Migrate Ethernet Routing Switch to Universal Hardware Fabric Engine Edge Solution

9037362-00 Rev AB
July 2022

Legal Notice

Extreme Networks, 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 Extreme Networks 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

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, 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 Extreme Networks trademarks, see: www.extremenetworks.com/company/legal/trademarks

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/

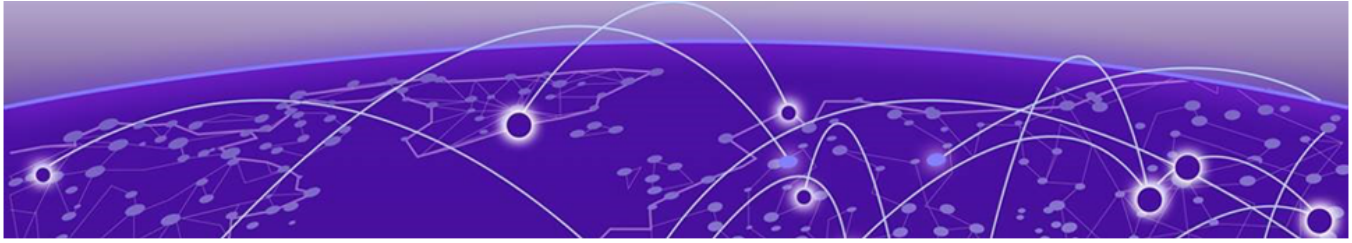

Table of Contents

Preface

This document provides configuration examples to help you replace an existing Ethernet Routing Switch device with an ExtremeSwitching universal hardware device.

Note

This document does not include information about Fabric Attach (FA) server functionality, directly attached FA client devices, or FA-proxy switches on the Extreme Networks Fabric Engine™ Edge.

For information about how to install universal hardware and select an initial operating system, see the following documents:

- *ExtremeSwitching 5320 Series Quick Reference*
- *ExtremeSwitching 5320 Series Hardware Installation Guide*
- *ExtremeSwitching 5420 Series Quick Reference*
- *ExtremeSwitching 5420 Series Hardware Installation Guide*
- *ExtremeSwitching 5520 Series Quick Reference*
- *ExtremeSwitching 5520 Series Hardware Installation Guide*
- *ExtremeSwitching 5720 Series Quick Reference*
- *ExtremeSwitching 5720 Series Hardware Installation Guide*
- *Read Me First – Universal Hardware*

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/.

Help and Support

If you require assistance, contact Extreme Networks 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 Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks 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 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

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

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks 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 Extreme Networks 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 https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

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.

Migrate the Configuration to Fabric Engine Edge Solution

This section provides information to configure a universal hardware Fabric Engine Edge switch operating as a Fabric Connect node and to configure Shortest Bridging Path (SPB) and Intermediate System-to-Intermediate System (IS-IS).

Before you replace an existing Ethernet Routing Switch (ERS) configuration with the universal hardware Fabric Engine edge solution, consider the following key decision points:

- Will the edge switch use Network Access Control (NAC)?

  Tip
  If you use NAC then you should use Switched UNI (S-UNI) mode because it is more flexible in supporting the available RADIUS assigned attributes, which the RADIUS server can return. With NAC, RADIUS assigned attributes can automate assigning VLANs to ports, so a S-UNI configuration remains transparent.

- Will the universal hardware edge switch be deployed as a Distributed Virtual Routing (DvR) Leaf?

  Note
  A DvR Leaf supports S-UNI mode only.
  DvR support varies by product and software release. For more information, see the *Fabric Engine Feature Support Matrix* for the specific software release.

On the Fabric Engine edge, you can apply VLANs on ports in two distinct ways:

- C-VLAN-UNI Mode

  In C-VLAN-UNI mode, you create every VLAN globally on the switch and assign membership of that VLAN to ports. You can configure VLAN ports as untagged, tagged, or untagPvidOnly. For some of these settings, you must configure a default port VLAN ID (PVID) on a per port basis. You can assign a Layer 2 service I-SID VLAN to extend that same VLAN to other switches in the fabric.

  The Spanning Tree Protocol always operates on C-VLAN-UNI ports unless you disable it.

  C-VLAN-UNI mode is very similar to VLAN configuration on an ERS and presents the easiest migration option to the Fabric Engine edge solution.

- S-UNI Mode

In S-UNI mode, the ports are flex-uni enabled. You do not need to create global VLANs. Instead, configure Layer 2 I-SIDs globally and assign ports directly to the Layer 2 I-SID. If the port is to process untagged traffic, then a VLAN-ID is not required. However, if the port is to process tagged traffic, then you must specify a VLAN-ID on a per port basis.

The Spanning Tree Protocol never operates on S-UNI ports.

S-UNI Mode is more powerful than C-VLAN-UNI mode. With S-UNI, a VLAN-ID and a given port (VID, port) maps to a Layer 2 VSN I-SID. With this UNI type, VLAN-IDs can be reused on other ports and therefore mapped to different I-SIDs.

This configuration approach is significantly different from the way VLANs are configured on an ERS.

An additional consideration is the starting point of all configuration on the Fabric Engine edge switch. There are two possible factory default configurations on a Fabric Engine switch:

- The following list identifies the default configuration if you use the **`boot config flags factorydefaults`** command and reset the switch:
  - All ports are disabled by default.
  - All ports are untagged members of default VLAN 1 and are in C-VLAN-UNI mode.
  - All ports have Spanning Tree Protocol enabled.
- The following list identifies the Zero Touch Deployment-ready configuration mode:
  - All ports are enabled by default.
  - All ports are flex-uni enabled and are untagged members of the new default onboarding VLAN 4048. This VLAN is a Private-VLAN and all ports operate as Private-VLAN isolated members.
  - Auto-sense functionality is enabled by default on all ports. If you globally configure a switch with a RADIUS server and you globally enable EAPOL, all Auto-sense access ports automatically perform both EAP and NEAP when they do not detect other possible Auto-sense states. This means that if you enable NAC, port level configuration is not necessary.

    

    Note
    Zero Touch Deployment-ready configuration mode is obtained when the switch resets and the switch does not have an existing primary or secondary configuration file loaded (for example, `/intflash/config.cfg`).

  The following guidelines are suggested:

  - If the Fabric Engine edge deploys in DvR Leaf mode and/or you enable NAC on the switch:
    - Ensure the switch boots in Zero Touch Deployment-ready configuration mode so that flex-uni and Auto-sense are enabled on all access ports.
    - Configure the RADIUS server and globally enable EAPOL. Zero Touch Provisioning Plus (ZTP +) performs these actions while the switch onboards.
  - If the Fabric Engine edge switch does not deploy in DvR Leaf mode and you do not enable NAC on the switch:
    - Enable the **`boot config flags factorydefaults`** command, save the configuration, and reset the switch.

      Or

- If the switch boots in Zero Touch Deployment-ready configuration mode, before you configure a port, disable Auto-sense on that port. This disables Auto-sense on the port and flex-uni at the same time.
- Configure the VLAN membership similar to your ERS configuration. For information about VLAN configuration using C-VLAN-UNI, see CLI Command Examples on page 9 .

◦ If the Fabric Engine edge switch deploys in DvR Leaf and you do not enable NAC on the switch:

- If the switch does not boot in Zero Touch Deployment-ready configuration mode, enable flex-uni on all the access ports.
- If the switch boots in Zero Touch Deployment-ready configuration mode, disable Auto-sense on all the access ports and enable flex-uni on the same ports.
- Manually configure the VLAN membership using S-UNI. For more information about VLAN configuration using S-UNI, see CLI Command Examples on page 9.

CLI Command Examples

The following section provides the CLI commands to migrate an existing Ethernet Routing Switch (ERS) configuration to a universal hardware Fabric Engine edge solution.

Table 1: Product Migration

ERS hardware	Release tested	Universal hardware	Release tested
Ethernet Routing Switch 3600 Series	6.5.2	5320 Series	8.7
Ethernet Routing Switch 4900 Series	7.7.2	5420 Series	
Ethernet Routing Switch 5900 Series		5520 Series	

Universal Hardware Fabric Engine Edge Switch DvR Deployment

Most universal hardware Fabric Engine edge switch deployments use Distributed Virtual Routing (DvR). You must first enable the dvr-leaf-mode boot config flag and reset the switch before you can configure the DvR domain.

Note

DvR support varies by product and software release. For more information, see the *Fabric Engine Feature Support Matrix* for the specific software release.

You can configure the switch as a DvR leaf node without rebooting, as long as there is no unsupported configuration discovered on the switch.

```
configure terminal
boot config flags dvr-leaf-mode
Warning: Please carefully save your current configuration before
         enabling dvr-leaf-mode. Mgmt vlan interface will no longer be
         available without an associated i-sid. Enabling this flag will
         remove all non DVR Leaf configurations when save config is done.
Do you wish to continue ? (y/n) ? y
Warning: Please check if vrf-scaling boot flag is enabled on DVR controller.
         If so, enable it on DVR leaf also.
```

```
Warning: Please save configuration and reboot the switch
         for this to take effect.
save config
reset -y
configure terminal
dvr leaf 1
```

Fabric SPBM Configuration

The switches form a new fabric automatically, or they can connect to an existing fabric that is Auto-sense-capable. If a switch connects to an existing, Auto-sense-capable fabric, it obtains an IP address and DNS information from a DHCP server using the onboarding I-SID/VLAN. The system can then automatically onboard the switch to the management servers, for example ExtremeCloud IQ or Extreme Management Center or ExtremeCloud IQ - Site Engine, to carry out provisioning deployment of the switch.

Follow this example if you do not use Auto-sense functionality or if you statically configure Fabric parameters on the Fabric Engine edge switch.

Configure SPBM Parameters

```
configure terminal
    interface loopback 1
        ip address 192.168.1.2/32
    exit
    spbm
    router isis
       system-id 9200.7435.0000
       ip-source address 192.168.1.2
       spbm 1
       spbm 1 b-vid 4051-4052 primary 4051
       spbm 1 nick-name  9.74.35
       spbm 1 ip enable
    exit
    vlan create 4051 type spbm-bvlan
    vlan create 4052 type spbm-bvlan
    router isis enable
```

Configure NNI

```
interface gigabitethernet 1/49,1/50
       no auto-sense enable  (#If running 8.3 or later software)
       isis
       isis spbm 1
       isis enable
       no shutdown
    exit
```

VLAN Configuration using Switched UNI

Enable Flex-UNI on access ports 1/1-1/11.

```
vlan members remove 1 1/1-1/11   (#if default VLAN 1 is on the ports)
interface gigabitEthernet 1/1-1/11
   flex-uni enable
exit
```

Create Data I-SID 10, Voice I-SID 20, and Wireless I-SID 30 and add untagged port members to each I-SID.

```
i-sid 10
   untagged-traffic port 1/1-1/4
exit
i-sid name 10 DATA

i-sid 20
   untagged-traffic port 1/5-1/8
exit
i-sid name 10 VOICE

i-sid 30
   untagged-traffic port 1/9-1/11
exit
i-sid name 10 WIRELESS
```

VLAN Configuration using C-VLAN-UNI

In a non-DvR universal hardware Fabric Engine edge switch deployment, you can deploy a mix of Switched UNI (S-UNI) and traditional Customer VLAN (C-VLAN) UNIs. The following example shows a C-VLAN UNI deployment.

Create VLANs, map to I-SIDs, and add port members.

```
configure terminal
vlan create 10 name DATA type port-mstprstp 0
vlan create 20 name VOICE type port-mstprstp 0
vlan create 30 name WIRELESS type port-mstprstp 0
vlan i-sid 10 10
vlan i-sid 20 20
vlan i-sid 30 30
vlan member add 10 1/1-1/4
vlan member add 20 1/5-1/8
vlan member add 30 1/9-1/11
ssh
```

Nodal Management Configuration

Configure the management interface circuitless IP (CLIP) address.

```

mgmt clip
ip address 192.168.1.1/32
enable
exit
```

SNMPv3

```
snmp-server user snmpuser group initial md5 des
    Enter the authentication protocol password : ************
    Re-enter the authentication protocol password : ************
    Enter the privacy protocol password : ************
    Re-enter the privacy protocol password : ************
    snmp-server view snmpview 1.3
```

SSH

```
boot config flags sshd
    ssh
```

System Identification

```
snmp-server name Wire-Closet-Floor1-Switch1
    snmp-server location HQ-Building
    snmp-server contact ACME-ABC
```

DNS

```
ip name-server primary 8.8.8.8
```

Change rwa CLI Password

```
cli password rwa read-write #This command prompts you to provide the
    original rwa password and to configure and confirm the new password.
```

Load License File

```
load-license <file name>
```

ERS Filter Configuration

You can use one of the following syntax examples to configure Ethernet Routing Switch (ERS) QoS filters. All examples perform the same filtering and both a security filter and a QoS remarking filter examples are provided.

ERS Original QoS Policy Filter Example

The following syntax is powerful but complicated.

```
! Security filter example
qos if-group name TaggedLinks class trusted
qos if-assign port 25-26 name TaggedLinks
qos l2-element 1 name VLAN100 vlan-min 100 vlan-max 100 ethertype 0x800
qos ip-element 101 name "10.31.64.0/25" dst-ip 10.31.64.0/25
qos ip-element 102 name "172.16.2.0/24" dst-ip 172.16.2.0/24
qos classifier 1001 set-id 1001 name "Mgmt1" element-type ip element-id 101
qos classifier 1002 set-id 1001 name "Mgmt1" element-type l2 element-id 1
qos classifier 1003 set-id 1002 name "Mgmt2" element-type ip element-id 102
qos classifier 1004 set-id 1002 name "Mgmt2" element-type l2 element-id 1
qos classifier-block 10001 block-number 10001 name "DenyBlock1" set-id 1001 in-profile-
action 1 eval-order 1
qos classifier-block 10002 block-number 10001 name "DenyBlock1" set-id 1002 in-profile-
action 1 eval-order 1
qos policy 101 name "DenyBlock1" if-group TaggedLinks clfr-type block clfr-id 10001
precedence 14
! QoS remarking filter example
qos l2-element 2 name VLAN200 vlan-min 200 vlan-max 200 ethertype 0x800
qos ip-element 201 name "Qos-Remark-UDP" protocol 17 dst-port-min 2000 dst-port-max 2000
qos ip-element 202 name "Qos-Remark-TCP" protocol 6 dst-port-min 2000 dst-port-max 2000
```

```
qos classifier 2001 set-id 2001 name "QosUDP" element-type ip element-id 201
qos classifier 2002 set-id 2001 name "QosUDP" element-type l2 element-id 2
qos classifier 2003 set-id 2002 name "QosTCP" element-type ip element-id 202
qos classifier 2004 set-id 2002 name "QosTCP" element-type l2 element-id 2
qos classifier-block 20001 block-number 20001 name "QoSBlock1" set-id 2001 in-profile-
action 7 eval-order 1
qos classifier-block 20002 block-number 20001 name "QoSBlock1" set-id 2002 in-profile-
action 7 eval-order 1
qos policy 201 name "QoSBlock1" port 1-24 clfr-type block clfr-id 20001 precedence 13
```

ERS Interim ACL Syntax Example

The following syntax has many limitations.

```
! Security filter example
qos ip-acl name "Deny-10.31.64.0" dst-ip 10.31.64.0/25 drop-action enable
qos ip-acl name "Deny-172.16.2.0" dst-ip 172.16.2.0/24 drop-action enable
qos acl-assign port 25-26 acl-type l2 name "VLAN-100"
qos acl-assign port 25-26 acl-type ip name "Deny-10.31.64.0"
qos acl-assign port 25-26 acl-type ip name "Deny-172.16.2.0"

! QoS remarking filter example
qos ip-acl name "QoSUDP" protocol 17 dst-port-min 2000 dst-port-max 2000 update-dscp 46
update-1p 6
qos ip-acl name "QoSTCP" protocol 6 dst-port-min 2000 dst-port-max 2000 update-dscp 46
update-1p 6
qos acl-assign port 25-26 acl-type ip name "QoSUDP"
qos acl-assign port 25-26 acl-type ip name "QoSTCP"
```

ERS Final QoS Traffic Profile Syntax Example

The following syntax is compact and powerful.

```
! Security filter example
qos traffic-profile classifier name "DenyNets" dst-ip 10.31.64.0/25 vlan-min 100 vlan-max
100 ethertype 0x800 drop-action enable block A
qos traffic-profile classifier name "DenyNets" dst-ip 172.16.2.0/25 vlan-min 100 vlan-max
100 ethertype 0x800 drop-action enable block A
qos traffic-profile set port 25-26 name DenyNets

! QoS remarking filter example
qos traffic-profile classifier name "QoS-Remark" protocol 17 dst-port-min 2000 dst-port-
max 2000 vlan-min 200 vlan-max 200 ethertype 0x800 update-dscp 46 update-1p 6 block A
qos traffic-profile classifier name "QoS-Remark" protocol 6 dst-port-min 2000 dst-port-
max 2000 vlan-min 200 vlan-max 200 ethertype 0x800 update-dscp 46 update-1p 6 block A
qos traffic-profile set port 1-24 name QoS-Remark
```

ERS ACL filter examples translates on Fabric Engine into the following CLI configurations, which are more intuitive than the preceding ERS syntax examples.

Fabric Engine Filter Configuration

You can use one of the following syntax examples to configure Fabric Engine QoS filters.

On a DvR Leaf, you must use an InVsn ACL.

```
filter acl 1 type inVsn matchType uniOnly name "DenyNets"
filter acl i-sid 1 2000100
filter acl ace 1 1 name "Deny-10.31.64.0"
```

```
filter acl ace action 1 1 deny
filter acl ace ethernet 1 1 ether-type eq ip
filter acl ace ip 1 1 dst-ip mask 10.31.64.0 25
filter acl ace 1 1 enable
filter acl ace 1 2 name "Deny-172.16.2.0"
filter acl ace action 1 2 deny
filter acl ace ethernet 1 2 ether-type eq ip
filter acl ace ip 1 2 dst-ip mask 172.16.2.0 24
filter acl ace 1 2 enable
filter acl 2 type inVsn matchType uniOnly name "QoS-Remark"
filter acl i-sid 2 2000200
filter acl ace 2 1001 name "QoS-Remark-UDP"
filter acl ace action 2 1001 permit internal-qos 6 remark-dot1p 6 remark-dscp phbef
filter acl ace ethernet 2 1001 ether-type eq ip
filter acl ace ip 2 1001 ip-protocol-type eq udp
filter acl ace protocol 2 1001 dst-port eq 2000
filter acl ace 2 1001 enable
filter acl ace 2 1002 name "QoS-Remark-TCP"
filter acl ace action 2 1002 permit internal-qos 6 remark-dot1p 6 remark-dscp phbef
filter acl ace ethernet 2 1002 ether-type eq ip
filter acl ace ip 2 1002 ip-protocol-type eq tcp
filter acl ace protocol 2 1002 dst-port eq 2000
filter acl ace 2 1002 enable
```

You can also use the InVsn syntax shown in the preceding example on a non-DvR Leaf regular Fabric Engine Backbone Edge Bridge (BEB) switch. However, on a regular Fabric Engine BEB switch, you can also use the inVlan type.

```
filter acl 1 type inVlan name "Securit+QoS"
filter acl vlan 1 100
filter acl ace          1 1 name "Deny-10.31.64.0"
filter acl ace action   1 1 deny
filter acl ace ethernet 1 1 ether-type eq ip
filter acl ace ip       1 1 dst-ip mask 10.31.64.0 25
filter acl ace          1 1 enable
filter acl ace          1 2 name "Deny-172.16.2.0"
filter acl ace action   1 2 deny
filter acl ace ethernet 1 2 ether-type eq ip
filter acl ace ip       1 2 dst-ip mask 172.16.2.0 24
filter acl ace          1 2 enable
filter acl ace          1 101 name "QoS-Remark-UDP"
filter acl ace action   1 101 permit internal-qos 6 remark-dot1p 6 remark-dscp phbef
filter acl ace ethernet 1 101 ether-type eq ip
filter acl ace ip       1 101 ip-protocol-type eq udp
filter acl ace protocol 1 101 dst-port eq 2000
filter acl ace          1 101 enable
filter acl ace          1 102 name "QoS-Remark-TCP"
filter acl ace action   1 102 permit internal-qos 6 remark-dot1p 6 remark-dscp phbef
filter acl ace ethernet 1 102 ether-type eq ip
filter acl ace ip       1 102 ip-protocol-type eq tcp
filter acl ace protocol 1 102 dst-port eq 2000
filter acl ace          1 102 enable
```

ACL ACE rules can be defined as:

- Primary Bank: ACE ID range 1-1000
- Secondary Bank: ACE ID range 1001-2000

You can use both Primary and Secondary Banks for Security and QoS ACEs. The switch performs a parallel search on both ACE lists. If actions do not conflict, both actions apply. If actions conflict, the action from the Primary Bank has precedence.

ACL types inPort and outPort are also available but are not shown in the preceding examples.