



# Fabric Edge Design and ERS Migration Guide

9037907-00 Rev AA  
October 2023



Copyright © 2023 Extreme Networks, Inc. All rights reserved.

## Legal Notice

, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

## Trademarks

and the logo are trademarks or registered trademarks of , Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on trademarks, see:

## Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses.

End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>



# Table of Contents

---

<b>Preface.....</b>	<b>4</b>
Text Conventions.....	4
Documentation and Training.....	5
Help and Support.....	6
Subscribe to Product Announcements.....	6
Send Feedback.....	7
<b>Overview.....</b>	<b>8</b>
<b>VSP Edge Fabric Concepts.....</b>	<b>9</b>
Reasons for Fabric to the Edge.....	9
Fabric Edge Concept.....	10
Onboard Segment.....	11
Plug-and-Play Deployment.....	12
Multi-Area.....	12
<b>Fabric Edge Solution Elements.....</b>	<b>13</b>
Fabric Edge Switches and Default Gateway Routing (DVR/VRRP).....	14
Default Gateway and Routing at MDF.....	15
Port Auto-Sense.....	16
Host Attachment and Peer device detection with auto-sense.....	16
Zero Touch Fabric.....	21
Management Integration and automated Onboarding (ZTP+).....	23
Network Access Control.....	24
Radius VSA support:.....	25
Dynamic Radius based ACLs with Extreme-Dynamic-ACL VSA.....	25
<b>Scaling VSP Edge Fabric with Multi-Area.....</b>	<b>27</b>
<b>Migrating to Fabric Edge while introducing Multi-Area.....</b>	<b>29</b>
<b>Migrating to Fabric Edge from ERS Edge Switches.....</b>	<b>33</b>
Migrating from a Fabric Edge or Fabric Attach ERS switch.....	33
Migrating from a Fabric Attach Edge ERS Stack.....	34
Migrating from a Fabric Edge ERS Switch.....	35
<b>Appendix A: Acronyms.....</b>	<b>37</b>
<b>Index.....</b>	<b>39</b>



# Preface

---

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.






## Text Conventions

---

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

**Table 1: Notes and warnings**

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

**Table 2: Text**

Convention	Description
screen displays	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words <i>enter</i> and <i>type</i>	When you see the word <i>enter</i> in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says <i>type</i> .
<b>Key names</b>	Key names are written in boldface, for example <b>Ctrl</b> or <b>Esc</b> . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press <b>Ctrl+Alt+Del</b>
<i>Words in italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
<b>NEW!</b>	New information. In a PDF, this is searchable text.

**Table 3: Command syntax**

Convention	Description
<b>bold text</b>	Bold text indicates command names, keywords, and command options.
<i>italic text</i>	Italic text indicates variable content.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ <b>x</b>   <b>y</b>   <b>z</b> }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
<b>x</b>   <b>y</b>	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member[member...]</i> .
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

## Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware and software compatibility](#) for Extreme Networks products  
[Extreme Optics Compatibility](#)  
[Other resources](#) such as white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit [www.extremenetworks.com/education/](http://www.extremenetworks.com/education/).

---

## Help and Support

---

If you require assistance, contact using one of the following methods:

### Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

### The Hub

A forum for customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by employees, but is not intended to replace specific guidance from GTAC.

### Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit [www.extremenetworks.com/support/contact](http://www.extremenetworks.com/support/contact).

Before contacting for technical support, have the following information ready:

- Your service contract number, or serial numbers for all involved products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

## Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to [The Hub](#).
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

## Send Feedback

---

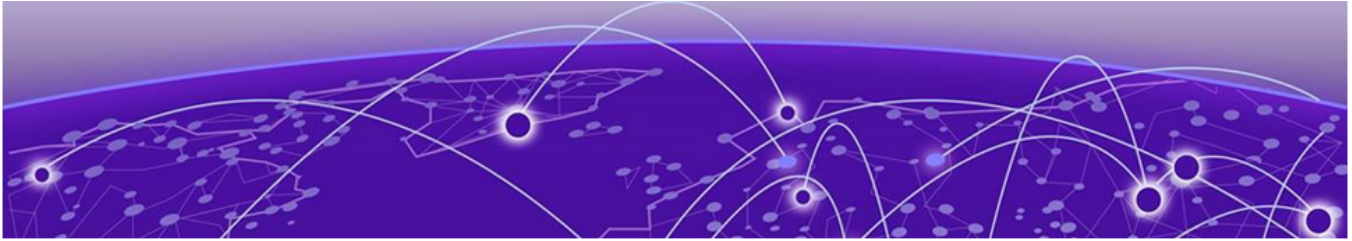
The Information Development team at has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, do either of the following:

- Access the feedback form at .
- Email us at .

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.



## Overview

---

This document provides design guidelines for a Fabric to the Edge solution based on the Extreme VOSS/Fabric Engine switch operating system, which includes VSP and Universal platforms. It also provides a migration guide for migrating existing ERS edge deployments to fabric edge.

Enterprise networking requirements have evolved, but the basic way that networks are deployed and operated has largely remained the same.

Driven primarily by IoT, network security through segmentation has become important to ensure that only the devices which are allowed to communicate with each other can do so, while remaining isolated from the rest of the IT environment.

With traditional networking solutions, the connectivity services (VLANs for Layer 2 and IP subnets; VRFs for Layer 3 separation), as well as the physical infrastructure are tightly coupled. Since connectivity service configuration is “locked” into the infrastructure, network changes are complex to implement and require extensive planning prior to implementation. Network changes typically require long maintenance windows.

With fabric-based solutions, the infrastructure layer and the service layer are logically separated from each other and are only loosely coupled at the service access layer. As a result, services can be deployed independent of the physical topology of the underlying infrastructure. This enables provider-like connectivity service provisioning and automation of service deployments. The foundation for heavily segmented logical networks is built, as required for security reasons for networks where IoT devices are available everywhere.

Expanding the reach of fabric to the edge of the network is the next logical step in creating a true end-to-end service enabled infrastructure with end-point-only provisioning and true zero-touch deployment.





# VSP Edge Fabric Concepts

---

[Reasons for Fabric to the Edge](#) on page 9

[Fabric Edge Concept](#) on page 10

[Onboard Segment](#) on page 11

[Plug-and-Play Deployment](#) on page 12

[Multi-Area](#) on page 12

Extreme's Fabric Engine and Virtual Operating System Software (VOSS) based VSP or Universal Platforms with SPB (IEEE 802.1Q) fabric to the edge is a novel concept where the fabric is extended all the way to the network access layer, enabling the attachment of clients (users, phones and IoT devices) directly to fabric enabled switches. While this has already been possible, the new Fabric to the edge features add a broad set of implicit automation capabilities, facilitating a smooth user experience.

An Edge fabric solution does not provide a stacking approach, where a set of edge switches are managed with one management IP address. It maintains all switches as separate entities. The physical deployment topology does not change compared to a non-fabric edge deployment, but the way of operating the network is different and simplified.

This document outlines how a fabric-based edge is designed, deployed and operated and what its core benefits and differences are.

## Reasons for Fabric to the Edge

---

The design goal of extending fabric to the Campus-Edge (IDF) is to simplify all operational aspects of a network solution, from initial deployment to network expansions, and daily operations. Additionally, the potential failure domain is reduced to a single switch, which typically reduces the affected users, in the case of software or hardware failures, to only 48 user ports.

This is accomplished by removing everything that is not essential in providing a viable edge solution by either omitting it or merging it into the single fabric protocol, reducing the configuration required for an edge switch to a minimum.

Additional focus has been put on implicit automation of the fabric solution through zero touch fabric, reducing the need for network operators to explicitly configure and automate the infrastructure.

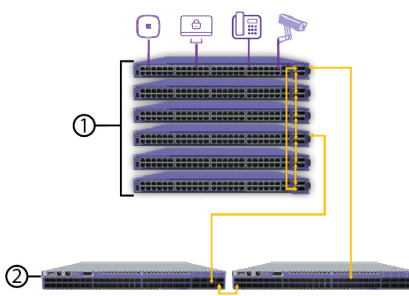
## Fabric Edge Concept

A fabric edge solution expands the fabric from the core and aggregation (MDF) layer of the network, to the access the (IDF) switching layer. Instead of stacked IDF access switches, the IDF switches remain standalone switches that are individually managed. Switch stacking was originally invented to reduce the configuration effort at the network edge, allowing network operators to apply network configurations such as VLAN IDs one time at the network edge (stack) and then add user ports to it on demand.

With Fabric to the Edge, there is no stacking and each switch is managed individually. However, by minimizing the amount of configuration required at the edge through port auto-sense automation capabilities, fabric edge is much simpler to manage than traditional stacked architectures.

Many networks rely on zero-trust approaches where end-users and end-devices are authenticated by a centralized Network Access Control solution before they are granted access to the network. With this approach the hosts are not only authenticated, but VLANs with IP Subnets, service IDs, and user policies (filters) are applied through Network Access Control (NAC), using EAPoL and/or MAC based authentication.

This approach removes the need for pre-configuration of VLANs and user policies on edge switches, as they are dynamically applied based on the authentication results.

 <p><b>Figure 1: Deploy flexible port templates to multiple ports simultaneously</b></p>	<p>Not only NAC based deployments, but also non-NAC based networks can benefit from a fabric to the edge solution: For static mappings, client deployment simplification can be achieved by deploying flexible port templates from XIQ-Site Engine that can be applied to a bulk of ports simultaneously. Based on a smart port functionality, switch-to-switch link configuration is automated with Zero-touch-fabric, which automatically establishes fabric connectivity among devices within an IDF, as well as towards the MDF, since there is no need to configure stacking or uplinks to the aggregation layer anymore.</p>
<p>1 - IDF</p>	<p>2 - MDF</p>

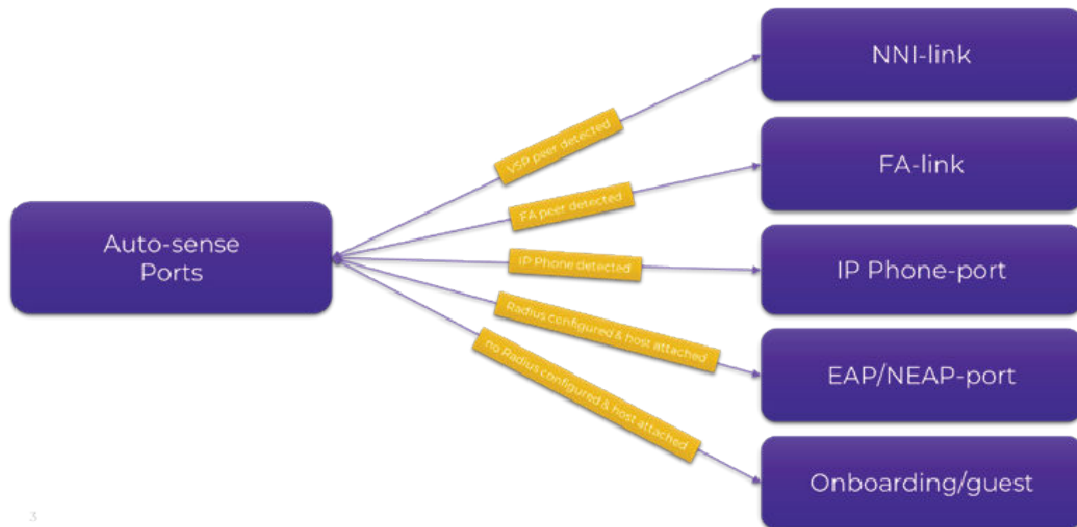
Edge automation is enabled by this new port functionality where a port state can change based on sensing what is connected to it. This smart port functionality is called port auto-sense.

Zero-touch-fabric leverages the port auto-sense functionality to detect whether a fabric switch is connected to another fabric capable switch. If detected, the fabric is automatically expanded to the connected switching device, signaling and negotiating all relevant fabric configuration parameters across the fabric link, enabling a plug and play deployment model.

In addition to fabric link detection, auto-sense port functionality can also detect fabric-attach (FA) capable devices such as EXOS and ERS switches, and Access Points or third-party FA capable devices, enabling automated service signaling directly from the FA device.

Auto-sense ports can also detect whether they are connected to IP Phones or hosts with or without 802.1X login procedures.

This elaborate auto-sense port state-machine reduces the need for edge switch configurations dramatically, and simplifies IDF deployments significantly.

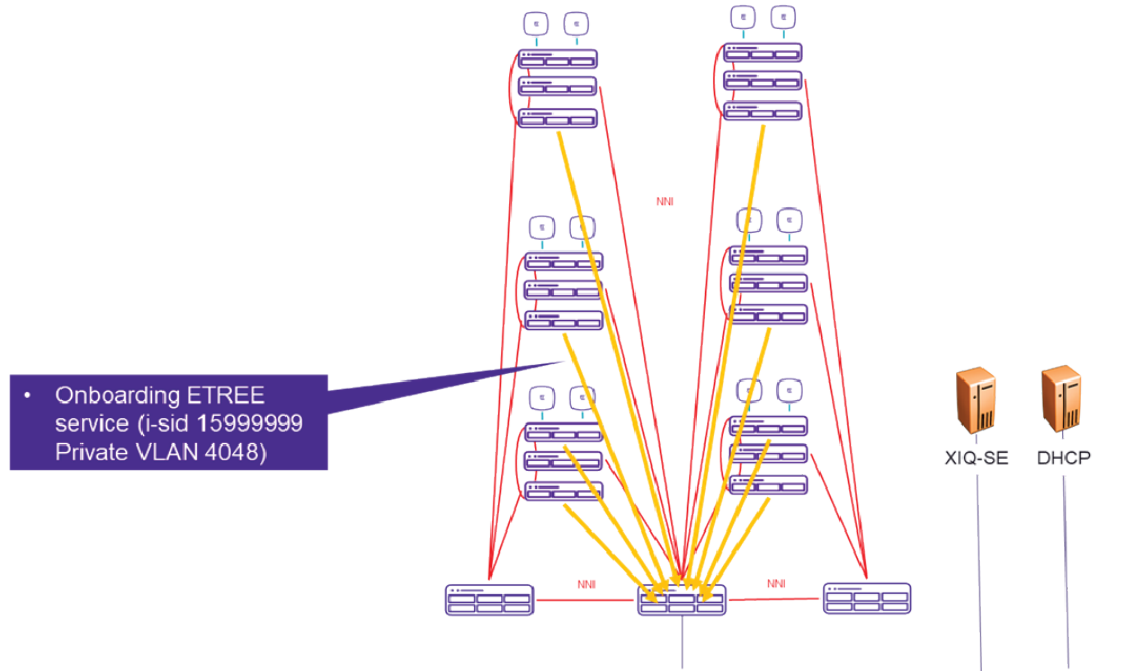


**Figure 2: Plug & Play Enabled by Auto-sense Ports**

For more information on auto-sense, see [Port Auto-Sense](#) on page 16.

## Onboard Segment

An additional important element of this zero-touch deployment solution is the secure onboarding service (PVLAN/E-TREE ISID: 4048/15999999). The fabric automatically creates an isolated “dark” onboarding segment. Each network device that boots without a configuration can securely reach the network management services such as DHCP, DNS, Radius, network management servers and, if desired, cloud services. The onboarding-service ensures secure reachability to the management tools for all connected network devices as well as end-devices. End-devices remain in an isolated guest segment until they are assigned to a specific user segment.



**Figure 3: Onboard Segment**

## Plug-and-Play Deployment

Fabric capable switches can be deployed as plug-and-play devices with factory default settings, which means there is no configuration file on the systems. During the onboarding procedure using XIQ or XIQ-SE, an automated software upgrade is performed if it is required. The switches form a new fabric automatically or can connect to an existing fabric that is auto-sense capable, get an IP address from a DHCP server, and onboard to the management servers such as XIQ and XIQ-Site Engine automatically for further provisioning.

Ports on those devices accept any device into a guest or onboarding segment, which ensures touchless onboarding for any connected end-device.

After the switches are onboarded to XIQ Site-Engine, a (ZTP) starter configuration can be downloaded, and optionally RADIUS server reachability information and credentials can be deployed. The network is then fully EAP/NEAP enabled. The provided deployment experience has been seamless.

## Multi-Area

For larger networks, a fabric based end-to-end architecture can increase the number of nodes in a fabric to a point where the network should be segmented into multiple Interior-Gateway-Protocol (IGP) IS-IS areas. With SPB multi-area, a highly scalable option is provided. SPB multi-area allows creating very large fabric topologies with tens of thousands of fabric nodes in a single end-to-end fabric providing a seamless, consistent user and operational experience even extending to branch offices.



# Fabric Edge Solution Elements

[Fabric Edge Switches and Default Gateway Routing \(DVR/VRRP\)](#) on page 14

[Port Auto-Sense](#) on page 16

[Zero Touch Fabric](#) on page 21

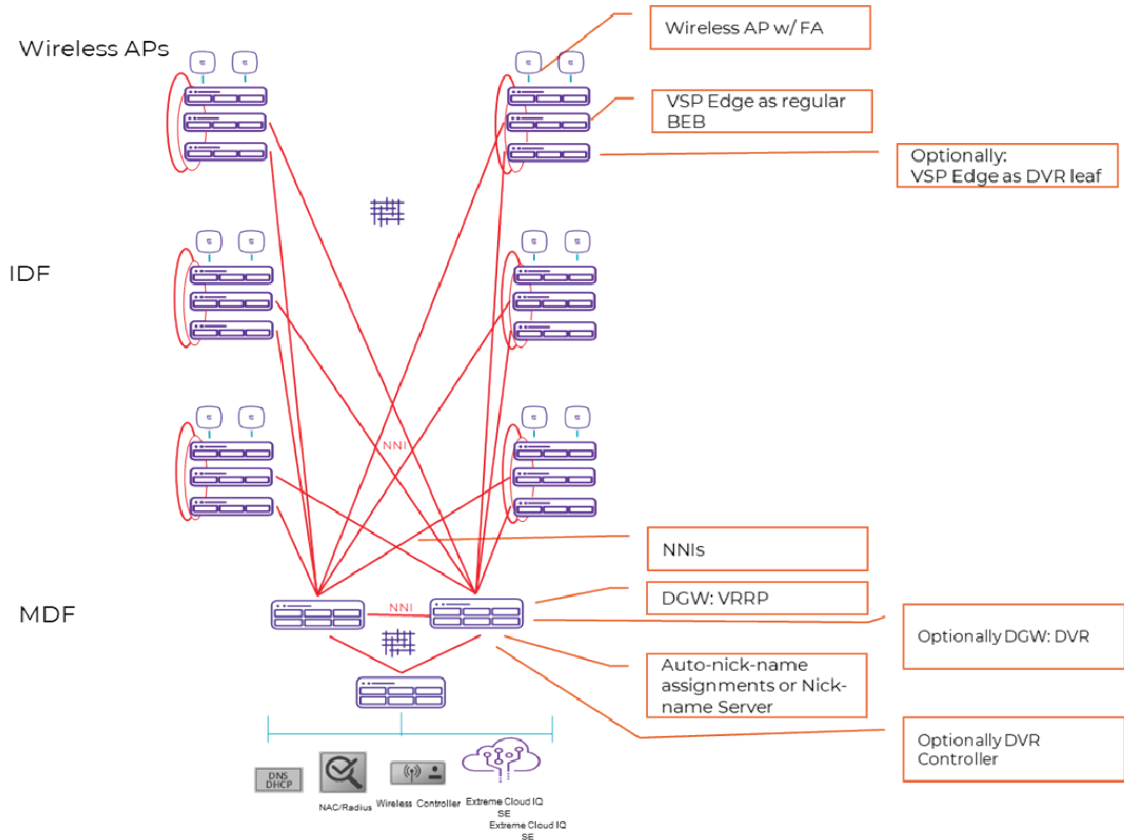
[Management Integration and automated Onboarding \(ZTP+\)](#) on page 23

[Network Access Control](#) on page 24

Table 4 illustrates the elements of a fully automated Fabric edge solution. When all the elements are deployed, the network operator reaps the maximum benefits from the solution. The solution can also be operated with a sub-set of the items deployed. Certain aspects of the solution must be operated manually or use alternative management options. For example, a network operator can decide to configure the fabric manually; the network operator does not want a zero-touch fabric deployment. When the solution is deployed, it provides a similar user experience for end-user connectivity.

**Table 4: Elements of a Fully Automated Fabric Edge Solution**

Item	Traditional (Fabric) Networking	Fabric to the Edge
IDF / Access switch interconnects	Stacking	Zero Touch Fabric - NNIs (Optionally DVR-leaf)
MDF / Aggregation switch interconnects	SMLT / Fabric Attach	Zero Touch Fabric - NNIs (with auto nick-name or nick-name server)
L3 routing	RSMLT / VRRP	VRRP (optionally DVR controller)
Management integration	Manual initial config and onboarding	Automated onboarding (ZTP+), management ISID
Host attachment (clients, phones, APs, IoT)	Manual per port config, XIQ-SE port templates	Auto-sense or XIQ-SE port templates
Per port Network Access Control (NAC) config	Manual EAP / NEAP config per port	Auto-sense
User based filter policies	Dynamic user based policies / Dynamic Radius ACLs	Dynamic Radius ACLs
Fabric scale	Fabric in core and aggregation layer only	Fabric to the Edge with SPB Multi-area



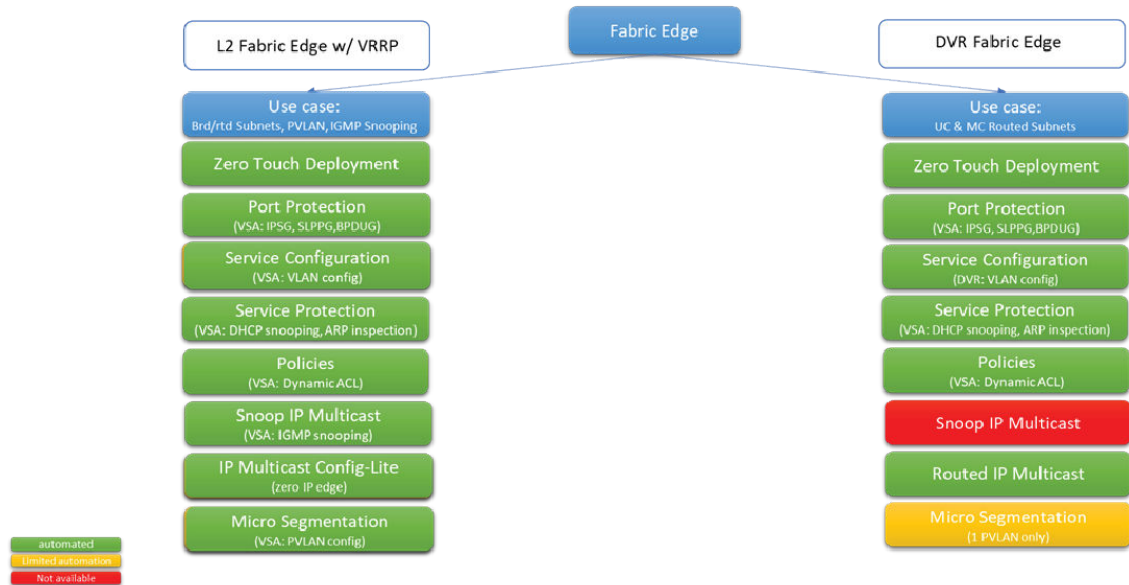
**Figure 4: VSP Fabric Edge Deployment Overview**

## Fabric Edge Switches and Default Gateway Routing (DVR/VRRP)

Fabric Edge Switches are not stacked; they are operated as individual single units. Since those switches are not managed in the IDF as a single entity, Fabric Edge is used to reduce the configuration on each switch in the IDF to a minimum and as a result, reduce the churn of configuration to a minimum. This is accomplished by using port “auto-sense” which drastically reduces the need for manual edge port configuration.

Auto-sense ports are based on the VOSS/Fabric Engine Flex Uni functionality. If NAC with Radius is deployed, then port VLAN I-SID service bindings can be applied through Radius authentication VSA responses. When no NAC is deployed, auto-sense I-SID configuration allows dynamic assignments of I-SIDs to devices based on their LLDP signature, such as wireless AP, camera, IP phone, or client.

There are two deployment models for router redundancy and Fabric Edge deployments: VRRP or DVR based:



**Figure 5: Deployment Models for Router Redundancy**

## Default Gateway and Routing at MDF

The L2 Fabric Edge with VRRP solution provides the most feature rich deployment model while at the same time keeping operational models consistent with the rest of the fabric infrastructure. Especially in deployments where Network Access Control is used not only for client authentication but also for application of port and service protection features, a deployment can be fully automated such that access ports have no configuration at all. Any necessary configuration is applied during user authentication. Extreme with Extreme Control provides a complete solution packet for this deployment model. Other third party Radius systems can also be used by importing the corresponding Extreme dictionaries.

Additionally, micro segmentation or “dark” ISIDs are available in this deployment model by assigning an I-SID to a PVLAN. The PVLAN can be created on demand through a Radius VSA response.

Optionally, DVR as a Fabric Edge deployment model can be leveraged for use cases where IP Multicast routing is the predominant driver.

With DVR I-SID based capabilities such as IP Unicast and IP Multicast, routing can be enabled on the DVR controllers centrally. This functionality can then be applied to all DVR leafs on a per I-SID basis, keeping the switch configuration at the edge very light.

Additionally, in such a deployment option with a DVR controller/leaf setup, a DVR-VRRP interoperation function can be leveraged in the case where some non-DVR BEBs are using the same I-SIDs.



**Note**

In a DVR Edge setup, IGMP snooping is not supported. All IP Multicast are routed.



## Port Auto-Sense

Following are additional details of the port auto-sense capabilities. It is a best practice to review which part of the port auto-sense state machine will be used prior to deploying a Fabric Edge solution. Setting global auto-sense configuration parameters and downloading them as switch starter configurations provides the desired outcomes.

Here is a list of the current global auto-sense configuration options:

```
auto-sense voice i-sid <1-6777215> c-vid <1-4094>
auto-sense onboarding i-sid <1-6777215> (default 15999999)

auto-sense fa wap-typel i-sid
auto-sense fa camera i-sid
auto-sense faproxy-switch i-sid
auto-sense fa ovs i-sid
auto-sense fa authentication-key
auto-sense fa message-authentication

auto-sense isis hello-auth type hmac-md5
auto-sense isis hello-auth type hmac-sha-256
auto-sense isis hello-auth type simple
auto-sense isis hello-auth type none

auto-sense access-diffserv
auto-sense dhcp-detection
auto-sense qos 802.lp-override
auto-sense type none

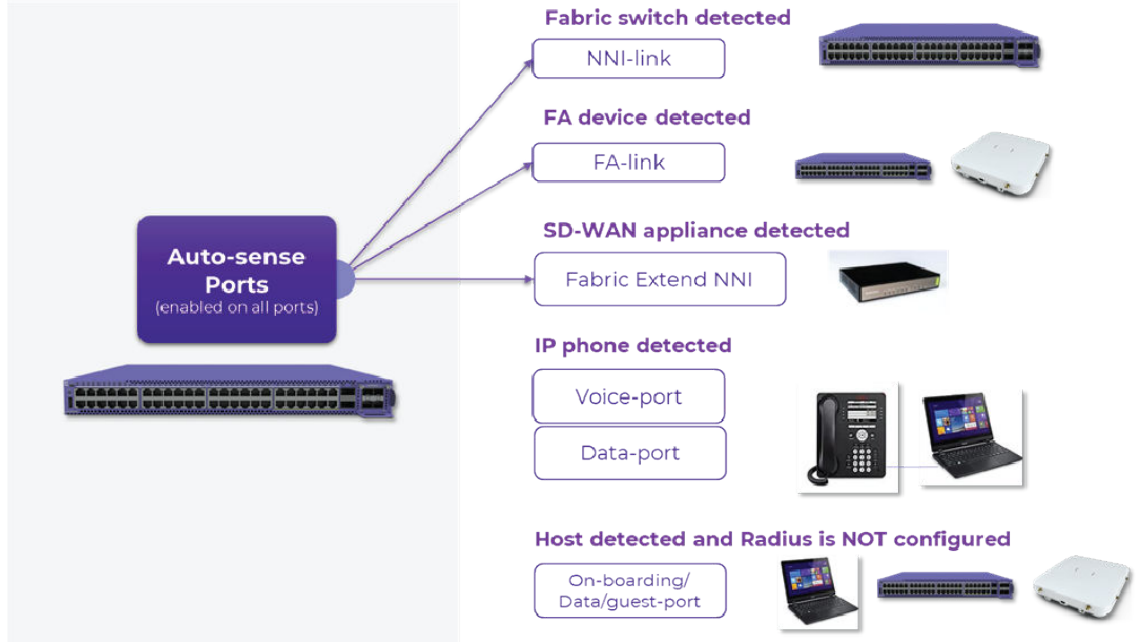
auto-sense eapol voice lldp-auth
auto-sense eapol fa wap-typel status authorized
auto-sense eapol fa camera status authorized
auto-sense eapol fa virtual-switch status authorized
```

## Host Attachment and Peer device detection with auto-sense

The switch is sensing neighbor information on all auto-sense ports and converts the ports as follows:

- Zero Touch Fabric (ZTF) is started if a VSP peer with auto-sense or an NNI peer configuration with release 8.3 or later is detected
- If an FA capable device is detected, then the FA state is selected based on neighbor identification
  - FA Proxy-Switch
  - FA Wireless AP
  - FA Camera
- If an IP phone is detected on a port, the switch starts signaling LLDP-MED, if auto-sense voice parameters are set globally
- If an SD-WAN device is detected, the switch can learn Fabric Extend Configuration automatically.
- If none of the above is detected, the port is classified as a user/host (UNI) port.





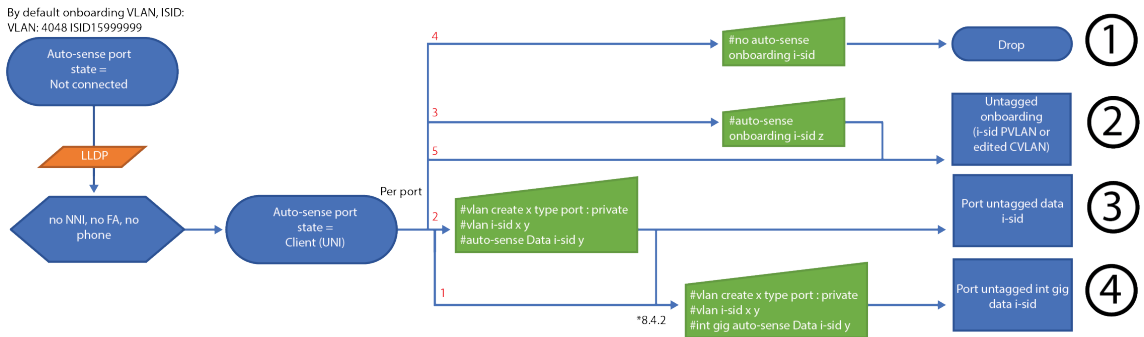
**Figure 6: Auto-Sense Ports**

Following are the detailed flow charts for the different auto-sense states:



**Figure 7: Auto-Sense Fabric NNI**

1	Port is operating in NNI state.
---	---------------------------------



**Figure 8: Auto-Sense Client UNI without NAC**

1	Drop
2	Onboarding state
3	Global data i-sid for untagged client device state
4	Per port data i-sid for untagged client device state

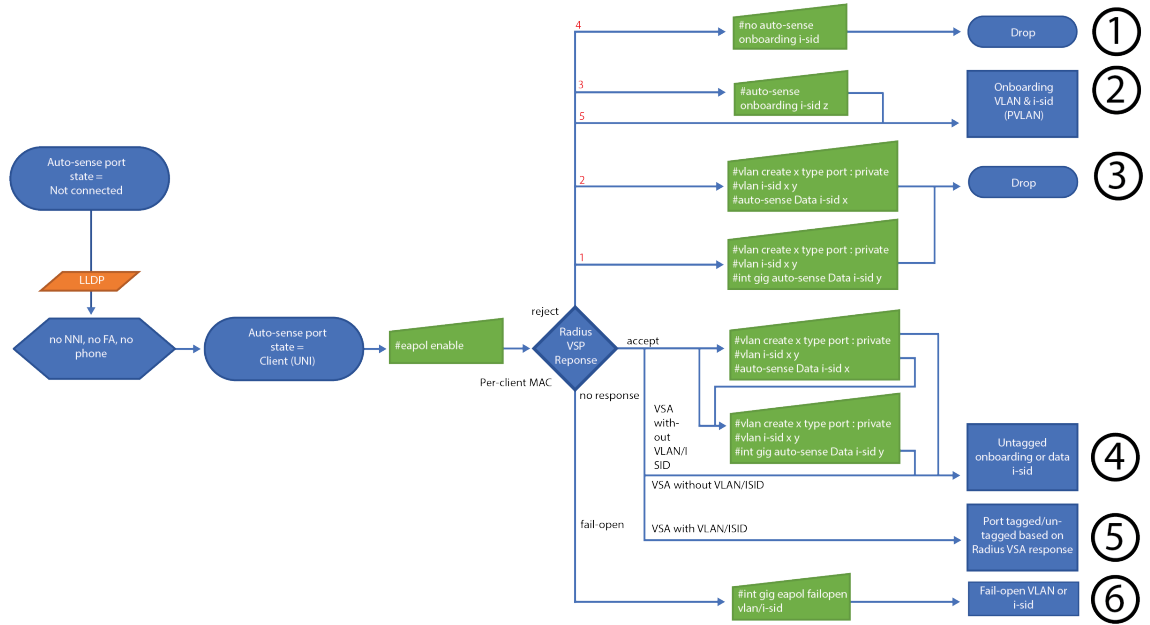


Figure 9: Auto-Sense Client UNI with NAC

1	Drop
2	Onboarding and guest i-sid state with NAC
3	No onboarding, no guest i-sid reject state
4	Authenticated client device on onboarding or data i-sid
5	Authenticated client device state with VLAN/i-sid assignment
6	Fail-open state in case no response from Radius

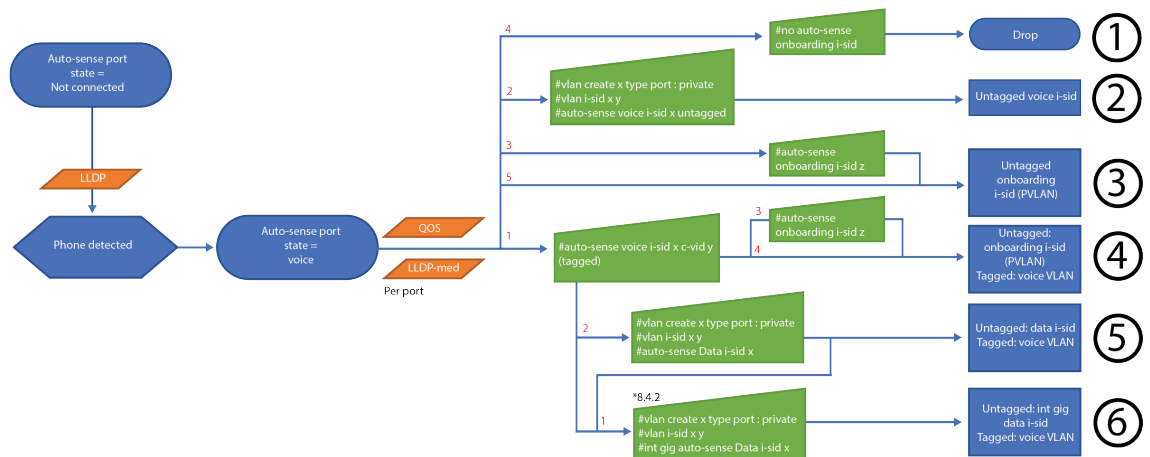
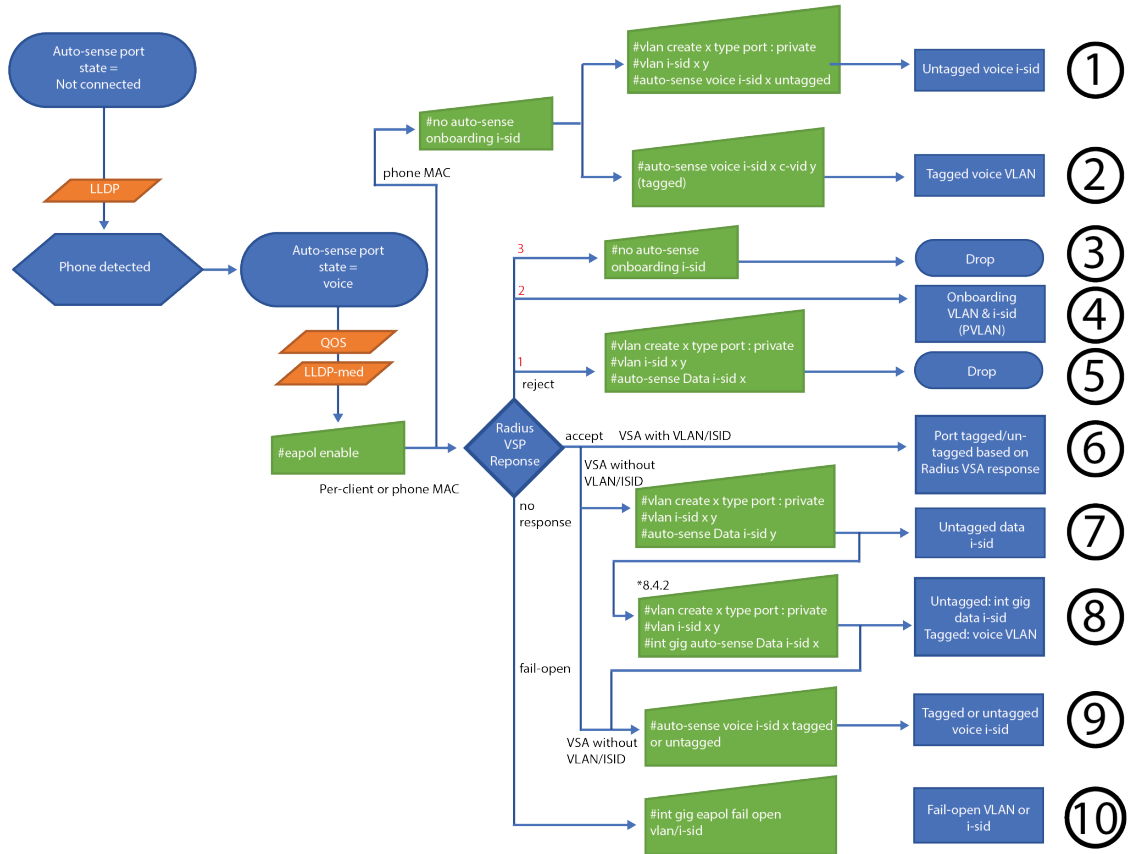


Figure 10: Auto-Sense Voice UNI without NAC

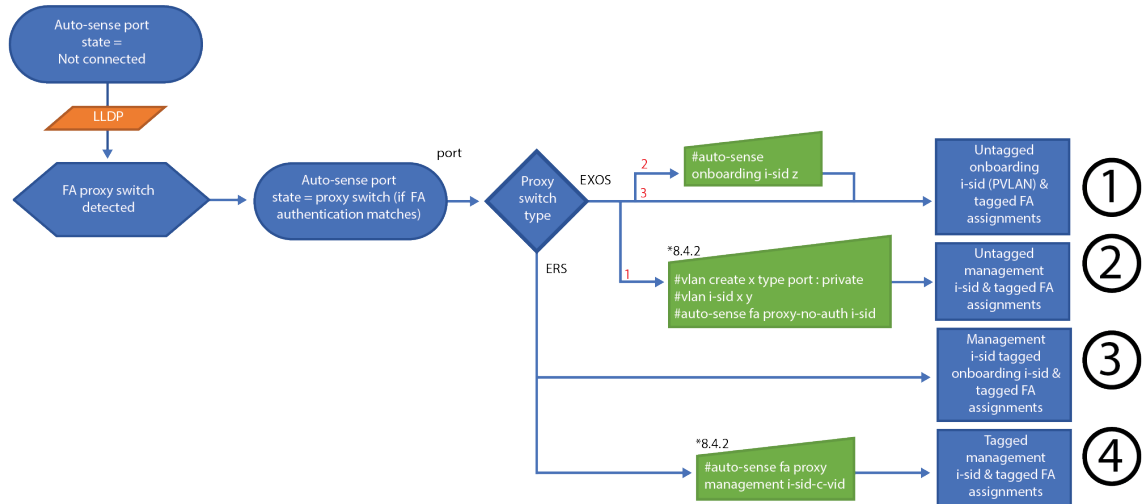
1	Drop
2	Untagged phone without authentication on voice i-sid
3	Untagged unauthenticated phone or device behind phone on onboarding i-sid

4	Unauthenticated tagged phone on voice i-sid and untagged device behind tagged phone on onboarding i-sid
5	Unauthenticated tagged phone on voice i-sid and untagged device behind tagged phone on global data i-sid
6	Unauthenticated tagged phone and untagged device behind tagged phone on per port data i-sid



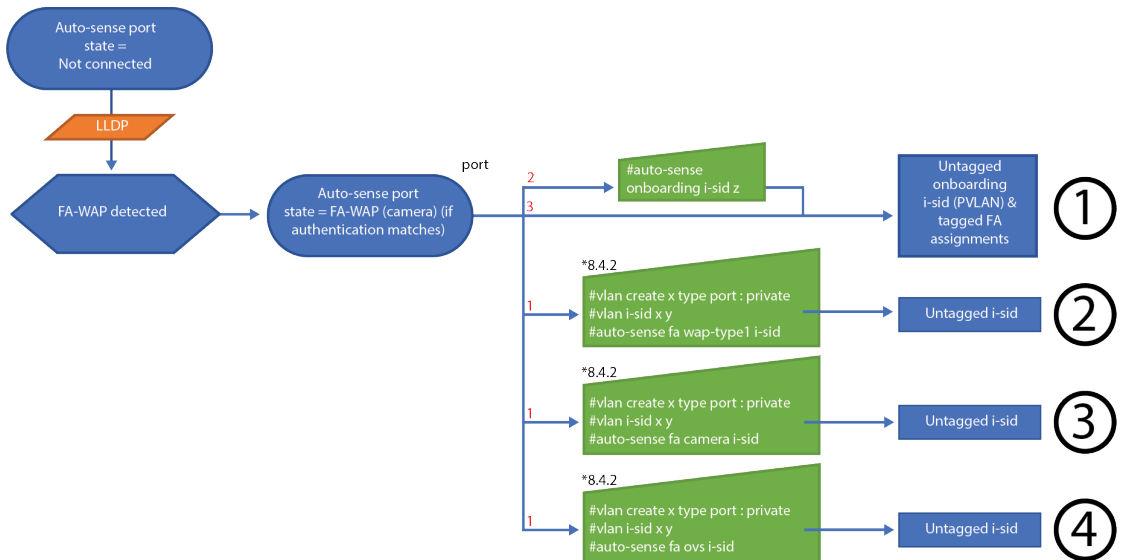
**Figure 11: Auto-Sense Voice UNI with NAC**

1	Lldp authenticated untagged phone on voice i-sid
2	Lldp authenticated tagged phone on voice i-sid
3	Drop
4	Rejected device classified on guest/onboarding i-sid
5	Rejected device dropped
6	Phone or device authenticated and classified in Radius provided i-sid
7	Phone or device authenticated and classified into global data i-sid
8	Phone or device authenticated and classified into per port data i-sid
9	Phone (or device) authenticated and classified into tagged or untagged voice i-sid
10	If configured fail-open i-sid if no response from Radius



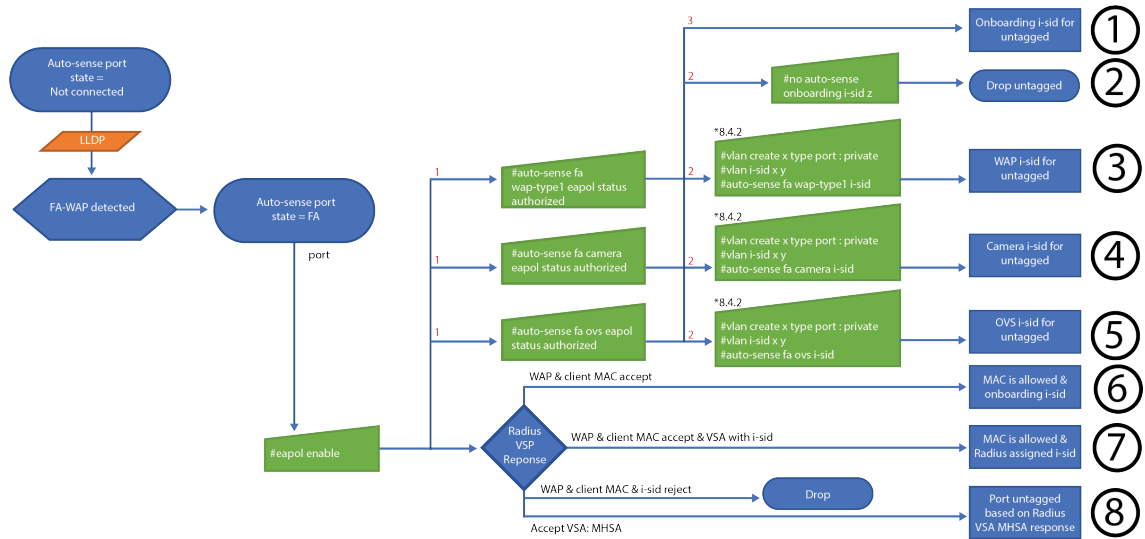
**Figure 12: Auto-Sense FA Proxy Switch**

1	Management of FA EXOS switches on untagged onboarding i-sid. FA for tagged bindings.
2	Management of FA EXOS switches on untagged proxy-switch-i-sid (without FA authentication)
3	Management of FA ERS switches on tagged onboarding i-sid. FA for tagged bindings.
4	Management of FA ERS switches on tagged proxy-switch management i-sid.



**Figure 13: Auto-Sense FA WAP, Camera, Open Virtual Switch without NAC**

1	FA enabled device untagged on onboarding i-sid
2	FA enabled device untagged on dedicated wap-i-sid
3	FA enabled device untagged on dedicated camera-i-sid
4	FA enabled device untagged on dedicated open-vswitch-i-sid



**Figure 14: Auto-Sense FA WAP with NAC**

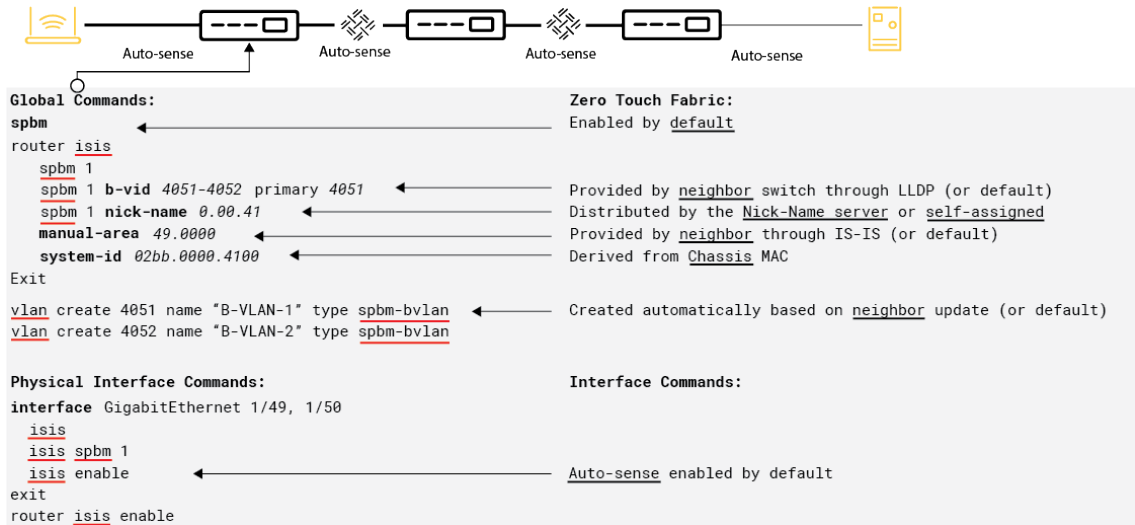
1	Removes Radius authentication on auto-sense port that detected wap-type1, camera, or ovs, and sends untagged traffic sent into onboarding i-sid.
2	Removes Radius authentication on auto-sense port that detected wap-type1, camera, or ovs, and drops untagged traffic.
3	Removes Radius authentication on auto-sense port that detected wap-type1. Untagged traffic sent into wap-i-sid.
4	Removes Radius authentication on auto-sense port that detected camera. Untagged traffic sent into camera-i-sid.
5	Removes Radius authentication on auto-sense port that detected ovs. Untagged traffic sent into ovs-i-sid.
6	WAP or client MAC accepted on onboarding i-sid
7	WAP or client MAC accepted on Radius provided i-sid
8	WAP or client MAC dropped
9	WAP MAC authenticated, any other MAC allowed on port (for authentication by WAP)

## Zero Touch Fabric

Zero touch fabric relies on the following key functionalities:

- Port Auto-sense
- Dynamic IS-IS Area & BVID assignments
- Dynamic Nick-Name assignment through auto-nickname or nickname server

For a new fabric node to participate in an SPB fabric, it needs to agree on a few parameters with the existing fabric. The parameters are Common IS-IS area ID and Backbone VLAN IDs, Unique System ID, and Nick-Name.



### Figure 15: Zero Touch Fabric

All configuration elements to establish fabric connectivity are either set by default or derived from a peer switch, so a newly introduced fabric node can be brought online without any pre-configuration.

IS-IS Area ID and Backbone VLAN IDs are exchanged and automatically negotiated on a per link basis when a switch is connected to an Auto-Sense enabled port on an existing fabric switch. The System ID is derived from the Chassis MAC address and is available at startup. The Nick-Names can be auto-signed by the node itself or can be assigned by a DHCP-like Nick-Name server.

To accomplish this, one or two network nodes per area are selected by the network administrator to be the seed switch acting as a Nick-Name server for the area. It is a best practice to use Nick-Name server functionality, especially in a Multi-Area setup.

Switches communicate on the automatically established Fabric Area Network (FAN) I-SID with each other in order for the nick-name server to hand out the requested unique Nick-Names. The Nick-name servers themselves need static Nick-Names and are assigned a prefix so that they can serve a unique range of nick-names in a network.



#### Note

It is important that between two adjacent IS-IS areas the Nick-Names are unique.

Example configuration of Nick-name server configuration with a prefix of a.1. Setting a unique prefix avoids name collisions with statically deployed Nick-names: (for example, `spbm nick-name server prefix a.10.00`).

A fabric link only establishes if the IS-IS authentication keys are configured and match. Otherwise, a new device is connected like any other end-host to the network on the onboarding PVLAN/ETREE-ISID. The switches still onboard to XIQ-SE and the authentication keys can then be applied.

Similarly for Universal Switches, which boot with the EXOS OS by default, they connect as FA-proxy devices to auto-sense ports and automatically onboard to XIQ/XIQ-SE.

From there they can then be converted to VOSS devices where the onboarding procedure restarts and the fabric establishes.

For green-field deployments the first fabric device typically has to be selected as the Nick-Name server for the IS-IS area. It also hands out the IS-IS area ID and BVIDs to be used in the area. A best practice is to configure those statically on the first configured fabric node in the area. If they are not manually configured, default values are applied instead.

When VSP switches are booted without a configuration file, SPB with ZTF is automatically enabled and all ports are up and in the Auto-Sense state, ready to establish a fabric connection.

---

## Management Integration and automated Onboarding (ZTP+)

---

When a VSP switch is booted from defaults (without a configuration file), it already has a Private VLAN (PVLAN) 4048 configured globally. This is the VLAN where the switch sends DHCP requests and launches Zero Touch Onboarding using its Zero Touch Client(s) for XIQ/XIQ-SE.

Private VLAN is a construct where VLAN port members are isolated or promiscuous. Devices connected to isolated ports cannot talk to each other, even if they are in the same L2 VLAN. Only promiscuous ports in the PVLAN can communicate with isolated ports and other promiscuous ports in the same L2 VLAN.

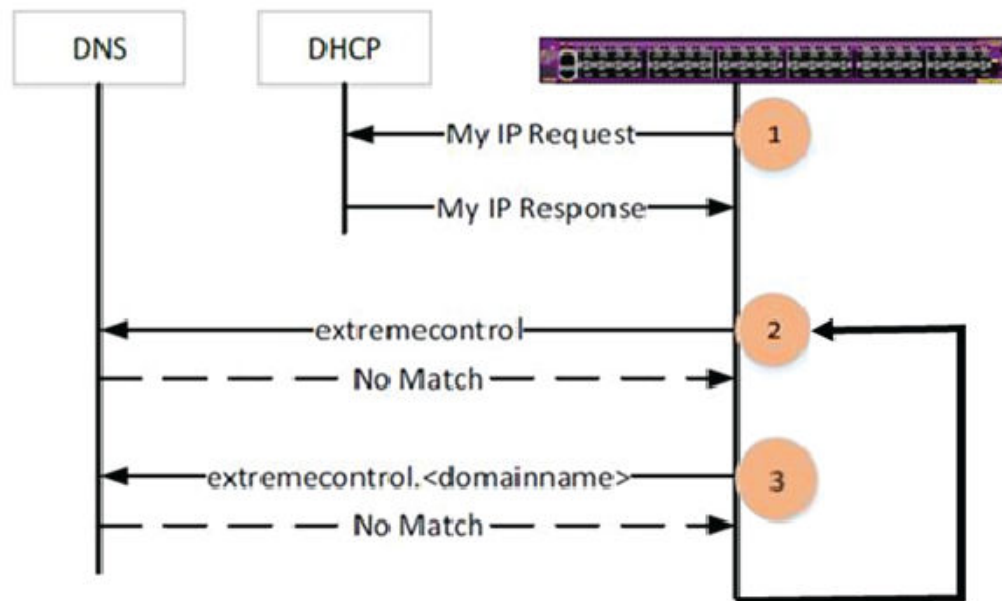
The onboarding I-SID is the I-SID mapped to the PVLAN 4048 which by default it is set to I-SID 15999999.

Use of Private-VLAN greatly helps prevent any L2 loops in this onboarding L2 segment and additionally provides secure segmentation.

VSP switches that are booted without a configuration file automatically execute a set of zero-touch procedures to facilitate an automated onboarding to XIQ and XIQ-Site Engine.

The automated procedures are as follows:

- Enable SPBM
- Enable router ISIS
- Enable auto-sense on all ports in isolated mode with the onboarding private VLAN (PVLAN) 4048 configured
  - Create private vlan 4048, secondary 4049
  - Set vlan 4048 as mgmt vlan
  - Set I-SID 15999999 to vlan 4048
  - Enable auto-sense on all ports
- Set QOS untrusted I2 and I3 on all ports
- Send a DHCP request on all active ports of the onboarding PVLAN
- After an IP address is received, activate the XIQ Cloud and XIQ-SE ZTP+ agents for registering with the management tools. For this to work, the DNS entry “extremecontrol” needs to point to the XIQ-Site Engine server.



- Management tools then start their onboarding procedures, which can include Universal Hardware persona changes, software upgrades, provisioning of Starter Configurations and launching of workflows.



#### Note

If applicable, the switch then converts the port where it received the DHCP response from PVLAN-isolated to PVLAN-promiscuous. This ensures that any further switches that are connected to this switch have bridged reachability to the DHCP server. If the DHCP response was received through a tunnel or IP routed interface, no additional action is taken.

## Network Access Control

Zero trust networking with a robust network access control (NAC) function is becoming one of the key defense mechanisms against network intrusion. A fabric edge solution is fully NAC enabled and provides client authentication benefits that include client to VLAN/I-SID mapping. Additionally, when a client connects to a network by using Extreme-Dynamic-Config VSAs per port or VLAN protection attributes such as IGMP-, DHCP snooping, IP Source Guard and SLPP- and BPDU guard can be automatically applied.

For auto-sense ports, if EAPOL is configured globally and Radius server addresses are provisioned, then all auto-sense ports are able to handle EAP/NEAP authentication. A few guidelines apply:

- Ensure that the corresponding dictionary used includes the supported VSAs



- Ports that are sensed to be in a UNI state are automatically operated in the EAP MHMA-MV state (Multi-Host, Multi Authentication, Multi-VLAN). MHSA (Multi-Host, Single Authentication) can be applied through an “Extreme-Dynamic-MHSA” VSA response.
- A vendor specific attribute (Extreme-Dynamic-Config) is used for the dynamic configuration of Port and VLAN attributes

## Radius VSA support:

### Per VLAN settings:

- I-SID
- Create VLAN/PVLAN
- IGMP Snooping
- DHCP Snooping
- ARP Inspection
- D-ACL
- IP Multicast-Lite (supported starting with release 9.0)

### Per port settings:

- I-SID
- Port Speed
- Port Duplex
- SLPP Guard
- BPDU Guard
- IP Source Guard
- Traffic Control (WoL – Wake on LAN)
- Port-Bounce
- Re-Auth
- D-ACL

### Per MAC settings:

- I-SID
- D-ACL

## Dynamic Radius based ACLs with Extreme-Dynamic-ACL VSA

Additionally, on EAP/NEAP-enabled ports, dynamic ACL can be assigned through VSA attributes, which allows the application of user based policies to authenticated devices. The dynamic behavior of the ACL depends on the EAP port state (MHMV or MHSA) - which is defined under Extreme Networks vendor ID 1916 and uses the value 251.

### Examples:

The following examples provide the RADIUS configuration for the corresponding CLI filter configuration. This example is for MAC 0a:0a:0a:0a:0a:0a on port 1/1 and EAP in MHMV mode.

```
filter acl 1 type inPort
filter acl port 1 1/1
filter acl ace 1 1 name RadiusGuest-Rule01
filter acl ace ethernet 1 1 src-mac eq 0a:0a:0a:0a:0a:0a
filter acl ace ethernet 1 1 ether-type eq 0x800
filter acl ace ip 1 1 ip-protocol-type eq 17
filter acl ace protocol 1 1 dst-port eq 53
filter acl ace 1 1 action permit
filter acl ace 1 1 enable
filter acl ace 1 2 name RadiusGuest-Rule02
filter acl ace ethernet 1 2 src-mac eq 0a:0a:0a:0a:0a:0a
filter acl ace ethernet 1 2 ether-type eq 0x800
filter acl ace ip 1 2 dst-ip mask 192.0.2.1 24
filter acl ace 1 2 action permit
filter acl ace 1 2 enable
filter acl ace 1 3 name RadiusGuest-Rule03
filter acl ace ethernet 1 3 src-mac eq 0a:0a:0a:0a:0a:0a
filter acl ace 1 3 action deny
filter acl ace 1 3 enable
```

The RADIUS VSA does not specify the MAC or the port number because they are already known at the EAP level:

```
Extreme-Dynamic-ACL = "CLIENT RadiusGuest",
Extreme-Dynamic-ACL += "acl inPort",
Extreme-Dynamic-ACL += "ace 1 sec ethernet ether-type eq 0x800 & ip ip-protocol-type eq
17 & protocol dst-port eq 53 action permit",
Extreme-Dynamic-ACL += "ace 2 sec ethernet ether-type eq 0x800 & ip dst-ip mask 192.0.2.1
24 action permit",
Extreme-Dynamic-ACL += "ace 3 sec action deny"
```



# Scaling VSP Edge Fabric with Multi-Area

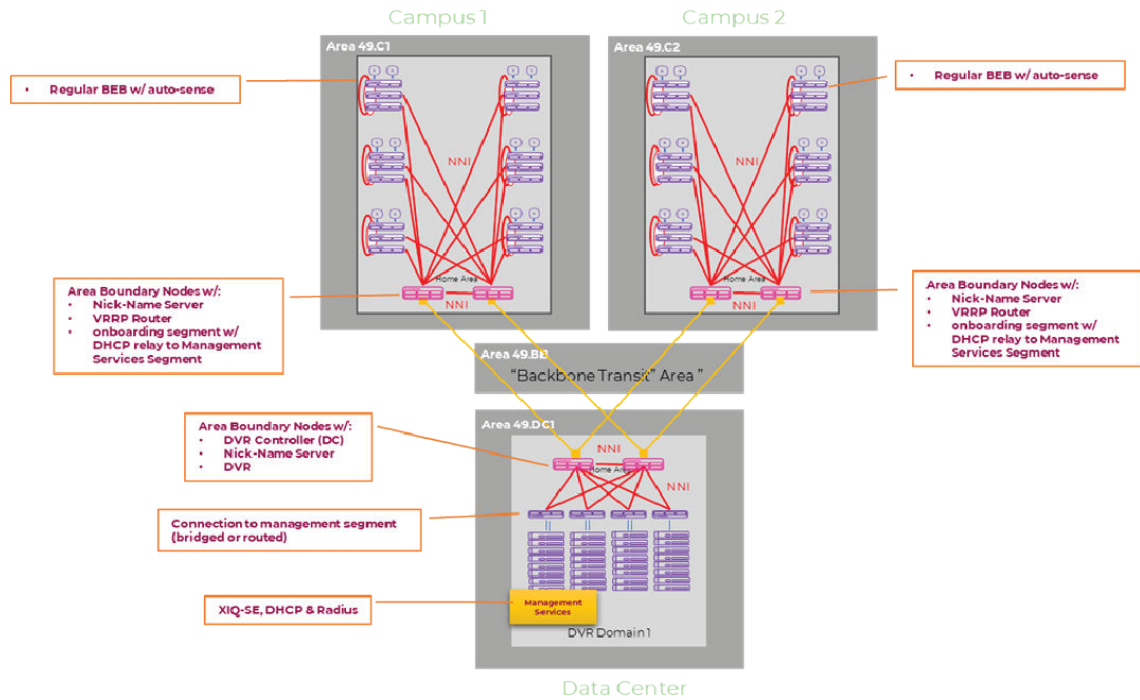
---

The number of fabric nodes can exceed 500 easily when deploying a fabric edge solution. The typical recommended maximum number of fabric enabled nodes within an area in a multi-area network is 500. For single area deployments, the maximal number of supported nodes is provided per product in the release notes. With SPB Multi-Area support, fabric areas can be interconnected, which enables fabrics that are built with tens of thousands of active nodes within a single fabric.

Consider the following guidelines when designing multi-area networks:

If Zero Touch Fabric is used, each IS-IS area needs its own Nick-Name servers. Nick-Name allocation cannot be extended across area boundaries, and all Nick-Names need to be unique across adjacent areas.

- DVR Controller – Leaf relations for a DVR domain are required to be in the same area. For example, a DVR controller cannot have leafs in another area. Use multiple DVR domains instead, because the DVR backbone can be extended between area boundaries.
- The default onboarding segment can be extended between areas. Depending on the size of the network, it might make more sense to keep onboarding segment (PVLAN 4048 – ISID 15999999) areas local and use different IP subnets per area.
- For larger multi-area deployments, plan for a “Backbone Transit Area” (BBT) design, where individual areas are interconnected using the BBT area. This design allows for scale out approaches when extending the network design. This is also the best approach when a lot of smaller areas need to be interconnected.
- I-SID assignments are network wide (across areas). A good I-SID allocation design is recommended. Best practices include defining ranges for area-local and network-wide I-SIDs.
- Area boundary nodes interconnect IS-IS areas and can redistribute services between areas. Redistribution is turned off by default, and needs to be configured according to the service deployment requirements.



**Figure 16: Four-area Campus Network Example**

Figure 16 shows all elements of a VSP edge solution with an IS-IS multi-area design approach for larger deployments where the total fabric node count exceeds 500 nodes.

The network does not require the use of all automation elements such as ZTF, ZTP+, but the use of automation elements is recommended to reap all the benefits of automation.

The example Four Area Campus network consists of MDF (aggregation layer) nodes that provide the following functionality:

- Multi-Area boundary nodes (for large buildings where a lot of edge switches are being deployed) with the home-area being the internal area of the building.
- Nick-Name server functionality to enable Zero Touch Fabric Deployment for the IDF switches.
- The onboarding ISID (default = 15999999) provides reachability to the management segment, including a DHCP server for IP address acquisition.

The wiring closet (IDF) switches are depicted as operating in DVR leaf mode. This is not mandatory, but it is beneficial, especially if IP Multicast or L3 virtualization (L3 VSNS) are deployed.

The Data Center Spine nodes provides similar Multi-Area configuration to the MDF nodes if a multi-area design is deployed.

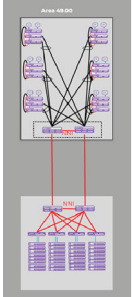


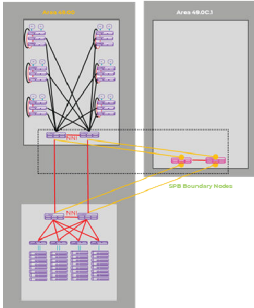
## Migrating to Fabric Edge while introducing Multi-Area

---

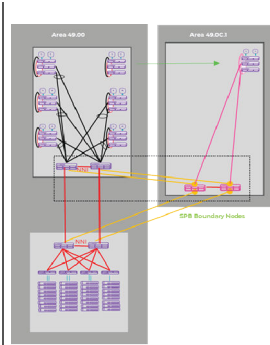
Here is an example scenario where a network is migrated from a traditional Fabric Attach/MLAG/SMLT edge to a fabric edge solution, while at the same time introducing a new area for the migrated fabric edge network.

Any existing SPB fabric can be expanded using this step by step approach while keeping migration risks at a minimum.

 <p><b>Figure 17: Interconnected Campus Network and Data Center Network</b></p>	<p>In this scenario a Campus network and a Data Center network are interconnected. The Data Center is fully fabric enabled, while only the aggregation layer is operating in fabric mode in the Campus network. The Campus wiring closets (IDF) are stacked switches using a link-trunking method, and are dual homed to two aggregation layer switches (MLAG/vIST). The aggregation layer (MDF) nodes are fabric attach server capable switches and have a fabric connect (SPB) connection to the Data Center, and possibly other buildings that are fabric enabled. Typically, the aggregation layer nodes also provide the default gateway function for some of the user subnets of the Campus network.</p>
--	--

 <p><b>Figure 18: New MDF Switches</b></p>	<p>To provide a fabric to edge solution while introducing a new IS-IS area, a best practice is to introduce a new set of aggregation layer nodes that are able to provide the multi-area capability. The new MDF nodes have their home-area in the new building, and the interconnections to the existing IS-IS area are remote-area links. For more information on home-areas and remote-areas, refer to the VSP configuration guide starting with VOSS release 8.4.</p> <p>In this example, the existing MDF nodes and the new area boundary nodes are illustrated with the dotted square. The new MDF switches can be introduced without any disruption to the existing infrastructure.</p> <p>L3 default gateway routing remains on the existing MDF switches until the IDF migration to fabric edge is completed. To ensure all services are available in the new area as well as the existing area, configure inter-area redistribution policies accordingly.</p>
--	---

	<p>When the MDF switches are in place, the new fabric to the edge nodes can be introduced to the new area and users can be migrated over to the new IDF switches at your own pace. The IDF switches can either be deployed using the automated ZTP+ / ZTF deployment option where the new edge</p>
--	--



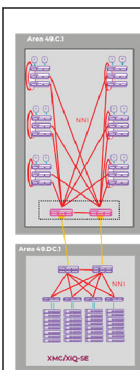
**Figure 19: New Fabric to the Edge Switches**

fabric nodes are brought up without any configuration, or they can be pre-staged. In the ZTP+/ZTF deployment option, the switches join the fabric automatically, get their management IP address through DHCP on the “onboarding i-sid” and then onboard to XMC/XIQ-SE automatically where they then get their initial starter configuration.

To facilitate this deployment option, the network operator needs to ensure that the onboarding ISID 15999999 provides reachability to the management segment including the DHCP server.

For ZTF, a Nick-name server functionality needs to be enabled in the new Campus area (49.0C1) on the MDF multi-area boundary nodes.

As a final task, the L3 Default Gateway routing function can be migrated to the new aggregation (MDF) nodes.



**Figure 20: Campus Area Operating as a Fabric to the Edge Network**

After all users have been migrated off the old IDF switches, all old switches can be decommissioned or redeployed for other uses.

The result of this migration is that now the network consists of two SPB IS-IS areas with a Campus area that is operating as a fabric to the edge network.

The same approach of introducing a new area can be taken if the network already exists, based on a fabric to the edge solution, which is based on ERS nodes:



**Figure 21: Fabric to the Edge Process**





# Migrating to Fabric Edge from ERS Edge Switches

[Migrating from a Fabric Edge or Fabric Attach ERS switch](#) on page 33

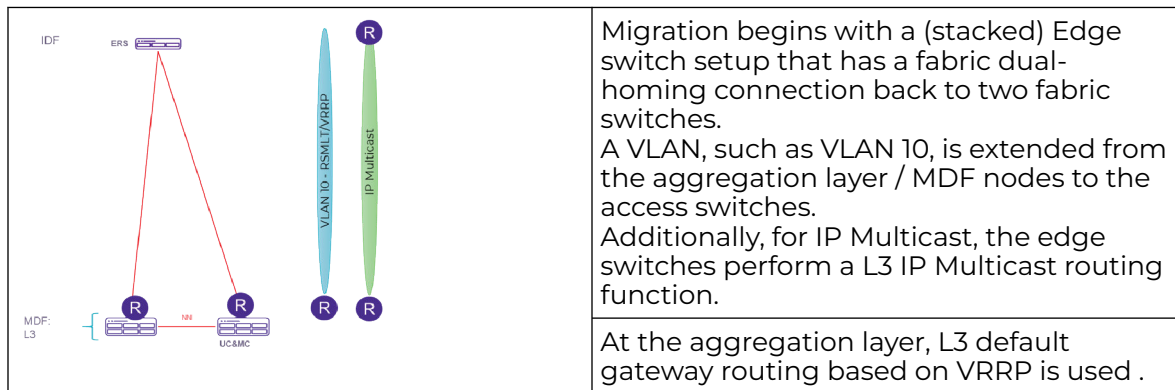
[Migrating from a Fabric Attach Edge ERS Stack](#) on page 34

[Migrating from a Fabric Edge ERS Switch](#) on page 35

The following is a high level description of how to migrate to a VSP Fabric Edge solution from different networking starting points.

## Migrating from a Fabric Edge or Fabric Attach ERS switch

Here is a high level description of how to migrate to a VSP Fabric Edge (DVR) solution from a Fabric Edge or Fabric Attach ERS switch. Fabric edge switches are deployed in non-DVR mode, so this is the typical migration approach.



To migrate an ERS Fabric Edge Switch to a VOSS Fabric edge switch, follow these best practices:

	<ol style="list-style-type: none"> <li>1. Introduce the new VSP Edge switches. Keep VRRP as the DCW routing function.</li> <li>2. For VLAN/ISIDs where no Multicast is in use, migrate users to the new VSP edge switches while still using VRRP as the default GW function.</li> <li>3. For VLAN/ISIDs where Multicast routing is required, configure SPB IP Multicast lite on VSP/fabric edge.</li> <li>4. Migrate users and decommission the ERS Fabric Edge switch.</li> </ol>
--	--

### Migrating from a Fabric Attach Edge ERS Stack

Here is a high level description of how to migrate to a VSP Fabric Edge (DVR) solution from a Fabric Attach Edge ERS Stack.

	<p>Migration begins with a (stacked) Edge switch setup that has a LAG dual-homing connection back to two fabric switches in a VIST cluster setup. A VLAN, such as VLAN 10, is extended from the aggregation layer / MDF nodes to the access switches. Optionally, Fabric Attach (FA) is deployed to automate VLAN to ISID mapping.</p> <p>At the aggregation layer L3 default gateway routing based on VRRP or RSMLT is used.</p>
--	---

To migrate a traditional Edge Switch to a Fabric edge switch, follow these best practices:

	<ol style="list-style-type: none"> <li>1. Enable DVR controller on the Aggregation Layer switches and enable DVR-VRRP interop mode on the switch.</li> <li>2. Introduce the new VSP Edge switches as DVR leafs.</li> <li>3. For VLAN/ISIDs where no Multicast is in use, migrate users to the new VSP edge switches</li> <li>4. For VLAN/ISIDs where Multicast routing is required, convert ISID to DVR routed with IP multicast routing enabled prior to migrating users to the VSP edge switches, then migrate users.</li> <li>5. Optionally: Convert all ISIDs to DVR enabled routing where ISIDs are stretched beyond the aggregation layer pair to optimize traffic forwarding and avoid traffic tromboning.</li> </ol>
--	--

## Migrating from a Fabric Edge ERS Switch

Here is a high level description of how to migrate to a VSP Fabric Edge (DVR) solution from a Fabric Edge ERS Switch.

	<p>Migration begins with a (stacked) Edge switch setup that has a fabric dual-homing connection back to two fabric switches.</p> <p>A VLAN, such as VLAN 10, is extended from the aggregation layer / MDF nodes to the access switches.</p> <p>Additionally, for IP Multicast, the edge switches perform a L3 IP Multicast routing function.</p> <p>At the aggregation layer, L3 default gateway routing based on VRRP is used.</p>
--	---

To migrate an ERS Fabric Edge Switch to a VOSS Fabric edge switch, follow these best practices:

	<ol style="list-style-type: none"> <li>1. Enable the DVR controller on the Aggregation Layer switches with DVR-VRRP interop mode enabled on the switch.</li> <li>2. Introduce the new VSP Edge switches as DVR-leafs.</li> <li>3. For VLAN/ISIDs where no Multicast is in use, migrate users to the new VSP edge switches, still using VRRP as the default GW protocol.</li> <li>4. For VLAN/ISIDs where Multicast routing is required, migrate clients to <u>NEW</u> VLANs/ISIDs on the VSP edge, that have DVR with IP Multicast enabled.</li> <li>5. Remove the ERS switches after all users are migrated.</li> <li>6. Optionally: Convert all ISIDs to DVR enabled routing, where ISIDs are stretched beyond the aggregation layer pair to optimize traffic forwarding and avoid traffic tromboning.</li> </ol>
--	---



# Appendix A: Acronyms

---

**BVID**

Backbone VLAN ID

**DVR**

Distributed Virtual Routing

**EAP**

802.1X Extensible Authentication Protocol for end-system authentication

**ERS**

Extreme Ethernet Routing Switch supporting Fabric Connect

**EXOS**

Extreme Summit Switch supporting Fabric Attach

**FA**

Fabric Attach

**IDF**

Intermediate Distribution Frame

**ISID**

I-component Service Identifier per IEEE 802.1ah.

**IS-IS**

Intermediate Systems to Intermediate Systems Protocol established at IETF in 1990 as rfc1142.

**MDF**

Main Distribution Frame

**MLAG**

Multi-Chassis Link Aggregation

**Multi-Area**

Interconnection of multiple IS-IS areas through multi-area boundary nodes.

**NAC**

Network Access Control

**NEAP- non-EAP**

MAC based end-system authentication

**Nick-name Server**

Function to automatically distribute SPB Nick-names to other devices

**NNI**

Network to Network Interface.

**SLPP**

Simple Loop Prevention Protocol

**SMLT**

Split Multi-Link Trunking

**SPB**

Shortest Path Bridging: IEEE 802.1aq/ IEEE 802.1Q-2018.

**UNI**

User to Network Interface.

**VRF**

Virtual Route Forwarder

**VSA**

Vendor Specific (Radius) Attributes

**VSP**

Extreme Virtual Switching Platform supporting Fabric Connect

**ZTF**

Zero Touch Fabric for SPB deployments

**ZTP+**

Zero Touch Provisioning with automated XMC/XIQ-SE onboarding



# Index

---

## A

announcements 6

## C

conventions  
notice icons 4  
text 4

## D

documentation  
feedback 7  
location 5

## F

feedback 7

## N

notices 4

## P

product announcements 6

## S

support, *see* technical support

## T

technical support  
contacting 6

## W

warnings 4