ExtremeSwitching™

Configuring Fabric Attach on Ethernet Routing Switch 3600 Series

Release 6.3
9035808 Rev AA
August 2019

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, please 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: www.extremenetworks.com/support/policies/software-licensing

Contents

Chapter 1: About this Document

This section discusses the purpose of this document, the conventions used, ways to provide feedback, additional help, and information regarding other Extreme Networks publications.

Purpose

This document provides instructions to configure Fabric Attach on the switch.

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that can be used throughout this document.

Table 1: Notice Icons

Icon	Alerts you to...
❗ **Important:**	A situation that can cause serious inconvenience.
✳ **Note:**	Important features or instructions.
➕ **Tip:**	Helpful tips and notices for using the product.
⚠ **Danger:**	Situations that will result in severe bodily injury; up to and including death.
⚠ **Warning:**	Risk of severe personal injury or critical loss of data.
⚠ **Caution:**	Risk of personal injury, system damage, or loss of data.

Table 2: Text Conventions

Convention	Description
Angle brackets (< >)	Angle brackets (< >) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. If the command syntax is `cfm maintenance-domain maintenance-level <0-7>` , you can enter `cfm maintenance-domain maintenance-level 4`.
Bold text	Bold text indicates the GUI object name you must act upon. Examples: • Click **OK**. • On the **Tools** menu, choose **Options**.
Braces ({ })	Braces ({ }) indicate required elements in syntax descriptions. Do not type the braces when you enter the command. For example, if the command syntax is `ip address {A.B.C.D}`, you must enter the IP address in dotted, decimal notation.
Brackets ([ ])	Brackets ([ ]) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command. For example, if the command syntax is `show clock [detail]`, you can enter either `show clock` or `show clock detail`.
Ellipses (…)	An ellipsis (…) indicates that you repeat the last element of the command as needed. For example, if the command syntax is `ethernet/2/1 [ <parameter> <value> ]...,` you enter `ethernet/2/1` and as many parameter-value pairs as you need.
Italic Text	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 that are not active links.
`Plain Courier Text`	Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages.

Table continues…

Convention	Description
	Examples: • `show ip route` • `Error: Invalid command syntax [Failed][2013-03-22 13:37:03.303 -04:00]`
Separator (>)	A greater than sign (>) shows separation in menu paths. For example, in the Navigation tree, expand the **Configuration** > **Edit** folders.
Vertical Line (|)	A vertical line (|) separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command. For example, if the command syntax is `access-policy by-mac action { allow | deny }`, you enter either `access-policy by-mac action allow` or `access-policy by-mac action deny`, but not both.

Documentation and Training

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

Getting Help

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: 1-800-998-2408 (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 and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) 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

Subscribing to Service Notifications

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

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form with your information (all fields are required).
3. Select the products for which you would like to receive notifications.

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

4. Click **Submit**.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please 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.

Chapter 2: New in this document

The following sections detail what is new in this document.

Trusted FA Client

The Trusted FA Client support allows I-SID/VLAN binding requests received from a FA Client to be selectively processed on secure ports (for example, ports under EAP/NEAP control). Previously, FA Client binding requests were ignored on secure ports.

For more information, see EAP and FA on page 25.

Chapter 3: Fabric Attach (FA)

Use the information in this chapter to help you understand Fabric Attach (FA), and how to configure and use Fabric Attach using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

This chapter includes the following sections:

- Fabric Attach Fundamentals
- Fabric Attach configuration using CLI
- Fabric Attach configuration using EDM

Fabric Attach Fundamentals

Fabric Attach (FA) extends the fabric edge to devices that do not support Shortest Path Bridging MAC (SPBM). With FA, non-SPBM devices can take advantage of full SPBM support, when support is available.

FA also decreases the configuration requirements on SPBM devices by off-loading some configuration to the attached non-SPBM devices and by automating certain configuration steps that occur most often.

FA Signaling

The FA elements communicate between themselves using FA Signaling. FA Signaling is an application level protocol that leverages standard network protocols, such as LLDP, to exchange messages and data between FA elements to orchestrate network automation.

FA Network Elements

The FA architecture involves the following FA elements:

- FA Server—An SPB capable network device connected to the fabric edge running the FA agent in FA Server mode. FA Servers receive requests to create services with specific I-SID/VLAN bindings.

  In the SPBM architecture an FA Server is a BEB. FA servers process requests for service creation from FA Proxy and/or FA Clients. An FA Server can operate in SPBM or VLAN provisioning mode.
- FA Proxy—A device running the FA agent in FA Proxy mode.

  An FA Proxy device may be capable of running SPB or not. SPB is always disabled on devices running FA Proxy. FA Proxy mode is enabled by default on devices supporting this mode.

FA Proxies support I-SID/VLAN assignment definition and have the ability to advertise these assignments for possible use by an FA Server, if connectivity permits.

- FA Client—A non-SPB network attached device running the FA agent in FA Client mode and able to advertise ISID/VLAN binding requests for service creation to an FA Proxy or FA Server. Non-FA clients without an FA agent are supported through the FA EAP support.
- FA Standalone Proxy–An FA device running the FA agent in FA Standalone Proxy mode. FA Standalone Proxy supports FA Proxy functionality in environments without an FA Server.

  An FA Standalone Proxy can be used to automate the configuration of traditional VLANs for devices connected to it, such as WLAN Access Points.

  The FA Standalone Proxy does not send provisioning requests upstream. An FA Standalone Proxy automatically accepts requests from FA clients and assumes that the upstream network has been provisioned appropriately.

  FA Standalone Proxy can be used in environments where the devices upstream from the FA Standalone Proxy do not support Fabric Attach, but the devices downstream from it support Fabric Attach.

FA Server, FA Proxy and FA Standalone Proxy devices use FA signaling in conjunction with Extreme Networks Identity Engines in order to automate configuration of services.

FA Element Discovery

An FA agent which controls FA functionality resides on all FA-capable devices (FA Server, FA Proxy, FA Standalone Proxy or FA Client). No agent-specific configuration is necessary.

FA Proxy and FA Server elements control FA through a global FA service setting (global SPBM setting) and through per-port settings that control the transmission of FA information using FA Signaling.

The first stage of establishing FA connectivity involves element discovery. In order for FA discovery to function, FA service and per-port settings must be enabled. Once these settings are enabled, the FA agent advertises its capabilities (FA Server, FA Proxy or FA Client) through FA Signaling. Following discovery, an FA agent is aware of all FA services currently provided by the network elements to which it is directly connected. Based on this information, an FA Client or an FA Proxy agent can determine whether FA data (I-SID/VLAN assignments) should be exported to an FA Proxy that acts as an external client proxy or an FA Server.

The FA service is enabled by default on FA Servers and FA Proxies. It is disabled by default on FA Standalone Proxy-only devices. Per-port settings are, by default, enabled on FA Proxies and disabled on FA Servers.

Port VLAN tagging mode updates occur when an element is discovered, provided that base zero-touch functionality is enabled. When an element is deleted or expires, all updated settings are cleared and roll back to their previous values.

Note:

An FA Proxy can communicate with, at most, one FA Server at a time. If multiple server connections exist, the first discovered server is considered the primary server. Multiple links (trunked) to a single server are supported as long as they form a logical interface. Multiple non-trunked links are not supported and data received on non-primary ports is ignored by an FA Proxy. FA Proxies or FA Clients can connect through a LAG/MLT to two FA Servers which form a Split-LAG or SMLT pair. Connections which may create loops, to multiple servers that are not in Split-LAG or SMLT mode, are not supported.

An FA Server can communicate with multiple, different FA Proxies and FA Clients.

FA Agent Startup and Initialization

During the FA agent startup and initialization sequence, the following are restored from non-volatile memory:

- FA service status
- FA port-level settings
- external client proxy status
- message authentication status and keys for all ports
- previously configured I-SID/VLAN assignments
- Auto Provision status
- Zero Touch settings
- FA Standalone Proxy settings
- extended logging support

In a stack environment, FA agent startup and initialization occurs on every unit in the stack, using the data restored from non-volatile memory.

The initialization sequence can also include operations geared towards cleaning-up settings that were previously configured in support of FA I-SID/VLAN assignments that were active on an FA Proxy or an FA Server before a system reset.

Note:

After a reboot the switch does not retain configurations (such as DHCP Snooping, ARP Inspection, IP Source Guard) you apply on a dynamic VLAN created by the FA agent.

FA Proxy I-SID-to-VLAN Assignment

Although administrators may configure I-SID-to-VLAN bindings on FA Proxies, I-SID-to-VLAN bindings are typically received by FA Proxies from FA Clients. If external client proxy support is enabled, standard processing requirements for bindings received from an FA Client are managed the same way that processing requirements for locally configured bindings are managed.

Each I-SID/VLAN association that is configured on an FA Proxy creates a Customer VLAN (C-VLAN) User-Network Interface (UNI), once the assignment becomes active following acceptance by an FA Server.

Note:

FA Proxy devices only support C-VLAN UNIs and don’t support switched UNIs.

If an I-SID-to-VLAN assignment is accepted by the FA Server, the assignment state is updated to *active*. If an I-SID-to-VLAN assignment is not accepted by the FA Server, the assignment state is updated to *rejected*.

The FA Proxy receives and displays assignment status information from the FA Server for each pending I-SID-to-VLAN assignment. Possible responses include:

- Assignment accepted (2)
- Rejection: generic (3)
- Rejection: Fabric Attach resources unavailable (4)
- Rejection: VLAN invalid (6)
- Rejection: VLAN resources unavailable (8)
- Rejection: application interaction issue (9)

Note:

Data exchanges (I-SID/VLAN assignments) between an FA Proxy and an FA Server/FA Client are supported, as are exchanges between an FA Server and an FA Proxy/FA Client. FA Proxy to FA Proxy and FA Server to FA Server interactions are not supported.

If the FA Proxy or FA Client has access to an FA Server, these assignments are advertised for possible use by the FA Server, using FA signaling.

All I-SID/VLAN assignments defined on an FA Proxy, as well as those received from FA Clients when client proxy operation is enabled, start in the ‘pending’ state. The I-SID/VLAN assignment state is updated based on feedback received from the FA Server. If an assignment is accepted by the FA Server, its state is updated to ‘active’. A server can also reject proposed I-SID/VLAN assignments. In this case, the assignment state is updated to ‘rejected’. Data describing the reason for the rejection may also be available.

FA Data Processing

Following discovery, an FA Proxy or FA Client transmits locally-defined I-SID/VLAN assignments through FA Signaling to an FA Server, which accepts or rejects these assignments.

The I-SID/VLAN assignment acceptance by the server can require actions to be performed by the FA agent on both the FA Proxy and the FA Server, to appropriately configure the communication channel (uplink) between the FA Proxy or FA Client and FA Server. Most actions undertaken based on assignment acceptance are undone when the I-SID/VLAN assignment is no longer needed.

I-SID/VLAN assignment rejection by the FA Server requires the FA Proxy to clean up any settings that the FA agent made related to feature operation, as well as log the rejection and any associated error type information for later analysis by an administrator. The amount of clean-up required depends on whether the port VLAN membership was established by the FA Proxy agent or by the administrator outside of the FA feature operation. An uplink port that is associated with a VLAN because of an accepted FA Proxy I-SID/VLAN assignment, and not because of an explicit administrator port VLAN membership action, will have the port VLAN membership cleared when the related I-SID/VLAN assignment is rejected by the FA Server or deleted by the FA Proxy administrator.

VLANs that are automatically created on an FA Proxy due to I-SID/VLAN assignment acceptance are automatically deleted when bindings are rejected or deleted.

No more than a single log message is generated for a rejected I-SID/VLAN assignment, regardless of how many times the assignments have been requested and rejected. Assignments that are rejected, accepted, and later rejected result in a log message being generated for each “new” rejection (two I-SID/VLAN assignment rejection log messages are generated in this case).

FA Proxy I-SID/VLAN assignment addition actions:

- Create port-based VLAN corresponding to I-SID/VLAN assignment VLAN.
- Update port VLAN membership to include I-SID/VLAN assignment VLAN.

FA Server I-SID/VLAN assignment addition actions:

- Create SPBM switched UNI VLAN corresponding to I-SID/VLAN assignment VLAN.
    - C-VLAN join operation does not initiate VLAN creation (VLAN already exists and is associated with the I-SID/VLAN binding I-SID).
- Update I-SID/VLAN mapping data to ensure Shortest Path Bridging-MAC (SPBM)-switched UNI support is enabled for the I-SID/VLAN/port tuple (in other words, create switched UNI). Port VLAN membership is updated by this action.

Additional actions can be required for I-SID/VLAN binding state transitions involving FA Client-generated data. The communication channel (that is, the downlink) between the FA Client and FA Proxy must be appropriately configured. This can require actions to be performed on the switch.

FA Proxy external client proxy I-SID/VLAN assignment addition actions:

- Update downlink port VLAN membership to include I-SID/VLAN assignment VLAN.

Each of these actions is performed by the FA Proxy and FA Server for each I-SID/VLAN assignment, unless the required data/settings have already been configured by the administrator. The successful transition from ‘pending’ to ‘active’ is gated by the successful completion of these actions. The FA agent tracks which settings have been updated based on I-SID/VLAN assignment processing (comparing them with settings established by the administrator), and cleans-up or undoes the settings that are related to I-SID/VLAN assignment support as much as possible when an assignment is no longer needed.

I-SID/VLAN assignment state transitions from ‘active’ to ‘rejected’ require complementary actions be performed by the FA Proxy and the FA Server to eliminate assignment-related settings:

FA Proxy I-SID/VLAN assignment deletion actions:

- Update uplink port VLAN membership to exclude I-SID/VLAN assignment VLAN.

- Delete port-based VLAN corresponding to I-SID/VLAN assignment VLAN.

FA Server I-SID/VLAN assignment deletion actions:

- Delete I-SID/VLAN/port association data to disable SPBM-switched UNI support for the I- SID/ VLAN/port tuple (to delete switched UNI). This action updates port VLAN membership.
- Delete SPBM-switched UNI VLAN corresponding to I-SID/VLAN assignment VLAN.
    - Previously joined C-VLANs are not deleted.

State transitions related to FA Client-generated bindings require additional complementary actions to be performed by the FA Proxy to eliminate assignment-related settings:

FA Proxy external client proxy I-SID/VLAN assignment deletion actions:

- Update downlink port VLAN membership to exclude I-SID/VLAN assignment VLAN.
- Delete port-based VLAN corresponding to I-SID/VLAN assignment VLAN.

Assignment status data returned by the FA Server for each pending I-SID/VLAN assignment drives the FA Proxy response processing. Assignment rejections can include information to indicate the reason for the rejection.

Rejection error codes include:

- FA resources unavailable(4)–the resources that are required for the FA agent to support additional I-SID/VLAN assignments are currently exhausted. The maximum number of assignments that can be supported has been reached.
- VLAN invalid(6)–the specified VLAN can’t be used to create a switched UNI at this time. The VLAN already exists and is either inactive or has an incorrect type for this application. This error is also returned if an FA Client or FA Proxy exports an bindings with an I-SID value of 0 and SPBM provisioning is enabled.
- VLAN resources unavailable(8)–the maximum number of VLANs that can be supported by the device has been reached.
- Application interaction issue(9)–a failure has been detected during FA interactions with the VLAN and/or the SPBM applications. The VLAN operations to create the required SPBM switched UNI VLAN or enable port tagging may have failed or the SPBM operation to create the switched UNI may have failed.

As with the actions initiated to support an assignment addition, actions related to assignment deletion are performed only if the targeted data was created during the I-SID/VLAN assignment addition phase. Previously-existing configuration data is not changed. No artifacts are left behind to indicate that automated operations have taken place, following an addition or deletion sequence. This goal may not always be achievable but all attempts are made to satisfy this requirement.

In addition to explicit I-SID/VLAN assignment state transitions, several events can occur that initiate assignment deletion processing. These include:

- I-SID/VLAN assignment timeout–A “last updated” timestamp is associated with all active assignments on the FA Server. When this value is not updated for a predetermined amount of time, the I-SID/VLAN assignment is considered obsolete. Obsolete assignment data and related settings are removed by the FA server agent. The timeout duration value allows FA Server settings to be maintained if temporary connectivity issues are encountered.

I-SID/VLAN binding timeout is also performed by an FA Proxy when it is providing client proxy services and FA Client data is present. Processing similar to that performed by the FA Server related to data aging is supported.

- I-SID/VLAN assignment list updates–The current I-SID/VLAN assignment list is advertised by an FA Proxy at regular intervals (dictated by FA Signaling). During processing of this data, an FA Server must handle list updates and delete assignments from previous advertisements that are no longer present. Though these entries would be processed appropriately when they timeout, the FA agent attempts to update the data in real-time and initiates deletion immediately upon detection of this condition.
- FA Server inactivity timeout–If primary FA Server advertisements are not received for a predetermined amount of time, the I-SID/VLAN assignments accepted by the server are considered rejected. I-SID/VLAN assignment data is defaulted (reverts to the ‘pending’ state) and related settings are removed by the FA Proxy agent. The timeout duration value has been chosen to allow FA Proxy settings to be maintained if temporary connectivity issues are encountered.

You can configure the timeout value used for FA device or binding aging with the **`fa timeout`** command. The default value is 240 seconds.

FA Proxy and FA Server Connection Maintenance

An FA Proxy can only interact with one FA Server at a time. If multiple server connections exist, the first discovered server is considered the primary server. All other servers discovered after this point in time are considered alternates. Typically only a single FA Server is discovered. If multiple servers are discovered, an indication is logged to identify this situation in case it is not intended. I-SID/VLAN assignment data is only exchanged between the FA Proxy and the primary FA Server.

When using LACP for uplink/downlink trunk, ports should be aggregated into a trunk and the LACP key should explicitly be associated with a MLT ID through the LACP Key/MLT ID mapping table.

Primary server failure is detected using a capabilities advertisement timeout. Once a predefined period of time without an FA Server advertisement from the current primary server expires, the primary server becomes undefined. Any FA Proxy I-SID/VLAN assignments previously accepted by the server are defaulted (reset to the ‘pending’ state) and related settings are cleared. An informational message (primary server lost) is logged when this transition occurs. I-SID/VLAN assignment data is not advertised until a new primary FA Server is selected. The same algorithm used at startup to select an initial primary server is used to select a new primary server.

FA Proxy/FA Server connectivity using Multi-link Trunking (MLT), Distributed Multi-Link Trunking (DMLT) or Split Multi-Link Trunking (SMLT) connections is supported.

Multiple links associated with the same trunk are treated as a single logical connection. The FA agent reconciles any issues related to MLT, DMLT and SMLT server connectivity and recognizes server uniqueness in the presence of (potentially) multiple capabilities advertisements (that is, FA Signaling received on multiple ports generated by the same server).

In MLT, DMLT and SMLT environments, FA Signaling is generated and received on all links connecting the FA Proxy and FA Server. An FA Proxy receiving an FA Server advertisement determines if a primary FA Server has been selected. If not, the FA Element System ID associated with an advertising FA Server is saved and primary server selection is completed. Once a primary server has been selected, system ID data associated with FA Server advertisements received on other ports is compared against the primary server data. If the system ID values are not the same, an error indication is logged. In all cases, the FA Proxy only generates FA Signaling containing I-SID/VLAN assignment data on the interfaces associated with the primary FA Server.

Note:

The FA Element System ID is structured such that the same system ID is generated on all links associated with a trunk connection between an FA Proxy and an FA Server even in an SMLT scenario where different physical devices are acting as a single logical entity.

In an SMLT environment, an FA Server takes additional actions to ensure that data is synchronized on both SMLT aggregation peers. In this configuration, the FA Server that receives and accepts advertised FA I-SID/VLAN assignments is responsible for generating messages that are sent across the Inter-Switch Trunk (IST) to inform the partner aggregation switch about FA settings that have been configured (for example, SPBM switched UNI VLAN). Similar actions are required when I-SID/VLAN assignments are deactivated.

Agent Stacking functionality

The FA agent is able to function in both standalone and stacked configurations. In a stack, the base unit FA agent acts as the master and pushes its configuration settings to all non-base units (NBUs), to synchronize data across all units. FA agents are active on all units and are able to process stack events as well as data distribution messages.

On an FA Proxy, connections to the primary FA Server can exist on any unit in the stack. When the unit with the active FA Proxy-to-FA primary server interface leaves the stack, any I-SID-to-VLAN assignments accepted by the server are aged-out. I-SID-to-VLAN assignment data is restored to the default *pending* state and related settings are removed by the FA Proxy agent.

The presence of multiple FA Server connections (for example, DMLT FA Proxy - Server connection) is taken into account when determining if FA Server connectivity has been lost.

FA Message Authentication and Integrity Protection

In order to secure the FA communication in terms of data integrity and authenticity, a keyed-hash message authentication code transmitted with FA TLV data is used to protect all FA signaling exchanges. The standard HMAC-SHA256 algorithm is used to calculate the message authentication code (digest) involving a cryptographic hash function (SHA-256) in combination with a shared secret key. The key is symmetric (known by both source and destination parties). By default, FA message authentication is enabled and a default key is defined to provide secure communication out-of-the-box.

You can configure message authentication status and authentication keys on a per-port basis.

When FA message authentication is enabled, the FA key (default or configured) is used to generate a Hash-based Message Authentication Code (HMAC) digest that is included in all FA TLVs (the FA Element TLV and the FA I-SID/VLAN Assignment TLV).. Upon receipt, the HMAC digest is recomputed for the TLV data and compared against the digest included in the TLV. If the digests are the same, the data is valid. If not, the data is considered invalid and is ignored.

The FA secure communication setting (enabled/disabled) and the symmetric key data are maintained across resets and restored during FA initialization.

Multiple authentication key support provides support for authentication using multiple keys, a user-defined key and a default key. Key usage can be restricted. Only the user-defined key (strict key-mode) or both the user-defined key followed if necessary by the default key (standard key-mode) can be used for authenticating messages. By default, only the user-defined key (strict key-mode) is used for authentication.

Message authentication status, authentication key and key-mode settings are maintained on a per-port basis.

Information related to authentication failures is passed to the EAP/NEAP agent for forwarding to a FA policy server for potential processing when the following criteria are met:

- the interface on which the FA Client is discovered is EAP/NEAP enabled
- the automated FA Client Port Mode Zero Touch option is enabled for FA Client element type

FA Client ingress interface, element type, authentication status, and related key information can be provided for additional upstream client processing.

FA Clients

FA Clients connect to an FA Proxy through standard, non MAC-in-MAC access ports, advertising configured I-SID/VLAN requests to the FA Server. In this scenario, the FA Proxy acts as a client proxy for the FA Client by passing I-SID/VLAN binding requests to a discovered FA Server and returning assignment status information to the FA Client. FA Clients can connect directly to an FA Server, as well.

Note:

External client proxy support must be enabled on an FA Proxy switch before FA client data is accepted by the FA Proxy. By default, external client proxy support is enabled on an FA Proxy.

I-SID/VLAN bindings received from an FA Client by an FA Proxy acting as a proxy for external clients are processed in much the same way locally administered assignments are processed. FA Proxy response processing takes care of VLAN creation and updates VLAN membership.

If the I-SID/VLAN client assignment is rejected by the FA Server, the FA Proxy performs any required clean-up tasks and also logs the rejection and any associated error type information for later analysis by an administrator.

Note:

A user assigned to Fail Open VLAN is not removed from I-SID/VLAN bindings using MHSA mode when the RADIUS server becomes unreachable.

FA Auto Provision

You can use Auto Provision with an FA Server-capable device to take advantage of Fabric Attach functionality in non-SPB environments. Auto Provision allows an FA Proxy device (that is also FA Server-capable) to function as an FA Server when SPBM is disabled. With Auto Provision you can designate the device as an FA Proxy or FA Server.

FA VLAN definitions, configured locally on an FA Proxy or through client processing, transparently replace I-SID/VLAN binding definitions in this scenario and allow all of the automated FA processing, with the exception of switched UNI-related operations, to be performed in the absence of SPBM operations. All existing FA default settings remain unchanged.

The Auto Provision support is set to *proxy* by default on an FA Server. The global SPBM setting always overrides the Auto Provision setting, therefore FA operation in an SPBM environment is not impacted at all by Auto Provision.

An FA Server can operate in SPBM or VLAN provisioning mode. In an SPB environment, when SPBM provisioning is operational, for each VLAN associated with an accepted I-SID/VLAN assignment, the FA Server creates an SPBM switched UNI VLAN , if the VLAN does not already exist. In a non-SPB environment, when VLAN auto-provisioning is operational, the FA Server creates port-based VLANs instead of SPBM switched UNI VLANs.

Once the FA Proxy selects a primary FA Server, the FA Proxy provision mode transitions to the provisioning mode operational on the FA Server.

The current provisioning mode on an FA Server determines the range of I-SID values that are acceptable in the proposed I-SID/VLAN assignment list. When SPBM is enabled, the acceptable I-SID range is 0-16777214. When SPBM Multicast is enabled, the acceptable I-SID range is 0-15999999. When SPBM is disabled and the auto provision mode is set to *server*, the FA Server only accepts bindings with an I-SID value of 0.

FA Zero Touch

FA Zero Touch eases the configuration process on FA-capable devices by automating specific configuration tasks required for FA functionality. For situations when you prefer or require manual configuration of the settings affected by Zero Touch, feature control is provided.

Fabric Attach must be enabled in order for Zero Touch to function. You must manually configure which FA Clients to associate with a Zero Touch option that automates tasks based on FA Clients discovery.

When base Zero Touch functionality is enabled, FA Proxy and FA Client devices can acquire management VLAN data from the connected FA Server or FA Proxy and use it to facilitate manageability and network configuration. When the feature is enabled, base Zero Touch auto-attach operation extracts management VLAN data from the primary FA Server advertisements and potentially uses this data to update the in-use management VLAN. This information can be cascaded to FA Clients, as well.

If the management VLAN being replaced was originally learned by the FA Proxy from FA Element TLV data pushed by the FA Server, the port membership of the now obsolete management VLAN is migrated to the new management VLAN automatically. If there is any user intervention during this automated process (for example, the Zero Touch auto-attach status is modified or the device management VLAN is manually updated) the obsolete management VLAN data remains as is.

Base ZT auto-attach functionality must be enabled in order to support port VLAN tagging mode updates.

Base ZT auto-attach support also transitions the connection between an FA Proxy and an FA Server to *Trusted* if it doesn't already support trusted QoS traffic processing. If the uplink (FA Proxy) or downlink (FA Server) interface is not already associated with a QoS Trusted interface group, a new QoS Trusted interface group ('FaTrustedIfcs') is created if necessary, and the interface is assigned to the interface group. FA Proxy or FA Server connection termination causes the QoS interface group associations to revert to their previous setting, or the default setting if prior setting data is not available.

By default, base Zero Touch support is enabled.

In addition to base Zero Touch functionality, you can configure the following Zero Touch options on an FA device:

IP Address Source Mode Update

When this option is enabled, IP address source mode is updated on the FA Proxy device (receiver) to *DHCP-When-Needed* and initiates DHCP-based IP address acquisition if an IP address is not manually configured.

IP address source mode update only occurs during base Zero Touch processing when a new management VLAN is processed if this option is enabled.

Automated trusted FA Client connection

When this option is enabled, the FA agent examines the list of discovered FA Clients and updates the QoS interface class assignment to 'Trusted' for certain client types, if the interface is not already associated with a 'Trusted' interface class.

QoS interface class assignment data that is updated by FA when an FA Client is discovered resets to the previous QoS interface class assignment when the FA Client information expires. FA Proxy or FA Server connection termination causes the QoS interface group associations to revert to their previous settings, or to default setting if prior setting data is not available. A system reset also causes the QoS interface class assignment for FA-updated interfaces to revert to the previous setting.

All FA updates to QoS settings are dynamic, with the exception of the creation of an FA Trusted QoS interface group ('FaTrustedIfcs').

QoS interface class data is updated based on the discovery and deletion (based on aging) of the following FA Client types:

- Wireless Access Point Type 1
- Wireless Access Point Type 2
- Switch
- Router

- IP Phone
- IP Camera
- IP Video
- Security Device
- Virtual Switch
- Server Endpoint
- ONA SDN
- ONA SPB-over-IP

Automated configuration only applies to FA-enabled ports.

Automated FA Client Port Mode

When this option is enabled and FA Clients are present, the EAP settings for the interface on which the client is discovered, are automatically updated based on the FA Client type. If the FA Clients of the appropriate type are deemed no longer valid (when element aging causes the FA Client to be deleted from the discovered elements list), the EAP port settings revert to the previous state. This is applicable for FA Proxy and FA Server devices.

When EAP port mode configuration is automated using the auto-port-mode-fa-client option, FA clients can be discovered but I-SID/VLAN binding processing, if requested, is not performed by the FA agent. In this scenario, I-SID/VLAN binding processing is controlled by EAP based on information received from IDE. Therefore, if the zero touch option auto-port-mode-fa-client is enabled for the discovered FA Client type or the port has been manually EAP-enabled, the FA agent ignores I-SID/VLAN binding data received from the FA Client.

Automated configuration only applies to FA-enabled ports.

The following FA Client types are supported:

- Wireless Access Point Type 1
- Wireless Access Point Type 2
- Switch
- Router
- IP Phone
- IP Camera
- IP Video
- Security Device
- Virtual Switch
- Server Endpoint
- ONA SDN
- ONA SPB-over-IP

Note:

The auto-port-mode-fa-client option is incompatible with the Zero Touch Client auto-client-attach and auto-pvid-mode-fa-client options.

Zero Touch Client installation

Zero Touch Client (ZTC) functionality supports automatically updating port VLAN membership, the port PVID, and possibly the default port priority, based on the presence and type of discovered FA Clients. An I-SID/VLAN binding can be installed, as well.

Note:

The auto-client-attach option must be enabled before Zero Touch Client specifications can be applied (either during discovery or retroactively).

Note:

The auto-client-attach option is incompatible with both the auto-port-mode-fa-client and auto-pvid-mode-fa-client options. You cannot enable these Zero Touch options for a client type at the same time.

The following FA Client types are supported:

- Wireless Access Point Type 1
- Wireless Access Point Type 2
- Switch
- Router
- IP Phone
- IP Camera
- IP Video
- Security Device
- Virtual Switch
- Server Endpoint
- ONA SDN
- ONA SPB-over-IP

Automated PVID FA Client Port Mode

Enabling this option initiates automatic port PVID and port management VLAN membership, based on the type of discovered FA Clients. This is applicable for FA Proxy and FA Server devices. Automated configuration is only applied to FA-enabled ports.

Data updated by Automated PVID FA Client Port Mode when an FA Client is discovered resets to the previous value when the FA Client information expires.

PVID and port VLAN data are updated based on the discovery and deletion (based on aging and port events) of the following FA Client types:

- Wireless Access Point Type 1

- Wireless Access Point Type 2
- Switch
- Router
- IP Phone
- IP Camera
- IP Video
- Security Device
- Virtual Switch
- Server Endpoint
- ONA SDN
- ONA SPB-over-IP

The `auto-pvid-mode-fa-client` option does not function over EAPOL.

Note:

The `auto-port-mode-fa-client` option is incompatible with the `auto-pvid-mode-fa-client` option. You cannot enable these Zero Touch options for a client type at the same time.

Note:

The `auto-pvid-mode-fa-client` option is incompatible with with the Zero Touch Client `auto-client-attach` option. You cannot enable these Zero Touch options for a client type at the same time.

Management VLAN Advertisement Blocking

The **`fa zero-touch auto-attach`** command is augmented with the optional parameter disable-mgmt-vlan-distribution. When this parameter is not specified, management VLAN data in the FA Element TLV is included, by default. This parameter causes the management VLAN data in the FA Element TLV to be zeroed indicating to the downstream FA devices that management VLAN data is not being advertised.

Note:

The management VLAN distribution setting does not impact FA agent management VLAN processing or usage in any other way. A management VLAN can still be learned or updated based on FA Server advertisements. Management VLAN port associations can be updated through all current mechanisms, including various zero-touch operations. The Zero Touch Auto-Attach setting overrides the management VLAN distribution setting. When Zero Touch Auto-Attach is disabled, management VLAN advertisement stops regardless of the management VLAN distribution setting.

For more information, see Disabling Management VLAN Distribution on page 45.

Automatic Management VLAN Assignment

The current **auto-pvid-mode-fa-client** ZT option allows the port PVID and port VLAN membership to be updated following FA Client discovery on a per-client basis using the management VLAN. This works well for FA Clients generating a mix of tagged and untagged data with management traffic being untagged (FA Proxy port tagging mode on the FA Client link set to **untagPvidOnly**).

For FA Clients that send management traffic tagged (possibly after learning the management VLAN from the FA Proxy), a slightly different option is now supported. The new per-client ZT option **auto-mgmt-vlan-fa-client** updates the port VLAN membership with the switch management VLAN but does not update the port PVID. If **auto-mgmt-vlan-fa-client** is enabled for a specific client type and if the specified FA Client type is discovered, the management VLAN is automatically added to the FA Client port on the switch. The dynamically added management VLAN ID is automatically removed from the port when the FA Client disconnects.

Note:

The **auto-mgmt-vlan-fa-client** option is incompatible with the **auto-pvid-mode-fa-client** and the **auto-port-mode-fa-client** options, as well as with the Zero Touch Client (ZTC) auto-attach support. Attempts to enable these Zero Touch options for a specific client type at the same time are rejected.

To configure Zero Touch options, see Configuring Fabric Attach Zero Touch options on page 42.

EAP and FA

With EAP and FA, FA-capable switches or stacks can forward traffic from EAP/NEAP clients over the SPB cloud. The traffic for authenticated clients is mapped to I-SIDs received from the Extreme Networks Identity Engines RADIUS server.

You must configure the desired bindings for EAP/NEAP clients on the RADIUS server. When confirming the authentication request, the RADIUS server also sends the corresponding binding for the EAP/NEAP client.

After an EAP/NEAP client is disconnected, the switch cleans-up the binding associated with the client, if no other EAP/NEAP client on that port uses it.

When an EAP/NEAP client successfully authenticates on an FA Proxy, the client port becomes a member of the VLAN from the I-SID/VLAN pair. The FA Proxy sends to the FA Server the binding received from the RADIUS server. If the FA Server rejects all the bindings, the client is disconnected. EAP clients are moved from AUTHENTICATED state to HELD state.

Note:

In case of a rejected binding, a delay of up to 30 seconds may exist from the time the client authenticates on the FA Proxy until the FA Server rejection response is received by the FA Proxy. Therefore, EAP client traffic may flow for up to 30 seconds until dropped.

On an FA Server, when an EAP/NEAP device is authenticated and an FA binding is received from the RADIUS server, a switched-UNI is created. This is automatically cleaned-up when the client is disconnected.

Access Points authentication

In MHSA mode, the switch also supports NEAP authentication for Access Points. Because Access Points cannot authenticate via EAP, the MHSA mode was improved as follows:

- MHSA now allows the first connected client to be a NEAP client. For each MAC seen on the port, the switch sends an Access Request to the RADIUS Server. After the first successful authentication, a configured number of auto-learned clients are granted access, as in previous MHSA behavior.
- a new option, 'no-limit', is available for configuring the switch to support an unlimited number of NEAP auto-learned clients. You can use this option when an Access Point connected to the switch supports an indeterminate number of devices.

  Previously, after the first successful EAP authentication, the switch allowed only a limited number of auto-learned NEAP clients.

  When the 'no-limit' option is enabled, the port forwards the traffic from all the devices on that port, without limiting their number. When the Access Point disconnects, the switch clears the mac-address-table for that port and blocks again all traffic. By default, the 'no-limit' option is disabled.

Note:

In FA Proxy or FA Standalone mode, the uplink port is automatically added to the Guest VLAN or Fail Open VLAN only when these VLANs are created using the **`fa vlan`** command.

Note:

EAP ports configured in MHSA mode with AP detected as an FA client will not be added to the Fail Open VLAN.

Note:

If SPBM is enabled, the ISID/VLAN bindings does not appear in the **`show fa assignment`** command. They can be checked for successful auto-creation using **`show i-sid`**, **`show vlan dynamic`**, and other VLAN show commands. In the LLDP TLV show commands they might also appear as *Pending* because only EAP is in charge of auto-creating bindings, if passed from RADIUS.

VSAs

The following is a list of VSAs added to support EAP FA functionality:

VSAs sent from RADIUS server to switch:

- Extreme-Fabric-Attach-VLAN-ISID

  This VSA consists of a (VLAN, I-SID) pair.

  Multiple (VLAN, I-SID) pairs are processed only in MHSA mode.
- Extreme-Auto-VLAN-Create

  If this VSA is set to TRUE, the VLANs received in all (VLAN, I-SID) pairs will be automatically created if they do not exist. This VSA is processed only in MHSA and MHMV modes.
- Extreme-Fabric-Attach-VLAN-PVID

  This VSA contains the value of the PVID that should be set on the port with the authenticated client. The Extreme-Fabric-Attach-VLAN-PVID VSA is processed only in MHSA mode.

Trusted FA Client

With Trusted FA Client, binding requests from FA Clients are processed by the FA agent even when the EAP port mode configuration is automated using the auto-port-mode-fa-client option or the port has been manually EAP-enabled.

The following limitations apply to the Trusted FA Client feature:

- Trusted FA Client functions in MHMV and MHSA modes.
- In this release the feature supports only NEAP clients.
- You must allow the use of VLAN IDs assigned by RADIUS for non-EAP clients in order for the feature to function in MHMV mode.
- If the Auto-Create-Vlan VSA is not sent by the RADIUS server, the FA Client binding is processed only when the VLAN already exists on switch.
- The bindings received from a trusted FA Client must meet the same restrictions as bindings received from the RADIUS server.

VSAs sent from IDE to the ERS switch:

- Extreme-Fabric-Attach-Client-Trust

  This VSA tells the switch to trust or not to trust the VLAN:ISID binding requests coming from an FA client when the port is in EAP/NEAP mode.

  This VSA can have the following values:

  - Extreme-Fabric-Attach-Client-Trust = 0 or Not sent: No FA Client VLAN:ISID binding request is trusted.
  - Extreme-Fabric-Attach-Client-Trust = 1: All FA Client VLAN:ISID binding requests are trusted.
  - Extreme-Fabric-Attach-Client-Trust = 2: Some FA Client VLAN:ISID binding requests are trusted (based on the VSA Fabric-Attach-Client-Trusted-Binding).
- Extreme-Fabric-Attach-Client-Trusted-Binding

  This VSA enables the administrator to control which VLANs and ISIDs the FA client can request. A maximum of 10 VSAs per client can be sent from Radius Server to the Switch. This VSA has a string maximum length of 64.

  This VSA has the following values:

  - For Extreme-Fabric-Attach-Client-Trust = 1:

    All FA Client VLAN:ISID binding requests are trusted and applied upon RADIUS authentication. You do not need to specify a binding range.
  - For Extreme-Fabric-Attach-Client-Trust = 2:

    Some FA Client VLAN:ISID binding requests are trusted. You must specify all VLAN:ISID bindings, including the individual VLAN:ISID bindings, as a range.

    The format of the VLAN:ISID binding is:

    minVlanValue-maxVlanValue:minIsidValue-maxIsidValue, where:

    - *minVlanValue* = minimum value of VLAN range

- *maxVlanValue* = maximum value of VLAN range
- *minIsidValue* = minimum value of ISID range
- *maxIsidValue* = maximum value of ISID range

Example:

If an FA client sends VLANs 101 through 110 with ISIDs 10010001 through 10010010, specify the VLAN:ISID bindings as a range, including the individual VLAN:ISID bindings (for example, for VLANs 101 and 108), as follows:

- Extreme-Fabric-Attach-Client-Trusted-Binding += 101-101:10010001-10010001,
- Extreme-Fabric-Attach-Client-Trusted-Binding += 103-105:10010003-10010005,
- Extreme-Fabric-Attach-Client-Trusted-Binding += 108-108:10010008-10010008

VSAs sent from switch to RADIUS server:

- Extreme-Fabric-Attach-Mode

  This VSA can have the following values:

  - 0 or not sent, when Switch is assumed to have no concept of SPB/AutoProv
  - 1, when the switch is an FA Server in VLAN provision mode
  - 2, when the switch is an FA Server in SPBM mode
  - 3, when the switch is an FA Proxy with the connected FA Server in VLAN provision mode
  - 4, when the switch is an FA Proxy with the connected FA Server in SPBM mode
  - 5 , when the switch is a FA Standalone Proxy
- Extreme-Fabric-Attach-Client-Type

  This VSA can have the following values:

  - 1, FA Element Type Other
  - 2, FA Server
  - 3, FA Proxy
  - 4, FA Server No Authentication
  - 5, FA Proxy No Authentication
  - 6, FA Client – Wireless AP Type 1 [clients direct network attachment]
  - 7, FA Client – Wireless Ap Type 2 [clients tunneled to controller]
- Fabric-Attach-Client-PSK

  This VSA can have the following values:

  - Not sent when PSK used unknown
  - 0, When Dual-key authentication is disabled
  - 10, When FA Client Failed FA TLV authentication using Default PSK
  - 11, When FA Client Passed FA TLV authentication using Default PSK
  - 100, When FA Client Failed FA TLV authentication using User Defined PSK

  - 101, When FA Client Passed FA TLV authentication using User Defined PSK
- Extreme-Fabric-Attach-Client-Id

  This VSA contains the MAC address of the FA client, exported via FA Signaling.

FA Standalone Proxy

FA Standalone Proxy introduces FA Proxy functionality in environments without an FA Server. Regardless of whether the FA Standalone Proxy upstream device is a non-Extreme Networks component or an Extreme Networks device on which FA Server functionality is not available, FA Standalone Proxy operation supports standard FA Proxy processing as if an FA Server has been discovered.

You can enable or disable FA Standalone Proxy support. By default, it is disabled. Enabling the FA Standalone Proxy mode enables immediate processing of pending I-SID/VLAN bindings, if other configuration data such as static uplink data allows the processing. Previously established settings based on FA Proxy operation, if present, are reset when FA Standalone Proxy operation is enabled.

Note:

In FA Standalone Proxy mode, I-SID values are not specified and are implicitly 0. Only bindings with an I-SID value equal to 0 are accepted for processing.

Disabling the FA Standalone Proxy mode resets configured I-SID/VLAN binding data to its default state and enables full FA Proxy operation.

In FA Standalone Proxy mode you must provide the FA Server uplink information, which is typically gathered through FA Server discovery. Once you provide this information, FA Standalone Proxy mode operates as if an FA Server has been discovered and is accepting I-SID/VLAN binding requests. The binding clean-up is similar to an FA Server timeout event, and occurs when the static uplink is deleted and when FA Standalone Proxy operation is disabled.

Note:

No interactions with an FA Server are supported in FA Standalone Proxy mode.

Note:

Before creating static uplink over a LAG, it`s highly recommended to manually bind LACP-key to an MLT-ID.

When using LACP for uplink trunk, ports should be aggregated into trunk.

Edge Automation Enhancements

Edge Automation Enhancements enable dynamic configuration of ports and VLANs that have users or devices connected to them, such as IP cameras, or Access Points.

RADIUS service requests are specified using the Fabric-Attach-Service-Request VSA.

Dynamic Configuration of Port-only Settings

Dynamic configuration can be applied to the following port-only settings:

- ability to configure port speed and duplex
- ability to enable BDPU filtering
- ability to enable SLPP Guard
- ability to enable IP Source Guard
- ability to set traffic-control for Wake on LAN (WoL) capable devices

The RADIUS user configuration attributes, which request the settings are as follows:

- Fabric-Attach-Service-Request = "BPDU"
- Fabric-Attach-Service-Request = "SLPPGUARD"
- Fabric-Attach-Service-Request = "SPEED:<speed>"
- Fabric-Attach-Service-Request = "DUPLEX:<duplex>"

  Note:

  Values for the DUPLEX attributes require the uppercase characters (HALF/FULL)
- Fabric-Attach-Service-Request = "IPSG"
- Fabric-Attach-Service-Request = "DHCPSNOOP82SUBID:<subscriber_id>"
- Fabric-Attach-Service-Request = "WOL"

Note:

IP Source Guard can be enabled only if the port is a member of a Dynamic ARP Inspection and DHCP Snooping enabled VLAN. DHCP must also be enabled globally.

Note:

As a best practice, speed and duplex must be sent from RADIUS if they are to be applied. This ensures that the link has the exact parameters desired for the device in question.

Port settings are applied when the client is the first and the only client authenticated on the port. The configuration settings are ignored if there is at least one authenticated client that pushed a set of port settings. It is expected that all clients connecting to a specific port require the same port settings. When all users on a port disconnect, all settings return to the values configured before the dynamic port settings were applied, with the exception of the traffic-control setting for WoL. For speed and duplex, port auto-negotiation returns to the original state.

Note:

Speed and duplex settings cause a port link-down link-up bounce, which removes the authenticated clients. It is necessary for the clients to reauthenticate immediately if these settings are pushed.

Note:

It is recommended to set MSTP Edge Port to True (or Spanning Tree Fast Learning if in STPG mode) on EAP-enabled ports. This prevents topology change notifications from being sent on that port and MAC addresses will not be cleared on outside topology changes, which prevents EAP clients from re-authenticating. This also speeds up reauthentication after a port bounce caused by changing speed and duplex.

Dynamic Configuration of VLAN Settings

Dynamic configuration can be applied to the following VLAN settings:

- ability to enable Dynamic ARP Inspection
- ability to enable DHCP Snooping
- ability to enable DHCP Snooping Option 82
- ability to enable IGMP snooping

Note:

DHCP Snooping and DHCP Snooping Option 82 have a global setting, which must be enabled statically in order for the feature to function properly. DHCP Snooping and Dynamic ARP Inspection trusted ports should also be configured statically.

The RADIUS user configuration attributes for VLAN settings can specify a single VLAN or a range of VLANs for each setting request.

The RADIUS user configuration attributes, which request the settings are as follows:

- Fabric-Attach-Service-Request += "DAI:<vid>[-<vid>]"
- Fabric-Attach-Service-Request += "DHCPSNOOP:<vid>[-<vid>]"
- Fabric-Attach-Service-Request += "DHCPSNOOP82:<vid>[-<vid>]"
- Fabric-Attach-Service-Request += "IGMPSNOOP:<vid>[-<vid>]"

Note:

IGMP Snooping cannot be enabled on SPBM switched UNI VLANs.

VLAN settings are applied on auto-created VLANs only. VLAN settings are applied if the client is the first and the only client authenticated that pushed the settings. It is assumed that all clients connecting to a specific VLAN require the same VLAN settings. If two or more clients join a VLAN, it is assumed that on that specific VLAN there is a set of enabled features wanted by all the clients joining the VLAN. If a client requests additional settings than those pushed by the first client, those requests are ignored.

VLAN settings persist until the auto-created VLAN is removed.

Note:

The new settings are not applied if the user authentication fails, if the new session is not valid in the FA context, or if Private VLAN context or the bindings are not consistent with the current configuration.

Fabric Attach configuration using Command Line Interface

This section provides procedural information you can use to configure Fabric Attach (FA) using Command Line Interface (CLI).

Displaying FA-specific settings

Use this procedure to display the FA configuration status.

Procedure

1. Log on to CLI to enter User EXEC mode.
2. To display the FA configuration status, enter the following command:

   ```
   show fa agent
   ```

Example

This example shows sample output for the **`show fa agent`** command default settings.

```
Switch(config)#show fa agent

Fabric Attach Service Status: Enabled
Fabric Attach Element Type: Proxy
Fabric Attach Zero Touch Status: Enabled
Fabric Attach Mgmt VLAN Distribution: Enabled
Fabric Attach Auto Provision Setting: Proxy
Fabric Attach Provision Mode: Disabled
Fabric Attach Client Proxy Status: Enabled
Fabric Attach Standalone Proxy Status: Disabled
Fabric Attach Agent Timeout: 240 seconds
Fabric Attach Extended Logging Status: Disabled
Fabric Attach Primary Server Id: <none>
Fabric Attach Primary Server Descr: <none>
```

This example shows sample output for the **`show fa agent`** command when management VLAN data in the FA Element TLV is disabled.

```
Switch(config)#show fa agent

Fabric Attach Service Status: Enabled
Fabric Attach Element Type: Proxy
Fabric Attach Zero Touch Status: Enabled
Fabric Attach Mgmt VLAN Distribution: Disabled
Fabric Attach Auto Provision Setting: Proxy
Fabric Attach Provision Mode: Disabled
Fabric Attach Client Proxy Status: Enabled
```

```
Fabric Attach Standalone Proxy Status: Disabled
Fabric Attach Agent Timeout: 240 seconds
Fabric Attach Extended Logging Status: Disabled
Fabric Attach Primary Server Id: <none>
Fabric Attach Primary Server Descr: <none>
```

This example shows sample output for the **`show fa agent`** command in FA Proxy mode.

Displaying Fabric Attach elements

Use this procedure to display discovered Fabric Attach elements.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To display the discovered FA elements, enter the following:

   ```
   show fa elements [<portlist> | trunk <trunknumber> | element-type
   {server | proxy | client} | auth-status  {auth-pass | auth-fail |
   not-auth} | client-type <6-17>]
   ```

Example

The following example displays sample output for the `show fa elements` command.

```
=============================================================================
Fabric Attach Discovered Elements
=============================================================================
UNIT/                MGMT                                            ELEM ASGN
PORT    TYPE         VLAN  STATE  SYSTEM ID                          AUTH AUTH
-----------------------------------------------------------------------------
1/5     Server       1234  T / S  6c:fa:58:dc:fc:00:00:00:01:05       AP   AP
1/36    Client       1     U / D  fc:a8:41:fa:f8:00:00:00:00:24       AP   N
=============================================================================
                    Fabric Attach Authentication Detail
=============================================================================
UNIT/                     ELEM OPER                 ASGN OPER
PORT   EXPANDED TYPE      AUTH STATUS               AUTH STATUS
-----------------------------------------------------------------------------
1/5    Server (Auth)      successAuth               successAuth
1/36   Switch             successAuth               none
State Legend: (Tagging/AutoConfig)
T=Tagged, U=Untagged, D=Disabled, S=Spbm, V=Vlan, I=Invalid
Auth Legend:
AP=Authentication Pass, AF=Authentication Fail, NA=Not Authenticated, N=None
-----------------------------------------------------------------------------
2 out of 2 total number of Fabric Attach discovered elements displayed
-----------------------------------------------------------------------------
```

Field	Definition
State	FA Element TLV state field data
Elem Auth	FA Element TLV authentication status

Table continues…

Field	Definition
Asgn Auth	FA I-SID/VLAN Assignment TLV authentication status
Elem Oper Auth Status	FA Element TLV authentication status detail data
Asgn Oper Auth Status	FA I-SID/VLAN Assignment TLV authentication status detail data

Variable Definitions

The following table describes the parameters for the `show fa elements` command.

Variable	Value
<portlist>	Specifies a port or a list of ports for which to display discovered FA elements.
trunk <trunknumber>	Specifies a trunk number for which to display discovered FA elements.
auth-status {auth-pass | auth-fail | not-auth}	Displays only specified authorized status FA elements.
element-type {server | proxy | client}	Displays only specified element type.
client-type <6-17>	Displays only specified client type.

Displaying I-SID-to-VLAN assignment information

Use this procedure to display information about I-SID-to-VLAN assignments.

Procedure

1. Log on to CLI to enter User EXEC mode.
2. To display I-SID-to-VLAN assignment information on an FA Proxy, enter the following commands:

   `show fa i-sid [<1-16777214>]`

   `show i-sid [<1-16777214>]`

   OR

   `show fa assignment [<1-16777214>]`

   `show i-sid [<1-16777214>]`

Example

The following example displays sample output for the **`show fa i-sid`** command.

```
Switch(config)#show fa i-sid

 I-SID     VLAN     Source        Status
--------   ----   -------------  --------
500        5      Proxy          Active
```

```
501       25    Client         Active
600       6     Proxy, Client  Active
13849     138   Proxy          Rejected (VLAN invalid)
16000000  1000  Proxy          Rejected (application interaction issue)
```

Variable definitions

The following table describes the parameters for the **show fa i-sid [<1–16777214>]** or **show fa assignment [<1–16777214>]** command.

Variable	Value
[<1-16777214>]	Specifies the Fabric Attach I-SID for which to display I-SID-to-VLAN assignment information. Values range from 1 to 16777214. If you do not specify a I-SID value, the switch displays information for all configured I-SID-to-VLAN assignments.

Creating an I-SID-to-VLAN assignment on an FA proxy

About this task

Use this procedure to create an association between an I-SID and a VLAN on an FA Proxy, when SPBM is disabled on switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To create an I-SID-to-VLAN assignment, enter the following command:

   ```
   i-sid <1–16777214> vlan <1–4094>
   ```

Result

Each FA Proxy I-SID-to-VLAN assignment creates a C-VLAN User Network Interface (UNI) when the assignment is active and accepted by an FA server.

Example

The following example creates an association between I-SID 600 and VLAN 3:

```
Switch(config)#i-sid 600 vlan 3
Switch(config)#
```

Variable definitions

The following table describes the parameters for the `i-sid <1–16777214> vlan <1–4094>` command

Variable	Value
i-sid *<1-16777214>*	Specifies the I-SID to associate with the selected VLAN. Values range from 1 to 16777214.
vlan *<1-4094>*	Specifies the VLAN to associate with the selected I-SID. Values range from 1 to 4094.

Deleting an I-SID-to-VLAN assignment on an FA Proxy

Use this procedure to remove the association between an I-SID and a VLAN on an FA Proxy.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To remove a specific I-SID-to-VLAN assignment, enter the following command:

   ```
   no i-sid <I-SID> vlan <VLAN>
   ```

3. To remove all configured I-SID-to-VLAN assignments, enter the following command:

   ```
   default i-sid
   ```

Variable definitions

The following table describes the parameters for the `no i-sid <I-SID> vlan <VLAN>` command

Variable	Value
i-sid *<1-16777214>*	Specifies the I-SID of the specific I-SID-to-VLAN assignment to remove. Values range from 1 to 16777214.
vlan *<1-4094>*	Specifies the VLAN of the specific I-SID-to-VLAN assignment to remove. Values range from 1 to 4094.

Configuring external client proxy support

Use this procedure to enable or disable external client proxy support.

About this task

This operation enables or disables external client proxy support. It does not impact communication with an FA Server.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. To enable external client proxy support, enter either of the following commands:

   ```
   fa proxy
   ```

   OR

   ```
   default fa proxy
   ```

3. To disable external client proxy support, enter the following command:

   ```
   no fa proxy
   ```

Configuring FA on switch ports

Use this procedure to enable or disable the FA operation on one or more switch ports.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To configure the FA operation on switch ports, enter the following command:

   ```
   [no][default] fa port-enable [<portlist>]
   ```

Variable definitions

The following table describes the parameters for the `[no][default] fa port-enable [<portlist>]` command.

Variable	Value
[<portlist>]	Enables the FA operation on the specified switch port or ports. If you do not specify a port, the FA operation is enabled on all switch ports.
[no]	Disables the FA operation on the specified switch port or ports. If you do not specify a port or ports, the FA operation is disabled on all switch ports.
[default]	Restores the FA operation on all switch ports to default.

Displaying switch port FA operation status

Use this procedure to display per-port FA operation status.

Procedure

1. Log on to CLI to enter User EXEC mode.
2. To display FA configuration information, enter one of the following commands:

   `show fa port-enable [<portlist> | enabled-port | disabled-port | enabled-auth | disabled-auth]`

   OR

   `show fa interface [<portlist> | enabled-port | disabled-port | enabled-auth | disabled-auth]`

Example

The following example displays sample output for the `show fa port-enable` command.

```
Switch(config)#show fa port-enable

                           Service
Unit Port IfIndex Trunk Advertisement Authentication Keymode
---- ---- ------- ----- --------------------- --------------
1    1    1                  Enabled   Enabled     Strict
1    2    2                  Enabled   Enabled     Strict
1    3    3                  Enabled   Enabled     Strict
1    4    4         2        Enabled   Enabled     Standard
1    5    5         2        Enabled   Enabled     Standard
1    6    6                  Enabled   Enabled     Strict
```

Variable Definitions

The following table describes the parameters for the `show fa port-enable` or `show fa interface` command.

Variable	Value
<portlist>	Specifies a port or a list of ports for which to display FA operation status. If you do not specify a port or ports, the switch displays FA operation status for all switch ports.
enabled-port	Displays only FA enabled ports.
disabled-port	Displays only FA disabled ports.
enabled-auth	Displays only authentication enabled ports.
disabled-auth	Displays only authentication disabled ports.

Configuring the FA authentication key

Use the following command to configure the FA authentication key on specified ports.

Note:

You can configure the FA authentication key only on secure images.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the FA authentication key:

   ```
   [default] fa authentication-key <portlist>
   ```

   Enter the authentication key, and then re-enter the key for confirmation. For security purposes, key data is hidden.

Variable Definitions

The following table describes the parameters for the `fa authentication-key` command.

Variable	Value
<portlist>	Specifies a port or a list of ports for which to define the authentication key.

Configuring FA message authentication support

Use the following procedure to configure the FA message authentication support on specified ports.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable the FA message authentication support:

   ```
   fa message-authentication [<PortList>] [key-mode <strict |
   standard>]
   ```

3. **(Optional)** Reset the FA message authentication support to default:

   ```
   default fa message-authentication
   ```

   Note:

   The default setting is *enabled*.

4. **(Optional)** Disable the FA message authentication support:

   ```
   no fa message-authentication [<PortList>]
   ```

Variable Definitions

The following table describes the parameters for the `fa message-authentication` command.

Variable	Value
<portlist>	Specifies a port or a list of ports for which to enable the FA message authentication support.
key-mode <strict | standard>	Specifies the Authentication key usage setting — the user-defined authentication key (strict) or both the user-defined and default authentication keys (standard) are used for FA TLV data authentication. Default key-mode is strict.

Configuring FA VLANs

Use this procedure to create or delete FA VLANs on an FA Proxy or FA Standalone Proxy.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To create FA VLANs, enter the following command:

   ```
   fa vlan <LINE>
   ```

3. To delete FA VLANs, enter the following command:

   ```
   no fa vlan <LINE>
   ```

4. To delete all configured FA VLANs, enter the following command:

   ```
   default fa vlan
   ```

Example

The following is an example of creating an FA VLAN and verifying the configuration.

```
Switch(config)#fa vlan 6
Switch(config)#show fa vlan

VLAN           Source             Status
----  -------------------------  --------
6     Proxy                      Pending

Binding Count: 1
```

Variable Definitions

The following table describes the parameters for the `show fa vlan` command.

Variable	Value
<LINE>	Specifies an individual VLAN ID or a range of VLAN IDs to create. A VLAN ID can range from 1 to 4094.

Displaying Fabric Attach VLAN information

Use this procedure to display Fabric Attach-specific VLAN information.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To display Fabric Attach VLAN information, enter the following command:

   ```
   show fa vlan [<1-4094>]
   ```

Example

The following example displays sample output for the `show fa vlan` command.

```
Switch(config)#show fa vlan

VLAN    Source      Status
----  -----------  --------
1007  Proxy        Pending
1008  Proxy        Pending
```

Enabling or disabling FA Zero Touch support

Use this procedure to enable or disable the global FA Zero Touch support on an FA Proxy or FA Standalone Proxy. By default, FA Zero Touch support is enabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. To enable FA Zero Touch support on an FA Proxy, FA Server, or FA Standalone Proxy, enter the following command:

   ```
   fa zero-touch
   ```

3. To disable FA Zero Touch support on an FA Proxy, FA Server, or FA Standalone Proxy, enter the following command:

   ```
   no fa zero-touch
   ```

4. To reset the FA Zero Touch support state to default, enter the following command:

   ```
   default fa zero-touch
   ```

Configuring FA Zero Touch options

Use this procedure to configure FA Zero Touch option settings.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To enable an FA Zero Touch option, enter the following command:

   ```
   fa zero-touch-options {{auto-client-attach | auto-mgmt-vlan-fa-client | auto-port-mode-fa-client | auto-pvid-mode-fa-client | auto-trusted-mode-fa-client |} [client-type {hint | <6-17>}] | ip-addr-dhcp}
   ```

   Note:

   The `auto-client-attach` option must be enabled before Zero Touch Client specifications can be applied (either during discovery or retroactively).

   Note:

   The `auto-port-mode-fa-client` option is incompatible with both the `auto-pvid-mode-fa-client` and `auto-client-attach` options.

   Note:

   The `auto-mgmt-vlan-fa-client` option is incompatible with the `auto-pvid-mode-fa-client` and the `auto-port-mode-fa-client` options, as well as with the Zero Touch Client (ZTC) auto-attach support.

3. To disable a specific FA Zero Touch option, enter the following command:

   ```
   no fa zero-touch-options {{auto-port-mode-fa-client | auto-mgmt-vlan-fa-client| auto-pvid-mode-fa-client | auto-trusted-mode-fa-client | auto-client-attach} | ip-addr-dhcp}
   ```

4. To clear all FA Zero Touch option settings, enter the following command:

   ```
   default fa zero-touch-options
   ```

Example

```
Switch(config)#fa zero-touch-options auto-mgmt-vlan-fa-client client-type 8,9
Switch(config)#show fa zero-touch-options

Fabric Attach Zero Touch Options:
auto-mgmt-vlan-fa-client
auto-port-mode-fa-client
```

```
auto-pvid-mode-fa-client
auto-trusted-mode
```

```
  4850GTS-PWR+(config)#show fa zero-touch-options client-data

Zero Touch Client Data

Type            Client Name             Applicable Zero Touch Options
----  --------------------------------  ------------------------------------
6     wap-type1                         auto-port-mode
7     wap-type2
8     switch                            auto-mgmt-vlan
9     router                            auto-mgmt-vlan auto-trusted-mode
10    phone
11    camera                            auto-trusted-mode
12    video
13    security-dev
14    virtual-switch                    auto-port-mode
15    srvr-endpt                        auto-pvid-mode
16    ona-sdn                           auto-port-mode
17    ona-spb-over-ip
```

Variable Definitions

The following table describes the parameters for the `fa zero-touch-options` command.

Variable	Value
auto-port-mode-fa-client	Automates the configuration of EAP port modes.
auto-pvid-mode-fa-client	Automates client PVID/Mgmt VLAN updates.
auto-trusted-mode-fa-client	Automates the FA Client connection default QoS treatment.
auto-mgmt-vlan-fa-client	Automates management VLAN updates.
ip-addr-dhcp	Automates DHCP IP address acquisition.
auto-client-attach	Automates client attach configuration.
client-type <6–17>	Specifies an FA client type or a list of FA client types. Following are the available client types: • 6—Wireless AP (Type 1) • 7—Wireless AP (Type 2) • 8—Switch • 9—Router • 10—IP Phone • 11—IP Camera • 12—IP Video • 13—Security Device • 14—Virtual Switch • 15—Server Endpoint • 16—ONA (SDN) • 17—ONA (SpbOIp)

Note:

Default FA client types WAP Type 1 (6) and Switch (8) are associated with the client type-specific Zero Touch options if no client-type data is provided with the CLI commands.

Displaying FA Zero Touch option settings

Use this procedure to verify the FA Zero Touch option settings.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To display the FA Zero Touch option settings, enter the following command:

   ```
   show fa zero-touch-options [client-data]
   ```

Example

The following is an example of configuring and displaying FA Zero Touch options.

```
Switch(config)#fa zero-touch-options auto-port-mode-fa-client client-type 6,14-16
Switch(config)#show fa zero-touch-options

Fabric Attach Zero Touch Options:

    ip-addr-dhcp
    auto-port-mode-fa-client
```

The following is an example of displaying client data.

```
Switch(config)#show fa zero-touch-options client-data

Zero Touch Client Data

Type            Client Name             Applicable Zero Touch Options
----  --------------------------------  ------------------------------------
6     wap-type1                         auto-port-mode
7     wap-type2
8     switch
9     router
10    phone
11    camera
12    video
13    security-dev
14    virtual-switch                    auto-port-mode
15    srvr-endpt                        auto-port-mode
16    ona-sdn                           auto-port-mode
17    ona-spb-over-ip

Type                        Client Description                         Origin
---- ---------------------------------------------------------------- --------
6    Wireless AP (Type 1)                                             Standard
7    Wireless AP (Type 2)                                             Standard
8    Switch                                                           Standard
9    Router                                                           Standard
10   IP Phone                                                         Standard
11   IP Camera                                                        Standard
```

```
12   IP Video                                                         Standard
13   Security Device                                                  Standard
14   Virtual Switch                                                   Standard
15   Server Endpoint                                                  Standard
16   ONA (SDN)                                                        Standard
17   ONA (SpbOIp)                                                     Standard
Zero Touch Client Data

Switch(config)#
```

Disabling Management VLAN Distribution

Use this procedure to exclude management VLAN data in the FA Element TLV. When this option is not specified, management VLAN data in the FA Element TLV is included, by default.

Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. Enter the following command to disable management VLAN distribution:

   `fa zero-touch disable-mgmt-vlan-distribution`

3. Enter the following command to disable zero-touch operations, including management VLAN distribution:

   `no fa zero-touch`

4. Enter the following command to enable management VLAN distribution:

   `default fa zero-touch`

Example

```
Switch enable
Switch config term
Switch (config)# fa zero-touch disable-mgmt-vlan-distribution
```

```
Switch (config)# show fa agent

Fabric Attach Service Status: Enabled
Fabric Attach Element Type: Proxy
Fabric Attach Zero Touch Status: Enabled
Fabric Attach Mgmt VLAN Distribution: Disabled
Fabric Attach Auto Provision Setting: Proxy
Fabric Attach Provision Mode: Disabled
Fabric Attach Client Proxy Status: Enabled
Fabric Attach Standalone Proxy Status: Disabled
Fabric Attach Agent Timeout: 240 seconds
Fabric Attach Extended Logging Status: Disabled
Fabric Attach Primary Server Id: <none>
Fabric Attach Primary Server Descr: <none>
```

Configuring FA Zero Touch Client

Use the following procedure to manipulate Fabric Attach Zero Touch Client (ZTC) specifications on a FA Proxy or FA Server.

Note:

The `auto-client-attach` option must be enabled before Zero Touch Client specifications can be applied (either during discovery or retroactively).

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To enable an FA Zero Touch Client, enter the following command:

   ```
   fa zero-touch-client standard {camera | ona-sdn | ona-spb-over-ip |
   phone | router | security-dev | srvr-endpt | switch | video |
   virtual-switch | wap-type1 | wap-type2} vlan <VLAN> [i-sid <ISID>]
   [priority <Priority>][keep-static]
   ```

3. To delete a specific FA Zero Touch Client, enter the following command:

   ```
   no fa zero-touch-client standard <ClientName>
   ```

4. To clear all FA Zero Touch Client settings, enter the following command:

   ```
   default fa zero-touch-client
   ```

Variable definitions

The following table describes the parameters for the `fa-zero-touch-client` command.

Variable	Value
standard	Specifies the Standard (pre-defined) client type. The following client types are available: • 6 - Wireless AP (Type 1) • 7 - Wireless AP (Type 2) • 8 - Switch • 9 - Router • 10 - IP Phone • 11 - IP Camera • 12 - IP Video • 13 - Security Device

Table continues…

Variable	Value
	• 14 - Virtual Switch • 15 - Sever Endpoint • 16 - ONA (SDN) • 17 - ONA (SpbOIp)
vlan ID <1–4094>	Specifies the VLAN ID.
ISID <0–16777214>	Specifies the Client I-SID for I-SID/VLAN binding generation.
priority <0–7>	Specifies the Client port priority.
keep-static	Specifies whether static VLANs should be kept or removed on the client port for the duration of the client connection.

Displaying FA Zero Touch Client

Use the following procedure to display Fabric Attach Zero Touch Client (ZTC) specifications on a FA Proxy or FA Server.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Enter the following command:

   ```
   show fa zero-touch-client
   ```

Example

The following example displays sample output for the `show fa zero-touch-client`.

```
Switch(config)#show fa zero-touch-client

Fabric Attach Zero Touch Client Auto-Attach Specifications

                                                              Static
Type           Client Name            VLAN I-SID    Priority  VLANs
---- -------------------------------- ---- -------- -------- -------
6    wap-type1                        123  11111       NA    remove
11   camera                           200  2000        5     remove
17   ona-spb-over-ip                  4001 40001       7     keep

Zero Touch Client Auto-Attach Specification count: 3
Switch(config)#
```

Configuring FA Standalone Proxy mode

Use this procedure to enable or disable the FA Standalone Proxy mode on the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To enable FA Standalone Proxy mode, enter the following command:

   ```
   fa standalone-proxy
   ```

3. To disable FA Standalone Proxy mode, enter the following command:

   ```
   no fa standalone-proxy
   ```

4. To restore the FA Standalone Proxy mode to default, enter the following command:

   ```
   default fa standalone-proxy
   ```

Displaying FA uplink values

Use this procedure to display FA static uplink values used in FA Standalone Proxy mode.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To display FA static uplink values, enter the following command:

   ```
   show fa uplink
   ```

Example

The following example displays sample output for the `show fa uplink` command.

```
Switch(config)#show fa uplink

Fabric Attach Static Uplinks:
    port - 0
    trunk - 8 (dynamic MLT [LAG admin key 300] - active)
```

Configuring the static uplink for FA Standalone Proxy mode

Use this procedure to specify a port or trunk to use as a static uplink associated with FA Standalone Proxy operation.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To specify a port uplink or a trunk uplink to use in FA Standalone Proxy mode, enter the following command:

   ```
   fa uplink {port <port> | trunk <trunkId>}
   ```

3. To clear static uplink data, enter the following command:

   ```
   no fa uplink
   ```

Variable Definitions

The following table describes the parameters for the `fa uplink` command.

Variable	Value
<port>	Specifies the port to use as a static uplink.
<trunkId>	Specifies the trunk ID to use as a static uplink.

Configuring Fabric Attach extended-logging

Use the following procedure to configure Fabric Attach extended-logging.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable Fabric Attach extended-logging:

   ```
    fa extended-logging
   ```

3. Disable Fabric Attach extended-logging:

   ```
   no fa extended-logging
   ```

Configuring the FA timeout

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To configure the FA timeout, enter the following command:

   ```
   fa timeout <45-480>
   ```

3. To reset the timeout to its default value, enter the following command:

   ```
   default fa timeout
   ```

Clearing FA statistics

Use the following procedure to clear FA summary and per-port statistics counters. You can clear global counters, counters for an individual port or range of ports, or all ports.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Clear FA statistics:

   ```
   clear fa statistics [summary | <PortList>]
   ```

Variable Definitions

The following table describes the parameters for the `show fa statistics` command.

Variable	Value
<portlist>	Specifies a port or a list of ports for which to display statistics counters.

Displaying FA statistics

Use the following procedure to display the FA summary and per-port statistics counters. You can display global counters, counters for an individual port or range of ports, or all ports. When no port data is specified, only data for ports that are FA-enabled is displayed.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Display FA statistics:

   ```
   show fa statistics [summary | <portlist>]
   ```

Variable Definitions

The following table describes the parameters for the `show fa statistics` command.

Variable	Value
<portlist>	Specifies a port or a list of ports for which to display statistics counters.

Fabric Attach configuration using Enterprise Device Manager

Use the procedures in this section to configure Fabric Attach (FA) using Enterprise Device Manager.

Configuring Fabric Attach

Use this procedure to configure Fabric Attach.

Procedure

1. From the navigation tree, select **Edit > Fabric Attach**.
2. Click the **Agent** tab.
3. To set the Auto Provision mode to FA Proxy, click **proxy** in the **AutoProvision** field.
4. To enable or disable FA Standalone Proxy mode, click **enable** or **disable** in the **StandaloneProxy** field.
5. To enable or disable external client proxy support, click **enable** or **disable** in the **ClientProxy** field.
6. Specify the port to use as a static uplink associated with FA Standalone Proxy operation in the **UplinkPort** field.
7. Specify the trunk to use as a static uplink associated with FA Standalone Proxy operation in the **UplinkTrunk** field.
8. Specify the agent timeout in the **Timeout** field.
9. To enable or disable extended logging, click **enable** or **disable** in the **ExtendedLogging** field.
10. Click **Apply**.

Variable definitions

Use the data in the following table to use the **Agent** tab.

Variable	Value
Service	Displays the service status.
ElementType	Displays the element type.
ProvisionMode	Displays the provision mode status
AutoProvision	Displays the Auto Provision mode.
StandaloneProxy	Specifies whether FA Standalone Proxy mode is enabled or disabled. The default is disabled.

Table continues…

Variable	Value
ClientProxy	Specifies whether external client proxy is enabled or disabled. The default is enabled.
UplinkPort	Specifies the port to use as a static uplink associated with FA Standalone Proxy operation.
UplinkTrunk	Specifies the trunk to use as a static uplink associated with FA Standalone Proxy operation.
Timeout	
ExtendedLogging	Specifies whether extended logging is enabled or disabled. The default is disabled.

Configuring an I-SID/VLAN assignment

Use the following procedure to configure an I-SID/VLAN assignment on an FA Proxy.

Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit**.
2. Click **Fabric Attach**.
3. In the work area, click the **I-SID** tab.
4. Click **Insert**.
5. Specify an I-SID in the **Isid** field.
6. Specify a VLAN in the **Vlan** field.
7. Click **Insert**.

Variable definitions

Use the data in the following table to use the **I-SID** tab.

Name	Description
Isid	Specifies the I-SID to associate with a VLAN.
Vlan	Specifies the VLAN to associate with an I-SID.
State	Indicates the state of the VLAN/I-SID assignment.
Source	Indicates the source of the VLAN/I-SID assignment.

Configuring per-port FA settings

Use the following procedure to enable or disable FA Signaling or to configure FA message authentication.

Procedure

1. From the navigation tree, select **Edit**.
2. In the Edit tree, double-click **Fabric Attach**.
3. On the work area, click the **Ports** tab.
4. To enable or disable the transmission of FA information in FA Signaling, select **enabled** or **disabled** in the **State** field for a specific port or ports.
5. To enable or disable message authentication, select **enabled** or **disabled** in the **MsgAuthStatus** field for a specific port or ports.
6. To configure the authentication key, enter an alphanumeric string of up to 32 characters in the **MsgAuthKey** field for a specific port or ports.
7. To configure the authentication key usage, select **strict** or **standard** in the **MsgAuthKeymode** field for a specific port or ports.
8. Click **Apply**.

Variable Definition

Variable	Value
IfIndex	Indicates the interface for which to configure FA operation and message authentication.
State	Enables or disables FA operation on the interface.
MsgAuthKey	Configures the authentication key for the specified interface.
MsgAuthStatus	Enables or disables FA message authentication on the interface.
MsgAuthKeymode	Specifies the Authentication key usage setting — the user-defined authentication key (strict) or both the user-defined and default authentication keys (standard) are used for FA TLV data authentication. Default key-mode is strict.

Displaying Fabric Attach elements

Use the following procedure to view discovered FA elements.

Procedure

1. In the navigation tree, expand the following folders: **Configuration>Edit**.
2. Click **Fabric Attach**.
3. In the work area, click the **Elements** tab.

Variable definitions

Use the data in the following table to use the **Elements** tab.

Name	Description
Ifindex	Indicates the interface through which the FA element was discovered.
Type	Indicates the FA element type.
Vlan	Indicates the management VLAN advertised by the FA element.
Id	Indicates the FA Element System ID, which is the unique system identifier used for connection management and limited device state distribution.
State	Indicates the state flag data associated with the discovered FA element.
Auth	Indicates the authentication status for the discovered element.
OperAuthStatus	Displays FA Element TLV authentication status detail data.
AsgnsAuth	Indicates FA I-SID/VLAN Assignment TLV authentication status.
AsgnsOperAuthStatus	Displays FA I-SID/VLAN Assignment TLV authentication status detail data.

Automating configurations for FA Clients

Use the following procedure to automate configurations for specific types of FA Clients.

Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit**.
2. Click **Fabric Attach**.
3. In the work area, click the **Zero Touch** tab.
4. To enable or disable Zero Touch support, click enable or disable in the **ZeroTouchService** field.
5. To enable or disable Fabric Attach Mgmt VLAN Distribution, click enable or disable in the **ZeroTouchMgmtVlanDist** field.
6. To enable Zero Touch options, select the appropriate check-box in the **OptionFlags** field.
7. Specify the FA Client type ID for the selected OptionFlag:
   - Specify the FA Client type ID in the **autoPortModeFaClient** field to automate the configuration of EAP port modes.
   - Specify the FA Client type ID in the **autoTrustedModeFaClient** field to automate the FA Client connection default QoS treatment.
   - Specify the FA Client type ID in the **autoPvidModeFaClient** field to automate client PVID/Mgmt VLAN updates.

- Specify the FA Client type ID in the in the **autoClientAttach** field to automate the FA Client Attach field.
- Specify the FA Client type ID in the in the **autoMgmtVlanFaClient** field to automate the FA Client auto mgmt Vlan.

8. Click **Apply**.

Variable definitions

Use the data in the following table to use the **Zero Touch Client** tab.

Name	Description
Type	Indicates the FA Client type ID.
Descr	Indicates the FA Client type.
OptionFlags	Opens the OptionFlags dialog box to specify the automated configurations for an FA Client type. • ipAddrDhcp — automates DHCP IP address acquisition. • autoPortModeFaClient: Automates the configuration of EAP port modes. • autoTrustedModeFaClient: Automates the FA Client connection default QoS treatment. • autoPvidModeFaClient: Automates client PVID/Mgmt VLAN updates. • autoClientAttach: Automates Zero Touch Client Attach configuration. • autoMgmtVlanFaClient: Automates the FA Client auto mgmt Vlan.
Disable all	Clears all options.
Select all	Selects all available options.
Ok	Confirms the selected options.
Close	Closes the OptionFlags dialog box.

Configuring Zero Touch Client Auto Attach

Procedure

1. In the navigation tree, expand the following folders: **Configuration > Edit**.
2. Click **Fabric Attach**.
3. In the work area, click the **Zero Touch Client Auto Attach** tab.
4. Click **Insert**.
5. Select the Zero Touch Client Auto Attach type from the **Type** list and click **Ok**.

6. Specify a VLAN in the **Vlan** field.
7. Specify I-SID in the **Isid** field.
8. Specify a priority in the **PortPriority** field.
9. Select keepStaticVlan to keep the static VLANs or select removeStaticVlans to remove the static VLANs from the **ExcludeStatic** options.

   Depending on the selection, the static VLANs are kept or removed on the client port for the duration of the client connection.
10. Click **Insert**.

Variable definitions

Use the data in the following table to use the **Zero Touch Client Auto Attach** tab.

Name	Description
ClientName	Specifies an FA client type or a list of FA client types. Following are the available client types: • 6—Wireless AP (Type 1) • 7—Wireless AP (Type 2) • 8—Switch • 9—Router • 10—IP Phone • 11—IP Camera • 12—IP Video • 13—Security Device • 14—Virtual Switch • 15—Server Endpoint • 16—ONA (SDN) • 17—ONA (SpbOIp)
Type	Specifies the Zero Touch Client Auto Attach type. If this type matches the FA interface type, Zero Touch Client Auto Attach specifications are applied to the port. Type 0 applies the specifications to non-EAP enabled, non-FA Client ports. Type 1 applies the specifications to non-EAP enabled, FA Client (any) ports. **Note:** Zero Touch Client Auto Attach specification processing terminates if no applicable interfaces are found.

Table continues…

Name	Description
Vlan	Specifies the VLAN ID. The value range is from 1 to 4094.
Isid	Specifies the Isid value. The value range is from 0 to 16777214.
PortPriority	Specifies 802.1p user priority. The value range is from 1 to 7.
ExcludeStatic	Specifies whether static VLANs should be kept or removed on the client port for the duration of the client connection. Default is RemoveStaticVlans.

Displaying Fabric Attach statistics

Use any one of the following procedures to view the Fabric Attach statistics:

- Displaying Fabric Attach statistics for ports on page 57
- Displaying Fabric Attach in a graph on page 58
- Displaying Fabric Attach statistics for chassis on page 60

Displaying Fabric Attach statistics for ports

About this task

Use the following procedure to view FA statistics based on port index.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Edit**
2. Click **Fabric Attach**.
3. In the work area, click the **Port Stats** tab.
4. Select a port row.
5. **(Optional)** Click **Graph** to view the statistics.
6. **(Optional)** Click **Clear Counters** to clear the counters and start over at zero.

Variable definitions

Use the data in the following table to use the **Port Stats** tab.

Name	Description
PortIndex	Indicates the port for which FA statistics are displayed.
DiscElemReceived	Indicates the number of FA Element TLVs received on the identified port.
DiscElemExpired	Indicates the number of discovered FA elements from received FA Element TLVs that have expired on the identified port. This counter is not incremented

Table continues…

Name	Description
	when elements are deleted for reasons other than expiration.
DiscElemDeleted	Indicates the number of discovered FA elements from received FA Element TLVs that have been deleted on the identified port. This counter is only incremented when elements are deleted for reasons other than expiration.
DiscAuthFailed	Indicates the number of received FA Element TLVs for which authentication was attempted and failed on the identified port.
AsgnReceived	Indicates the number of I-SID/VLAN bindings received in FA I-SID/VLAN Assignment TLVs on the identified port.
AsgnAccepted	Indicates the number of I-SID/VLAN bindings from received FA I-SID/VLAN Assignment TLVs that are accepted (activated) on the identified port. This counter is incremented when the binding transitions from a non-accepted state such as 'pending'or 'rejected' to the accepted state.
AsgnRejected	Indicates the number of I-SID/VLAN bindings from received FA I-SID/VLAN Assignment TLVs that are rejected on the identified port. This counter is incremented when the binding transitions from a non-rejected state such as 'pending' or 'accepted' to the rejected state.
AsgnExpired	Indicates the number of I-SID/VLAN bindings from received FA I-SID/VLAN Assignment TLVs that have expired on the identified port. This counter is not incremented when bindings are deleted for reasons other than expiration.
AsgnDeleted	Indicates the number of I-SID/VLAN bindings from received FA I-SID/VLAN Assignment TLVs that have been deleted on the identified port. This counter is only incremented when bindings are deleted for reasons other than expiration.
AsgnAuthFailed	Indicates the number of received FA I-SID/VLAN Assignment TLVs for which authentication was attempted and failed on the identified port.

Displaying Fabric Attach statistics in a graph

About this task

Use the following procedure to view FA statistics.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Edit**

2. Click **Fabric Attach**.
3. In the work area, click the **Port Stats** tab.
4. Select a port row.
5. Click **Graph**.

   The FA Stats tab appears.
6. From the work area, select **Poll Interval**.

   The table data refreshes automatically based on the value selected in the Poll Interval field.
7. **(Optional)** Click **Clear Counters** to clear the counters and start over at zero.

Variable definitions

Use the data in the following table to use the **FA Stats** tab.

Name	Description
DiscElemReceived	Indicates the number of FA Element TLVs received on the identified port.
DiscElemExpired	Indicates the number of discovered FA elements from received FA Element TLVs that have expired on the identified port. This counter is not incremented when elements are deleted for reasons other than expiration.
DiscElemDeleted	Indicates the number of discovered FA elements from received FA Element TLVs that have been deleted on the identified port. This counter is only incremented when elements are deleted for reasons other than expiration.
DiscAuthFailed	Indicates the number of received FA Element TLVs for which authentication was attempted and failed on the identified port.
AsgnReceived	Indicates the number of I-SID/VLAN bindings received in FA I-SID/VLAN Assignment TLVs on the identified port.
AsgnAccepted	Indicates the number of I-SID/VLAN bindings from received FA I-SID/VLAN Assignment TLVs that are accepted (activated) on the identified port. This counter is incremented when the binding transitions from a non-accepted state such as 'pending'or 'rejected' to the accepted state.
AsgnRejected	Indicates the number of I-SID/VLAN bindings from received FA I-SID/VLAN Assignment TLVs that are rejected on the identified port. This counter is incremented when the binding transitions from a

Table continues…

Name	Description
	non-rejected state such as 'pending' or 'accepted' to the rejected state.
AsgnExpired	Indicates the number of I-SID/VLAN bindings from received FA I-SID/VLAN Assignment TLVs that have expired on the identified port. This counter is not incremented when bindings are deleted for reasons other than expiration.
AsgnDeleted	Indicates the number of I-SID/VLAN bindings from received FA I-SID/VLAN Assignment TLVs that have been deleted on the identified port. This counter is only incremented when bindings are deleted for reasons other than expiration.
AsgnAuthFailed	Indicates the number of received FA I-SID/VLAN Assignment TLVs for which authentication was attempted and failed on the identified port.

Displaying Fabric Attach statistics for chassis

About this task

Use the following procedure to view FA statistics.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Graph**
2. Click **Chassis**.
3. In the work area, click the **Fabric Attach** tab.
4. Select a port row.
5. The table data refreshes automatically based on the value selected in the **Poll Interval** field.
6. **(Optional)** Click **Clear Counters** to clear the counters and start over at zero.

Variable definitions

Use the data in the following table to use the **FA Stats** tab.

Name	Description
DiscElemReceived	Indicates the number of FA Element TLVs received on the identified port.
DiscElemExpired	Indicates the number of discovered FA elements from received FA Element TLVs that have expired on the identified port. This counter is not incremented when elements are deleted for reasons other than expiration.
DiscElemDeleted	Indicates the number of discovered FA elements from received FA Element TLVs that have been

Table continues…

Name	Description
	deleted on the identified port. This counter is only incremented when elements are deleted for reasons other than expiration.
DiscAuthFailed	Indicates the number of received FA Element TLVs for which authentication was attempted and failed on the identified port.
AsgnReceived	Indicates the number of I-SID/VLAN bindings received in FA I-SID/VLAN Assignment TLVs on the identified port.
AsgnAccepted	Indicates the number of I-SID/VLAN bindings from received FA I-SID/VLAN Assignment TLVs that are accepted (activated) on the identified port. This counter is incremented when the binding transitions from a non-accepted state such as 'pending'or 'rejected' to the accepted state.
AsgnRejected	Indicates the number of I-SID/VLAN bindings from received FA I-SID/VLAN Assignment TLVs that are rejected on the identified port. This counter is incremented when the binding transitions from a non-rejected state such as 'pending' or 'accepted' to the rejected state.
AsgnExpired	Indicates the number of I-SID/VLAN bindings from received FA I-SID/VLAN Assignment TLVs that have expired on the identified port. This counter is not incremented when bindings are deleted for reasons other than expiration.
AsgnDeleted	Indicates the number of I-SID/VLAN bindings from received FA I-SID/VLAN Assignment TLVs that have been deleted on the identified port. This counter is only incremented when bindings are deleted for reasons other than expiration.
AsgnAuthFailed	Indicates the number of received FA I-SID/VLAN Assignment TLVs for which authentication was attempted and failed on the identified port.

Displaying Fabric Attach statistics summary

About this task

Use the following procedure to view FA statistics summary.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Edit**.
2. Click **Fabric Attach**.
3. In the work area, click the **Stats Summary** tab.

4. Select the **ClearGlobalErrorCounters(Summary)** check-box to clear the global error counters.

Variable definitions

Use the data in the following table to use the **Stats Summary** tab.

Name	Description
ClearGlobalErrorCounters(Summary)	Clears the global error counters.
DiscElemReceived	Indicates the number of FA Element TLVs received on the identified port.
DiscElemExpired	Indicates the number of discovered FA elements from received FA Element TLVs that have expired on the identified port. This counter is not incremented when elements are deleted for reasons other than expiration.
DiscElemDeleted	Indicates the number of discovered FA elements from received FA Element TLVs that have been deleted on the identified port. This counter is only incremented when elements are deleted for reasons other than expiration.
DiscAuthFailed	Indicates the number of received FA Element TLVs for which authentication was attempted and failed on the identified port.
AsgnReceived	Indicates the number of I-SID/VLAN bindings received in FA I-SID/VLAN Assignment TLVs on the identified port.
AsgnAccepted	Indicates the number of I-SID/VLAN bindings from received FA I-SID/VLAN Assignment TLVs that are accepted (activated) on the identified port. This counter is incremented when the binding transitions from a non-accepted state such as 'pending'or 'rejected' to the accepted state.
AsgnRejected	Indicates the number of I-SID/VLAN bindings from received FA I-SID/VLAN Assignment TLVs that are rejected on the identified port. This counter is incremented when the binding transitions from a non-rejected state such as 'pending' or 'accepted' to the rejected state.
AsgnExpired	Indicates the number of I-SID/VLAN bindings from received FA I-SID/VLAN Assignment TLVs that have expired on the identified port. This counter is not incremented when bindings are deleted for reasons other than expiration.
AsgnDeleted	Indicates the number of I-SID/VLAN bindings from received FA I-SID/VLAN Assignment TLVs that have

Table continues…

Name	Description
	been deleted on the identified port. This counter is only incremented when bindings are deleted for reasons other than expiration.
AsgnAuthFailed	Indicates the number of received FA I-SID/VLAN Assignment TLVs for which authentication was attempted and failed on the identified port.