*****	*****	*****

- Only SSH is permitted for management connections to the network devices. Telnet access is disabled.

Add CLI Credential

Description: wireless controller

User Name: netadmin

Type: SSH

Login Password: extreme

Enable Password: extreme

Configuration Password: extreme

1. Configure a Description
2. Configure a User Name
3. Configure SSH as the Type.
4. Configure a Login Password.
5. Configure an Enable Password.
6. Configure a Configuration Password.
7. Click Save

Save Cancel

- To create a new Wireless Profile for the wireless controllers, go to **Administration** → **Profiles** and click **Add**.

Name	SNMP Version	Read Credential	Write Credential	Max Access Credential	Read Security Level	Write Security Level	Max Access Security Level
public_v1_Profile	SNMPv1	public_v1	public_v1	public_v1			
EXTR_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
public_v2_Profile	SNMPv2	public_v2	public_v2	public_v2			
EXTR_v2_Profile	SNMPv2	public_v2	private_v2	private_v2			
snmp_v3_profile	SNMPv3	default_snmp_v3	default_snmp_v3	default_snmp_v3	AuthPriv	AuthPriv	AuthPriv
VOSS_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
BOSS_ESM_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
BOSS_4800_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
BOSS_v1_Profile	SNMPv1	public_v1	private_v1	private_v1			
VOSS_v2_Profile	SNMPv2	public_v2	private_v2	private_v2			
BOSS_ESM_v2_Profile	SNMPv2	public_v2	private_v2	private_v2			
BOSS_4800_v2_Profile	SNMPv2	public_v2	private_v2	private_v2			

Add Profile

Profile Name: v3_wireless

SNMP Version: SNMPv3

Read: default_snmp_v3

Write: **New...**

Max Access: default_snmp_v3

CLI Credential: snmpv3_aes, snmpv3_ewc, snmpv3_nac

Read Security: NoAuthNoPriv

Write Security: NoAuthNoPriv

Max Security: NoAuthNoPriv

Buttons: Save, Cancel

1. Configure a Profile Name
2. Select SNMP Version – SNMPv3
3. Select New...
4. Add SNMP Credential Window Appears.

Add SNMP Credential

Credential Name: snmpv3_ewc

SNMP Version: SNMPv3

User Name: ewc_v3

Authentication Type: SHA

Authentication Password: extreme11

Privacy Type: AES

Privacy Password: extreme12extreme

Buttons: Save, Cancel

1. Configure a Credential Name.
2. Select from SNMP Version: SNMPv3.
3. Configure a User Name.
4. Select from Authentication Type: SHA.
5. Configure an Authentication Password.
6. Select form Privacy Type: AES.
7. Configure a Privacy Password.
8. Click Save.

- The same SNMPv3 user with the same authentication protocol and password and the same privacy protocol and password must be created on the ExtremeWireless Controllers.

- Configure the created profile with the new SNMP and CLI credential:

Edit Profile: v3_wireless

Profile Name: v3_wireless

SNMP Version: SNMPv3

Read: snmpv3_ewc Read Security: AuthPriv

Write: snmpv3_ewc Write Security: AuthPriv

Max Access: snmpv3_ewc Max Security: AuthPriv

CLI Credential: wireless controller

Buttons: Save, Cancel

Callout 1: Use the newly created **snmpv3_ewc** for Read/Write/Max Access.

Callout 2: Use AuthPriv for Read Security/Write Security/Max Security.

Callout 3: Use the newly created **wireless controller** CLI credentials.

ExtremeWireless Controller SNMPv3 Configuration

Extreme Management Center uses non-default SNMPv3 credentials to manage wireless controllers. The same SNMPv3 user, password, authentication, and privacy protocols must be configured on both Extreme Management Center and on the wireless controllers.

To configure SNMPv3 on the wireless controllers go to **Controller → Network → SNMP → SNMPv3 → Add User Account**.

EWC1 and EWC2

The screenshot shows the EMC web interface with the following configuration details:

- Navigation:** Home, Logs, Reports, Controller (selected), AP, VNS, WIPS, Help, Logout
- Left Menu:** Administration, Logs, Network (selected), L2 Ports, Network Time, Routing Protocols, Secure Connections, SNMP, Topologies, Utilities, Services
- SNMP Common Settings:**
 - Mode: No SNMP SNMPv1/v2c SNMPv3
 - Contact Name: EWC1a
 - Location: [Empty]
 - SNMP Port: 162
 - Forward Traps: Critical
 - Publish AP as interface of controller: Enabled
- SNMPv3 Configuration:**
 - Context String: [Empty] Engine ID: controller_000C295613D0 RFC3411 Compliant:
 - Table:

User Name	Security Level	Authentication Protocol	Privacy Protocol	Account Enabled
ewc_v3	authPriv	SHA	AES	✓
 - Buttons: Delete Selected User, **Add User Account** (circled), Edit Selected User
 - Trap Configuration:
 - Trap 1: Destination IP: 172.9.99.119, User Name: ewc_v3
 - Trap 2: Destination IP: [Empty], User Name: [Empty]
 - Save button
- Footer:** [EWC1a | V2110 Small | 32 days, 07:34] User: netadmin [M] [1] [2] [I] Software: 10.41.07.0014 | Admin Users: 2 © 2006-2018 Extreme Networks. All Rights Reserved.

The Add SNMPv3 User Account window appears.

Add SNMPv3 User Account

Enabled:

User Name: ewc_v3

Security Level: authPriv

Authentication Protocol: SHA

Authentication Password: extreme11 Mask

Privacy Protocol: AES

Privacy Password: extreme12ex Mask

OK Cancel

Credentials must match those created in the Basic Extreme Management Center section of this document.
Authentication Password: **extreme11**
Privacy Password: **extreme12extreme**

SNMP Common Settings

Mode: No SNMP SNMPv1/v2c SNMPv3

Contact Name: EWC1a

Location:

SNMP Port: 162

Forward Traps: Critical

Publish AP as interface of controller: Enabled

SNMPv1/v2c | **SNMPv3**

Context String: Engine ID: controller_000C295613D0 RFC3411 Compliant:

User Name	Security Level	Authentication Protocol	Privacy Protocol	Account Enabled
ewc_v3	authPriv	SHA	AES	<input checked="" type="checkbox"/>

Delete Selected User Add User Account Edit Selected User

Trap 1: Destination IP: 172.9.99.119 User Name: ewc_v3

Trap 2: Destination IP: User Name:

Save

SNMPv3 User Account Created and enabled.

Domain Name System (DNS)

To obtain captive portal redundancy, DNS is used to provide one URL address for both ExtremeControl engines. If one engine is unreachable the second engine will take over because both are associated with the same FQDN.

Essentially, both ExtremeControl engine IPs are added to the same FQDN within the domain of the DNS server. Additional configuration is required on the external DHCP server which is detailed in the Captive Services Configuration subsection of the **Extreme Policy** section.

As an added layer of security, select the **Use Fully Qualified Domain Name** checkbox to hide the IP addresses of the ExtremeControl servers when an unregistered user is redirected. This is located in Extreme Management Center: **Access Control** → **Configuration** → **Captive Portals** → **Network Settings**.

The screenshot displays the Extreme Management Center interface. The left sidebar shows the navigation menu with 'Control' selected. The main content area is titled 'Network Settings' and contains several configuration options:

- Allowed Web Sites: Open Editor...
- Use Fully Qualified Domain Name: (highlighted with a red circle)
- Use Mobile Captive Portal:
- Display Welcome Page:
- Portal HTTP Port: 80
- Portal HTTPS Port: 443
- Force Captive Portal HTTPS:
- Redirection: Redirect User Immediately*:
 - Test Image URL: https://www.google.com/favicon.ico
 - Redirection: To URL
 - Destination: http://www.extremenetworks.com

At the bottom of the page, there is a note: ** When used as the portal in an Advanced Location configuration, all fields except Redirect User Immediately are inherited from the Access Control Configuration's base portal.* The interface also includes 'Enforce' and 'Refresh' buttons at the bottom left, and 'Save' and 'Cancel' buttons at the bottom right.

RADIUS (Login Management Configuration)

Access can be configured via several means. For full network administration security, we recommend RADIUS or LDAP authentication for Extreme Management Center, ExtremeWireless Controllers, and Extreme device login. The use of an external server is recommended to authenticate user access to Extreme’s appliances and switches for administrative purposes. Configuration of the authentication server will need to be completed prior to configuring XMC settings. For the purposes of this EVD, LDAP is being configured using Windows 2008 server as the authentication server.

To configure login authentication for Extreme Management Center, go to **Administration** → **Users**, set the Authentication Method to **LDAP**, and select **New** in the LDAP drop down field.

The screenshot shows the 'Users' configuration page in the Extreme Management Center. The 'Authentication Method' is set to 'LDAP'. The 'LDAP' dropdown menu is open, showing options: 'None', 'New...', 'Manage...', and 'None'. The 'New...' option is circled in red. Below the dropdown, the 'Authorized Users' table is visible, showing a user named 'root' with the 'NetSight Administrator' group and 'Automatic Member' set to 'false'.

User Name	Domain/Host Name	Authorization Group	Automatic Member ↑
root		NetSight Administrator	false

1. Enter **Configuration Name**.
2. Enter **LDAP Connection URLs** using the Authentication server URLs.
3. **Authentication Settings**: consists of the Administrator Username and Administrator password to access the Authentication server. Note that the Timeout settings default is 4 seconds, which may be increased depending on processing time and response of LDAP authentication requests.
4. **Search Settings**: Settings based on Authentication server settings.
5. **Schema Definition**: settings may readily appear by clicking "Populate Default Values" button (just above the Save button) and selecting the appropriate template, in our example "Active Directory User Defaults" is the correct template. Otherwise, the appropriate settings will need to be determined that is applicable to your authentication server.
6. Click **Save** to save your settings. Before or after saving, you can test your LDAP configuration by clicking the "Test" button.

- Active Directory: User Defaults
- Active Directory: Machine Defaults
- OpenLDAP Defaults
- Novell eDirectory Defaults

The LDAP configuration menu can also be accessed via **Control>Access Control>Configuration>AAA>LDAP Configurations**.

- The option to set the **Authenticate to OS on Failure to Authorization Group** checkbox allows the XMC server to still be accessible to a configured Authorization Group if authentication fails.

The screenshot shows the 'Users' configuration page in the Extreme Networks interface. Under the 'Authentication Method' section, the 'Authenticate to OS on Failure to Authorization Group' checkbox is checked and highlighted with a red circle. The 'LDAP' dropdown is set to 'Directory (sqa.net)' and the 'NetSight Administrator' dropdown is also visible.

- When a new user is added, an associated Authorization Group – with the appropriate capabilities – must be created in the Authorization Groups window.

The screenshot shows the 'Users' configuration page with the 'Add Authorization Group' dialog box open. The 'Add...' button in the 'Authorized Users' table is highlighted with a red circle. The dialog box shows the 'Add Authorization Group' form with fields for Name, Membership Criteria, and SNMP Redirect. The 'Capability' section is expanded, showing several capabilities with their IDs.

Capability	ID
NetSight Application Analytics (2 enabled)	
Application Analytics Read Access	APPID_READ
Application Analytics Read/Write Ac...	APPID_WRITE
NetSight Console (18 enabled)	
NetSight Inventory Manager (36 enabled)	
NetSight Medication Agent (enabled)	

To configure SSH access to Extreme Management Center, click **Manage SSH Configuration** under SSH Configuration. A popup will appear with appropriate fields to configure the port, primary and secondary RADIUS servers, and the SSH user that should have access.

The screenshot displays the Extreme Management Center interface. The left sidebar shows the navigation menu with 'Administration' selected. The main content area is titled 'Users' and shows the 'SSH Configuration' section. The 'Manage SSH Configuration' link is circled in red. A modal dialog titled 'SSH Configuration' is open, showing the following configuration options:

- Manage SSH Configuration
- Port: 22
- Disable Remote root Access:
- RADIUS Authentication
- Primary RADIUS Server: 172.9.99.105
- Secondary RADIUS Server: 172.9.99.115
- SSH Users table:

Username	Type	Administrative User
testssh1	Local	yes
testssh2	RADIUS	yes
netadmin	RADIUS	yes

Below the modal, the 'Authorized Users' table is visible:

User Name	Domain/Host Name	Authorization Group
root		NetSight Administrator
netadmin	sqa.net	netadmingroup
stevetech	sqa.net	techgroup1
shanetech	sqa.net	techgroup1
jimtech	sqa.net	techgroup1
alextech	sqa.net	techgroup1
livitech	sqa.net	techgroup1
shaneadmin	sqa.net	netadmingroup
steveadmin	sqa.net	netadmingroup
alexadmin	sqa.net	netadmingroup
jimadmin	sqa.net	netadmingroup
liviuadmin	sqa.net	netadmingroup

At the bottom, the 'Authorization Groups' table is also visible:

Name	Criteria	Users	Capabilities	Zones
NetSight Administrator		1	Full	
netadmingroup		6	Full	
techgroup1		5	Customized	

ExtremeWireless Controllers

Users connecting to the wireless controllers for management operations can be authenticated locally or by using a RADIUS server; the example below shows RADIUS requests forwarded to NAC servers which then uses LDAP to authenticate with the Active Directory server.

- To enable the use of a server, go to **Controller** → **Administration** → **Login Management**. Click the **Configure** button and enable RADIUS.

The screenshot shows the 'Administration' menu on the left with 'Login Management' selected. The main content area has two tabs: 'Local Authentication' and 'RADIUS Authentication'. Under 'Local Authentication', there are three user roles: 'Full Administrator' (with an 'admin' user listed), 'Read-only Administrator', and 'GuestPortal Manager'. The 'RADIUS Authentication' tab is active, showing 'Add User' and 'Modify User' sections. The 'Add User' section has fields for Group (set to 'Full Administrator'), User ID, Password, and Confirm Password, with an 'Add User' button. The 'Modify User' section has fields for User ID (set to 'undefined'), Password, and Confirm Password, with buttons for 'Change Password', 'Remove user', and 'Reset'. At the bottom, the 'Authentication mode' is 'Local, RADIUS', and the 'Configure' button is circled in red. A 'Save' button is also visible.

- In the **Login Authentication** dialog, verify that RADIUS is enabled.

The screenshot shows the 'Login Authentication Mode Configuration' dialog box. It contains a table with two columns: 'Enable' and 'Authentication'. The 'Local' row has a checked checkbox, and the 'RADIUS' row has a checked checkbox and is circled in red. To the right of the table are 'Move Up' and 'Move Down' buttons. At the bottom, the 'OK' button is circled in red, along with a 'Cancel' button.

Enable	Authentication
<input checked="" type="checkbox"/>	Local
<input checked="" type="checkbox"/>	RADIUS

- Go to the RADIUS Authentication tab to select the ExtremeControl engines as RADIUS servers. The NAS IP address is the IP address the wireless controller will use as a source when sending RADIUS requests. This address must be in the Switch list on ExtremeControl. Select the appropriate Authentication type configured for your topology; MS-Chap2 is used in this example. After configuring all fields, use the **Test** button to verify authentication.

Local Authentication | **RADIUS Authentication**

Use

Configured Servers

Nac1 | Up

Nac2 | Down

Test

View Summary

Auth * Use server for Authentication

NAS IP Address: 172.9.98.106

NAS identifier: EWC1a

Auth. type: MS-CHAP2

Reset

In this topology, RADIUS Authentication is configured to send RADIUS requests to the NAC servers. NAC is configured to use LDAP to authenticate using the Active Directory server.

NAS IP Address: 172.9.98.106
NAS identifier: EWC1a
Auth Type: MS-CHAP2

- In ExtremeControl, ensure that the “**mgmt=su:**” attribute is added to the **Netadmin** Policy Mapping (noted in **Profiles and Policy Mappings**).
- To test RADIUS connectivity:

Test RADIUS Servers

User ID: netadmin

Password: ●●●●●●

Test | Cancel

Enter Credentials:
User ID: netadmin
Password: extreme
Click Test

Test RADIUS Servers

RADIUS Test Results:
Successful

Close

Test of both RADIUS servers should return Successful.

Summit Access Switch

To configure login authentication on ExtremeSwitching, <mgmt-access> must be configured on the switch. With RADIUS <mgmt-access> enabled within the <aaa> module, any Administrator user that tries to connect to the network device via SSH or console will be authenticated first against the ExtremeControl configuration.

- The command <enable radius mgmt-access> is required for this to work.

Note

The resulting configuration below is added automatically to the access switch upon adding it to ExtremeControl. This process is documented in the [Wired User Access](#) section.

```
configure radius 1 server 172.9.99.120 1812 client-ip 172.9.90.11 vr VR-Default
configure radius 1 shared-secret encrypted "#$9ARiatRiZpmB24IGZifDv71WKUt/ig=="
configure radius 2 server 172.9.99.121 1812 client-ip 172.9.90.11 vr VR-Default
configure radius 2 shared-secret encrypted "#$LK58QAJ6bS/Yc3y36e+RrlRMjm+oGw=="
configure radius-accounting 1 server 172.9.99.120 1813 client-ip 172.9.90.11 vr VR-Default
configure radius-accounting 1 shared-secret encrypted "#$Lhw9XdTUKC1OhiRXjLFR3+YePeWjkQ=="
configure radius-accounting 1 timeout 10
configure radius-accounting 2 server 172.9.99.121 1813 client-ip 172.9.90.11 vr VR-Default
configure radius-accounting 2 shared-secret encrypted "#$/c/qfigRCQK5EeTeEvv3Pr+bqqh3Dg=="
configure radius-accounting 2 timeout 10
enable radius
enable radius mgmt-access
enable radius netlogin
configure radius timeout 10
enable radius-accounting
enable radius-accounting mgmt-access
enable radius-accounting netlogin
```

ERS Access Switch

To configure login authentication for ERS switches, three steps are involved:

- Configurations will need to be added to the appliance
- In XMC, the ERS switches need to be added and configured to the ExtremeControl engines.
- The User profile needs to be edited.

(Note: You may need to enforce the settings to ExtremeControl when complete.)

1. In the ERS switch:

- Configure the ExtremeControl appliances as the primary and secondary radius servers, along with a secret key, for authenticated login:

```
radius server host 172.9.99.120 key acct-enable
<shared secret>
<shared secret>
radius server host 172.9.99.121 secondary
cli password telnet radius
cli password serial radius
```

- Radius Password Fallback allows users to log in to ERS by using the locally configured password, if the RADIUS server is unavailable/unreachable for authentication. **It is highly recommended to verify the default login password has been changed when using RADIUS Fallback.** To ensure “fallback” is enabled, verify from the configuration:

```


4900_STACK#show radius-server
RADIUS Global Server
-----
Primary Host       : 172.9.99.120
Secondary Host    : 172.9.99.121
Port               : 1812
Time-out          : 10
Key               : *****
Radius Accounting  : Enabled
Radius Accounting Port : 1813
Radius Retry Limit : 3
Current Status    : Reachable via Primary
Time Until Next Check : 142

RADIUS EAP Server
-----
Primary Host       : 172.9.99.120
Secondary Host    : 172.9.99.121
Port               : 1812
Time-out          : 10
Key               : *****
Radius Accounting  : Enabled
Radius Accounting Port : 1813
Radius Retry Limit : 3
Current Status    : Reachable via Primary
Time Until Next Check : 142

RADIUS Non-EAP Server
-----
Primary Host       : 172.9.99.120
Secondary Host    : 172.9.99.121
Port               : 1812
Time-out          : 10
Key               : *****
Radius Accounting  : Enabled
Radius Accounting Port : 1813
Radius Retry Limit : 3
Current Status    : Reachable via Primary
Time Until Next Check : 142

Other Settings
-----
Password Fallback  : Enabled
RADIUS Encapsulation : MS-CHAP-V2

```



2. In XMC, add the ERS switch to the ExtremeControl engine and configure parameters. This procedure is explained in the following section:
3. Edit the ERS Radius attributes file and add/ensure the following attribute is defined:
 - Items 2 and 3 are detailed in the following section:

[Access Switch Provisioning/Fabric Attach](#)

Fabric Connect Switch

To configure login authentication for VSP switches, three steps are involved:

- Configurations will need to be added to the switch.
- In XMC, the VSP switches need to be added and configured to the ExtremeControl engines.
- The User profile needs to be edited.

(Note: You may need to enforce the settings to ExtremeControl when complete.)

1. In the VSP switch:

- Configure the ExtremeControl appliances as the primary and secondary radius servers, along with a secret key, for authenticated login:

```
radius server host 172.9.99.120 key ***** source-ip 10.0.0.210
radius server host 172.9.99.121 key ***** source-ip 10.0.0.210
radius enable
radius sourceip-flag
```

2. In XMC, add the VSP switches to the ExtremeControl engine and configure:

- Go to **Control**→**Access Control**→**Engines**→**Engine Groups**→**Default**→**Switches**→**Add**.
- Select the switches under **Add Device** to be configured.
- Select the **Switch Type** that supports your topology.
- Add the ExtremeControl **Primary Engine** (as well as a **Secondary Engine** if your topology includes it).
- Set the **Auth. Access Type** to **Management Access**.
- A custom RADIUS attribute profile can be created in the **RADIUS Attributes to Send** field by selecting **NEW** in the drop-down-field (Note: future XMC versions will include default VSP RADIUS attribute profiles).

The screenshot displays the Extreme Networks configuration interface for the 'Access Control' section. The main window shows the 'Engine Group - Default' configuration page with tabs for 'Details', 'Switches', 'End-Systems', and 'Access Control Engines'. The 'Switches' tab is active, and the 'Add...' button is circled in red. A dialog box titled 'Add Switches to Access Control Engine Group: Default' is open, showing a list of devices and configuration options. The 'Add Device' button in the dialog is also circled in red. The configuration options include:

- Switch Type: Layer 2 Out-Of-Band
- Primary Engine: NAC1/172.9.99.120
- Secondary Engine: NAC2/172.9.99.121
- Auth. Access Type: Management Access
- RADIUS Accounting: New...
- Management RADIUS Server 1: None
- Management RADIUS Server 2: None
- Network RADIUS Server: Cisco Per-User ACL, Cisco Wired Dynamic ACL, Cisco Wired RFC 3580 and Dynamic ACL, Cisco Wireless Dynamic ACL

The device list includes:

- All Devices (21 devices)
- Acc-120, Acc-121, Acc-220, Acc-221, Analytics
- BEB-7254-940, BEB-7254-950, BEB-7254-960, BEB-7254-970, BEB-8284-110, BEB-8284-111, BEB-8284-210, BEB-8284-211, BEB-8404-10, BEB-8404-20 (selected), CORE-8404-30, EWC1a, EWC1b

The 'Save' button is located at the bottom right of the dialog box.

- In the new **Add RADIUS Attribute Configuration** window, name your profile; in this instance we used **VSP Policy**.
- Add the RADIUS attributes profile configuration. For the profile configuration, use the following values, then click **SAVE**:

Filter-Id=Enterasys:version=1:%MANAGEMENT%policy=%POLICY_NAME%
 Service-Type=%MGMT_SERV_TYPE%
 Passport-Access-Priority=%CUSTOM1%

The screenshot shows the 'Add RADIUS Attribute Configuration' dialog box. The 'Name' field is set to 'VSP Policy'. The 'Attributes' field contains the following configuration: 'Filter-Id=Enterasys:version=1:%MANAGEMENT%policy=%POLICY_NAME%', 'Service-Type=%MGMT_SERV_TYPE%', and 'Passport-Access-Priority=%CUSTOM1%'. The 'Save' button is highlighted with a red circle. Two callout boxes with arrows point to the 'Name' field and the 'Attributes' field, with text: 'Name the custom profile.' and 'Enter the attributes configuration.' respectively.

- You can set **RADIUS Accounting** to **Enabled** according to the needs of your topology.
- Subsequent fields can be configured to match your topology. In our topology:
 - **Management RADIUS Server 1** set to **None** since RADIUS requests are passed through the NAC engines already configured.
 - **Policy Enforcement Point 1** and **2** set to **None**.
 - **Policy Domain** set to **Do Not Set** since we are only configuring **Management Access**.
- Then click **Save**.

- Final configuration view for step 2 shown below:

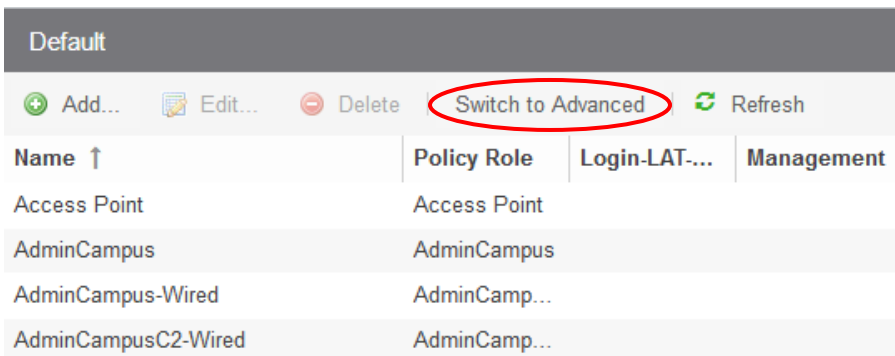
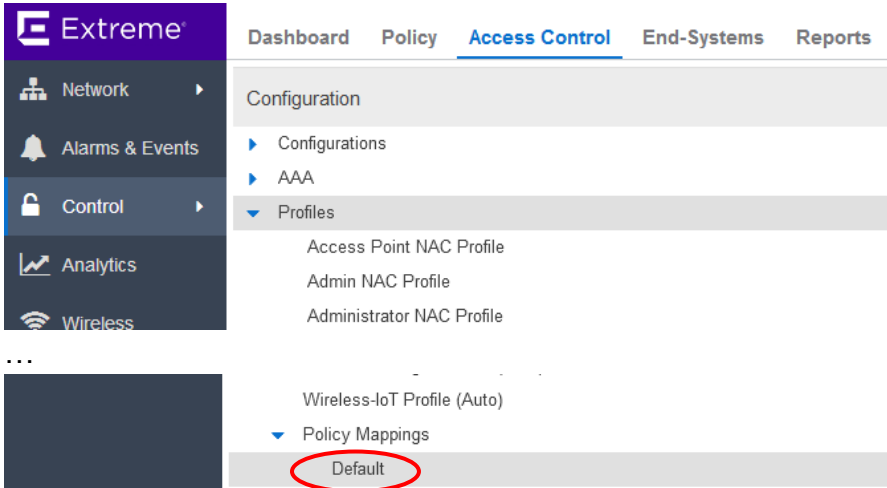
Switch Type:	Layer 2 Out-Of-Band	Select the Switch Type.
Primary Engine:	NAC1/172.9.99.120	Add the Control Engines.
Secondary Engine:	NAC2/172.9.99.121	
Auth. Access Type:	Management Access	Set the Auth Access Type to Management Access
Virtual Router Name:		
RADIUS Attributes to Send:	VSP Policy	Set RADIUS Attributes to VSP Policy and enable Accounting.
RADIUS Accounting:	Enabled	
Management RADIUS Server 1:	None	
Management RADIUS Server 2:	None	
Network RADIUS Server:	None	
Policy Enforcement Point 1:	None	
Policy Enforcement Point 2:	None	
Policy Domain:	-- Do Not Set --	

Advanced Settings...

Save Close

- In XMC, the User profile needs to be edited with one or more custom entries that maps to the RADIUS attribute values.

- Go to **Control**→**Access Control**→ **Configuration**→ **Profiles**→ **Policy Mappings**→ **Default** and change the view from Basic to Advanced by clicking on the **Switch to Advanced** button.



- Select the User profile/Policy mapping to be edited and click **Edit**. In this EVD, the **Netadmin (Administrator)** policy mapping is used for RADIUS authentication for all network devices.

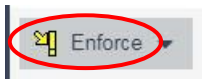
- Add/verify the following values in the listed fields and **Save**:
 - **Custom 1** is set to **6** (which is an Administrator privilege).

The screenshot shows the 'Edit Policy Mapping' dialog box with the following fields and values:

- Name: Netadmin (Administrator)
- Map to Location: Any
- Policy Role: Administrator
- VLAN [ID] Name: None
- VLAN Egress: Untagged (dropdown) U (text)
- Filter: Netadmin
- Port Profile: (empty)
- Virtual Router: (empty)
- Login-LAT-Group: Netadmin
- Login-LAT-Port: 1
- Custom 1: 6
- Custom 2: (empty)

Custom 1 value set to 6.

- Enforce the settings to the ExtremeControl Engine, at bottom of page:



Secure Shell (SSH)

SSH is disabled by default. We recommend the disabling of Telnet access to network devices and enable SSH for security and authentication purposes.

Secure Shell 2 (SSH2) is a feature of the Summit and Fabric Connect software that enables you to encrypt session data between a network administrator using SSH2 client software and the switch, or to send encrypted data from the switch to an SSH2 client on a remote system.

Summit Access Switch

Enter the command `<enable ssh2>`. The following output will be generated:

```
Slot-1 Stack.1 #disable telnet
Slot-1 Stack.1 #enable ssh2
WARNING: Generating new server host key
This could take up to 1 minute and cannot be cancelled. Continue? (y/N) Yes
.....
Key Generated.
```

ERS Access Switch

Enter the following commands to disable Telnet and enable SSH configuration for this Validated Design.

```
telnet-access disable
ssh
```

Fabric Connect Switch

Enter the following commands to disable Telnet and enable SSH configuration for this Validated Design.

```
no boot config flags telnetd
boot config flags sshd
ssh
save config
```

Multicast (IGMP)

Multicast has many applications. However, for most campuses the primary use case is for video delivery and security camera applications. In this design, IGMP and IGMP snooping will be configured for Layer 2 multicast.

Internet Group Management Protocol

IGMP and IGMP snooping should be enabled by default. If they are not enabled, you can enable them by issuing the following commands:

Summit Access Switches

```
enable igmp
enable igmp snooping
```

- Display the status of the IGMP table:

```
Slot-1 Stack.2 # show igmp snooping cache
Snooping/MVR Cache Timeout: 300 sec
```

Type	Group	Sender	Age	InVlan
snoop	225.4.1.1	172.90.1.10	63	VLAN_202
	Vlan	Port	Vid	
	VLAN_202	2:3	202	
		1:50	202	
snoop	225.4.1.1	172.90.1.15	48	VLAN_202
	Vlan	Port	Vid	
	VLAN_202	2:3	202	
		1:50	202	
snoop	225.4.1.1	172.90.1.20	57	VLAN_202
	Vlan	Port	Vid	
	VLAN_202	2:3	202	
		1:50	202	

Source IP of stream.

Ports that the stream is seen on.

SPB-Multicast Forwarding

In order to route multicast traffic through the Automated Campus, IP Multicast Forwarding must be enabled on all forwarding VLANs in the campus.

Note

- As BCB-930 is a core switching node, no multicast configuration is required.
- As BEB-960/970 and BEB-940/950 are Leaf nodes and subordinate to the Controllers, no multicast configuration is required.

The multicast configuration should resemble the following:

Campus 1 – BEB-110 and BEB-111

```

router isis
spbm 1 multicast enable
exit

interface Vlan 101
ip spb-multicast enable
exit

interface Vlan 102
ip spb-multicast enable
exit

interface Vlan 103
ip spb-multicast enable
exit

interface Vlan 104
ip spb-multicast enable
exit

interface Vlan 1050
ip spb-multicast enable
exit

interface Vlan 1051
ip spb-multicast enable
exit

interface Vlan 1052
ip spb-multicast enable
exit

router vrf iot
mvpn enable
exit

router vrf surveillance
mvpn enable
exit

```

Enable multicast on the global IS-IS instance.

Enable multicast on the required VLAN interfaces.

Enable multicast on the required VRFs.

Campus 2 – BEB-210 and BEB-211

The same settings are applied to the required VLANs/VRFs in Campus 2:

```

router isis
spbm 1 multicast enable
exit

interface Vlan 201
ip spb-multicast enable
exit

interface Vlan 202
ip spb-multicast enable
exit

interface Vlan 203
ip spb-multicast enable
exit

interface Vlan 204
ip spb-multicast enable

```

```
exit

interface Vlan 1050
ip spb-multicast enable
exit

interface Vlan 1051
ip spb-multicast enable
exit

interface Vlan 1052
ip spb-multicast enable
exit

router vrf iot
mvpn enable
exit

router vrf surveillance
mvpn enable
exit
```

Campus 3 – BEB-310 and BEB-311

The same settings are applied to the required VLANs/VRFs in Campus 3:

```
router isis
spbm 1 multicast enable
exit

interface Vlan 301
ip spb-multicast enable
exit

interface Vlan 302
ip spb-multicast enable
exit

interface Vlan 303
ip spb-multicast enable
exit

interface Vlan 304
ip spb-multicast enable
exit

interface Vlan 1050
ip spb-multicast enable
exit

interface Vlan 1051
ip spb-multicast enable
exit

interface Vlan 1052
ip spb-multicast enable
exit

router vrf iot
mvpn enable
exit

router vrf surveillance
mvpn enable
exit
```

Server Room Controllers - BEB-910 and BEB-920

```

router isis
spbm 1 multicast enable
exit

interface Vlan 900
ip spb-multicast enable
exit

interface Vlan 902
ip spb-multicast enable
exit

interface Vlan 904
ip spb-multicast enable
exit

interface Vlan 911
ip spb-multicast enable
exit

router vrf iot
mvpn enable
exit

router vrf surveillance
mvpn enable
exit

```

Enable multicast on the global IS-IS instance.

Multicast servers reside on the Production VLAN.

Video Surveillance Receivers reside on the Surveillance VLAN, receiving camera streams from the campuses.

As surveillance cameras and receivers reside on their own L3VSN, it is kept separate from other services.

- Display the status of the global IP Multicast over Fabric Connect configuration:

```

BEB-8284-110:1(config)#show isis spbm multicast
                        multicast : enable
                        fwd-cache-timeout (seconds) : 210

```

Specifies if multicast is enabled.

Specifies the forward cache timeout value in seconds.

- Display IP Multicast over Fabric Connect summary information for each S, G, V tuple:

```

BEB-8284-110:1#show isis spb-mcast-summary
=====
SPB Multicast - Summary
=====
SCOPE      SOURCE      GROUP      DATA      LSP  HOST
I-SID     ADDRESS    ADDRESS    I-SID      BVID  FRAG  NAME
-----
1800904   172.10.32.58  226.1.1.49  16000099  4052  0x7   BEB-8284-111
1800904   172.10.32.59  226.1.1.50  16000100  4052  0x7   BEB-8284-111
GRT       172.90.1.30  225.2.2.1   16000001  4052  0x3   BEB-7254-970
GRT       172.90.1.31  225.2.2.2   16000002  4052  0x3   BEB-7254-970
    
```

Indicates the IP multicast source address that maps to the I-SID.

Indicates the IP multicast group address that maps to the I-SID.

Indicates the host name of the router the stream was sourced from.

Indicates the I-SID that specifies the multicast streams when the scope is either the Layer 3 VSN or the Layer 2 VSN or any combination.

Indicates the data I-SID for the IP multicast route, which includes the source IP address, group IP address, and the local VLAN that the stream is received on (S,G,V tuple). SPBM uses the data I-SID to create the multicast tree.

- Display information about the multicast routes on the switch:

```

BEB-8284-110:1(config)#show ip mroute route vrf surveillance
=====
Mroute Route - VRF surveillance
=====
GROUP      SOURCE      SRCMASK      UPSTREAM_NBR  IF      EXPIR      PROT
-----
226.1.1.1  172.10.32.50  255.255.255.255  0.0.0.0      Vlan104  163      spb
226.1.1.1  172.10.32.60  255.255.255.255  0.0.0.0      Vlan104  1755     spb
226.1.1.2  172.10.32.51  255.255.255.255  0.0.0.0      Vlan104  196      spb
226.1.1.2  172.10.32.61  255.255.255.255  0.0.0.0      Vlan104  1637     spb
226.1.1.3  172.10.32.52  255.255.255.255  0.0.0.0      Vlan104  111      spb
    
```

The ifindex for the interface that receives IP datagrams.

Indicates the minimum amount of time remaining before this entry ages out. The value 0 indicates that the entry is not subject to aging.

Indicates the multicast protocol through which the switch learned this route.

Indicates the IP multicast group for this multicast route.

Indicates the sources for this multicast route.

The upstream neighbor from which IP datagrams are received. The field displays the value of 0.0.0.0 if the (S,G) source is local or if the RP is this router.

Wireless Multicast Forwarding

A mechanism that supports multicast traffic can be enabled as part of a topology definition. This mechanism is provided to support the demands of VoIP and IPTV network traffic, while still providing the network access control. Define a list of multicast groups whose traffic is allowed to be forwarded to and from the VNS using this topology. The default behavior is to drop the packets. For each group defined, you can enable Multicast Replication by group.

1. On the **VNS→Topologies** page, select the desired topology and click the **Multicast Filters** tab. Check the box for **Multicast bridging**:
2. Either manually enter a custom multicast group, or choose from one of the **Defined groups** in the drop-down, and click **Add**:

Topology: 1050-Administrator

The screenshot shows the configuration interface for Multicast Filters. The 'General' tab is active, and the 'Multicast Filters' section is expanded. The 'Multicast bridging' checkbox is checked and circled in red. Below it, a table is visible with columns 'IP', 'Group', and 'Wireless Replication'. The 'Defined groups' dropdown menu is open, showing a list of multicast groups, with 'All Multicast (0.0.0.0/0)' selected. The 'Add' button is also circled in red.

IP	Group	Wireless Replication
		<input type="checkbox"/>

Defined groups:

- All Multicast (0.0.0.0/0)
- All Multicast (0.0.0.0/0)
- Spectralink Mcst (224.0.1.116)
- Vocera Mcst (230.230.0.0/20)
- mDNS/Bonjour (224.0.0.251)
- WS-Discovery (239.255.255.250)
- All V6 Multicast (FF00::/8)
- mDNSV6/Bonjour (FF02::FB)

- Determine whether wireless replication is required, then click Save. Repeat this on all topologies requiring multicast support.

Topology: 1050-Administrator

General Multicast Filters

Multicast bridging (only the multicasts matching the rules defined will be allowed)

IP	Group	Wireless Replication !
0.0.0.0/0	All Multicast	<input checked="" type="checkbox"/>

IP Group:

Defined groups: All Multicast (0.0.0.0/0) ▼

Up Down

Add Delete

New New Group Delete Save

"Wireless replication" controls whether multicasts from wireless clients will be forwarded back to other wireless clients. Disabling wireless replication can save wireless bandwidth but some protocols (such as SpectraTalk's "Push to Talk" feature) won't work when wireless replication is disabled. When multicast bridging/forwarding is enabled while wireless replication is disabled multicasts to the address will only be forwarded from the wired network to wireless stations and from wireless stations to the wired network, not directly between wireless stations.

Loop Protection

A Loop Protection mechanism should be in place to prevent inadvertent Layer 2 loops from occurring at the access layer.

Summit Access Switch

STP Edge Port with Safeguard

Loop prevention and detection on an edge port configured for RSTP is called Edge Safeguard. You can configure edge safeguard on RSTP edge ports to prevent accidental or deliberate misconfigurations (loops) resulting from connecting two edge ports together or by connecting a hub or other non-STP switch to an edge port. Edge safeguard also limits the impact of broadcast storms that might occur on edge ports. This advanced loop prevention mechanism improves network resiliency but does not interfere with the rapid convergence of edge ports.

An edge port configured with edge safeguard immediately enters the forwarding state and transmits BPDUs. If a loop is detected, STP blocks the port. By default, an edge port without edge safeguard configured immediately enters the forwarding state but does not transmit BPDUs unless a BPDU is received by that edge port.

- To configure, enable Edge Safeguard on the switch's access ports:

```
config stpd s0 ports link-type edge <access ports> edge-safeguard enable bpdu-restrict
```

- Show the status of the feature:

```
Slot-1 Stack.17 # show stpd s0 ports detail 2:15
Stpd: s0      Port: 2:15      PortId: 808f      Stp: ENABLED      Path Cost: 20000
Port Mode     : 802.1D      Port Role        : Designated
Port State    : FORWARDING  Topology Change Ack: FALSE
Port Priority  : 128
Designated Root : 80:00:02:04:96:a1:bf:25      Designated Cost: 0, IntCost: 0
Designated Bridge : 80:00:02:04:96:a1:bf:25      Designated Port Id: 808f
Partner STP version : MSTP
Restricted Role   : Disabled
Active Role      : Disabled
Edge Port Safe Guard : Enabled
BPDU Restrict    : Enabled
maxAge: 20      msgAge: 0      fwdDelay: 15      helloTime: 2      maxHops: 20
Restricted TCN   : Off
Loop Protect     : Off
Loop Protect Partner : Incapable
Operational Edge : TRUE
Auto Edge       : On
Reflection BPDU  : On
Participating Vlans: Default
```

- When a loop is detected on enabled ports, the port that receives the BPDU is disabled:

```
Slot-1 Stack.22 # show stpd s0 ports 2:15,2:16
Port  Mode  State  Cost  Flags  Priority  Port ID  Designated Bridge
2:15  802.1D  FORWARDING  20000  eDee-m-GI-  128      808f      80:00:02:04:96:a1:bf:25
2:16  802.1D  DISABLED  20000  e?ee-m-GI-  128      8090      00:00:00:00:00:00:00:00
Total Ports: 2
```

```
Slot-1 Stack.23 # show stpd s0 ports 2:15,2:16 non-forwarding-reason
Port      State      Reason
-----
2:16     DISABLED   Placed in blocking state because a loopback condition
          has been detected.
```

ERS Access Switch

Simple Loop Prevention Protocol (SLPP and SLPP-Guard)

Simple Loop Prevention Protocol (SLPP) provides active protection against Layer 2 network loops on a per-VLAN basis. SLPP uses a lightweight hello packet mechanism to detect network loops. SLPP packets are sent using Layer 2 multicast and a switch will only look at its own SLPP packets or at its peer SLPP packets. It will ignore SLPP packets from other parts of the network. Sending hello packets on a per VLAN basis allows SLPP to detect VLAN based network loops for un-tagged as well as tagged IEEE 802.1Q VLAN link configurations. Once a loop is detected, the port is shut down.

```
interface Ethernet ALL
slpp-guard port 1/1-24,2/1-24,3/1-24 enable
exit
```

```
4900_4900_STACK(config)#show slpp-guard
SLPP-guard Ethertype: 0x8102
Unit/Port Link Oper SLPP-guard State Timeout TimerCount
-----
1/1       Down Down Enabled N/A      60      N/A
1/2       Down Down Enabled N/A      60      N/A
1/3       Up   Up   Enabled Monitoring 60      N/A
```

Fabric Connect Switch

Simple Loop Prevention Protocol (SLPP)

```
slpp enable
slpp vid 300
slpp vid 302
slpp vid 303
slpp vid 304

interface GigabitEthernet 2/1
slpp packet-rx
slpp packet-rx-threshold 5
exit

interface GigabitEthernet 2/2
slpp packet-rx
slpp packet-rx-threshold 5
exit
```

Its recommended to have one BEB in the SMLT pair set its SLPP interfaces to a higher threshold (5 vs 50). This will avoid both interfaces briefly going down when a loop is detected, resulting in less traffic loss.

```
BEB-8404-310:1(config)#show slpp
```

```
=====
                        SLPP Info
=====
```

```
operation : enabled
tx-interval : 500 milliseconds
vlan : 300,302,303,304
```

References

1. ExtremeSwitching Campus Switches

<https://www.extremenetworks.com/products/switching/campus-switching/>

https://documentation.extremenetworks.com/exos_22.5/EXOS_User_Guide_22_5.pdf

https://documentation.extremenetworks.com/exos_commands_22.5/EXOS_Command_Reference_22_5.pdf

https://documentation.extremenetworks.com/ERS_Series/ERS49005900/SW/76x/9035399_ConfigSysERS49005900_7.6_CG.pdf

https://documentation.extremenetworks.com/ERS_Series/ERS49005900/SW/76x/9035388_CLIRefERS49005900_7.6_CRG.pdf

2. ExtremeWireless Campus Solutions

<https://www.extremenetworks.com/products/wireless/>

https://documentation.extremenetworks.com/wireless/v10_41/UG/Wireless_User_Guide.pdf

https://documentation.extremenetworks.com/wireless/v10_41/CLI/Wireless/Open_Source_Declaration/c_about-this-guide.shtml

https://documentation.extremenetworks.com/wireless/v10_41/Integration_Guide/Wireless_Integration_Guide.pdf

3. Extreme Management Center

<https://www.extremenetworks.com/product/management-center/>

https://documentation.extremenetworks.com/netsight/8.1/9035435_InstallationGuide.pdf

https://documentation.extremenetworks.com/netsight/8.1/9035223-03_XMC.pdf

4. ExtremeControl

<https://www.extremenetworks.com/product/extremecontrol/>

https://documentation.extremenetworks.com/netsight/8.1/9035440-01_ExtremeControl.pdf

5. ExtremeAnalytics

<https://www.extremenetworks.com/product/extremeanalytics/>

https://documentation.extremenetworks.com/netsight/8.1/9035426_Analytics_Deployment.pdf

https://documentation.extremenetworks.com/netsight/8.1/9035425-01_ExtremeAnalytics.pdf

6. Extreme Management Center, ExtremeControl, ExtremeAnalytics Virtual Engine Installation Guide

https://documentation.extremenetworks.com/netsight/8.1/9035427_EMCAAA_Virtual_Engine_Install_Guide.pdf

7. GTAC Knowledge

<https://gtacknowledge.extremenetworks.com/>