Fabric Attach Client Variants Specification

Fabric Attach feature

Release Information	
Release	1.4
Feature Number	
CR Number	
Author/Editor	Extreme Networks, Roger Lapuh
Review	Extreme Networks, Ludovico Stevens

General Information

Note

This specification is preliminary and subject to change.

Summary:

This document serves as the requirements specification and functional description of the Fabric Attach feature for third party IoT Clients.

Feature Highlights:

- Allows attachment of non-SPB stations to a SPB network through a Fabric Attach Server
- Automatically map IoT devices to a pre-defined ISID/NSI based on the FA Client type.
- Leverages FA ZTC functionality.

Contents

Introduction

Overview

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

Fabric Attach Client Overview

Fabric Attach (FA) Client functionality may be supported by Extreme Networks devices, as well as by 3rd-party developed devices, that are capable of understanding and processing FA message/signaling data in the form of Extreme FA LLDP extensions. Several variants of an FA Client may be supported. Client device capabilities and the overall goals being targeted through FA Client connectivity determine the appropriate level of FA Client support that is required.

Four FA Client variants can be supported:

1. Basic
2. Basic Secured
3. Advanced
4. Advanced Secured

The characteristics of each FA Client variant are presented in the following sections. The variants are categorized based on the capabilities they support and transitioning to a different variant is as simple as enabling new functionality. To get things started, a quick overview of the core FA functionality is warranted.

Fabric Attach Operational Overview

To "extend" the fabric edge, the VLAN/I-SID service binding concept needs to be supported on non-SPBM devices. These FA devices pass this data to attached SPBM nodes where the mappings are processed and accepted or rejected. Specific actions to establish network paths are taken on the non-SPBM devices, referred to as FA Proxy and FA Client elements, as well as on the SPBM device, referred to as a FA Server, based on the outcome of the binding (i.e., service) "request" processing.

The FA Server, the FA Proxy and the FA Client are currently the three types of FA devices that comprise the FA ecosystem.

The FA Server is a fully-qualified SPBM device connected directly to the SPB fabric. One (or more) FA Proxy elements are connected to the FA Server through uplinks. FA Clients connect to a FA Server or a FA Proxy through standard access ports (non MAC-in-MAC). If deployed, FA Proxy acts as an external client proxy for the FA Client by passing client data (i.e., I-SID/VLAN binding requests) to the FA Server.

Fabric Attach Element Discovery

The first stage of establishing FA connectivity involves element discovery. A Fabric Attach agent resides on all FA-capable (i.e., Server/Proxy/Client) devices and advertises its capabilities (i.e., acting as a FA Server, a FA Proxy or specific type of FA Client) and current state through LLDP packets. A new organizationally specific Extreme Networks TLV, the FA Element TLV, has been defined to export FA element type and state data.

Fabric Attach Service Request Advertisement (not applicable to most IoT devices)

Following discovery, a FA agent is aware of all FA services currently provided by the network components to which it is directly connected. Based on this information, a FA Client agent can determine whether Fabric Attach service request data, namely locally configured or downloaded (e.g., from an orchestration manager) I-SID/VLAN assignments, should be exported to a FA Proxy or a FA Server.

Responses received from a FA Proxy/Server allows a FA Client to update network settings to support access to the requested services. It should be noted that there is no requirement that a FA Client support I-SID/VLAN binding configuration and service request advertisements. A compliant FA Client can simply rely on the upstream FA Proxy or FA Server to automatically update network settings based on client presence and FA Client-specific configuration data present on those devices.

FA Message Sequencing

FAC= Fabric attach Client, FAS = Fabric Attach Server

The FAC requests approval for each I-SID/VLAN mapping it has configured (simultaneously) from the FAS.

When the FAC is enabled, the FAS must approve each configured mapping.

Both the FAC and FAS will send element TLV's over LLDP at their respective LLDP announcement interval when they are enabled. When the FAC sees a valid FAS element TLV, it will continually send an assignment TLV (possibly containing more than one mapping) over LLDP. Initially, the status for each mapping is "assignment pending", but once the FAS accepts the mapping the status changes to "assignment accepted".

Similarly, the FAS must continually send out responses to the FAC's assignment TLV. The FAS is responsible for accepting or rejecting each mapping.

As stated above, all LLDPDU's are sent from both FAS and FAC at the LLDP announcement interval.

Timeout

A timeout occurs when:

- the FAC fails to see any element TLV's from FAS after 60s

the system ID inside the element TLV changes (and it isn't the first time receiving this TLV)

When a timeout occurs, all mappings previously accepted by the FAS go back to pending.

Fabric Attach LLDP Extensions

The new Fabric Attach TLVs are implemented as extensions to the LLDP standard, using its flexible extension mechanism. They are implemented as vendor-specific (Extreme OUI: 00-04-0D) TLVs using TLV type 127 as described in the 802.1ab (LLDP) standard. TLVs supporting the exchange of FA element data (i.e., the FA Element TLV) and I-SID/VLAN binding data (i.e., the I-SID/VLAN Assignment TLV) have been defined.

The FA Element TLV must be implemented by FA Clients wishing to join the FA ecosystem through FA signaling. The I-SID/VLAN Assignment TLV is optional, as other mechanisms are available on FA Proxy and FA Server devices to configure client access to various services.

Extreme FA Element TLV

This Extreme Networks proprietary TLV is used by FA elements to advertise their Fabric Attach capabilities. This data forms the basis for FA element discovery.

TLV format:

TLV Type **[127]**	TLV Length **[50 octets]**	Extreme OUI **[00-04-0D]**	Subtype **[11]**	HMAC-SHA Digest	Element Type	State	Mgmt VLAN	Rsvd	System ID
7 bits	9 bits	3 octets	1 octet	32 octets	6 bits	6 bits	12 bits	1 octet	10 octets

FA Element TLV data integrity and source validation is supported through the use of the HMAC-SHA256 message authentication algorithm. The HMAC-SHA256 generated digest size is 32 octets and the FA Element TLV includes a field to support the digest exchange between source and destination parties. Symmetric private keys are used for digest generation.

The HMAC-SHA256 digest is computed for the Element Type data (i.e., data for the digest computation starts at [0-based] byte 38 of the TLV) through the last octet of the System ID (i.e., [0-based] byte 51 of the TLV for a total of 14 bytes). This data, along with the message authentication key, is passed through the standard HMAC-SHA256 algorithm to produce the associated message digest. The digest is then placed in the HMAC-SHA256 Digest field in the TLV prior to transmission. Upon receipt, the digest is again computed and the resulting digest is compared against the received digest. If the received digest is the same as the newly computed digest, the TLV is considered authentic and processing can commence. If the comparison fails, the TLV is discarded and processing may be terminated.

FA Element TLV authentication **can be bypassed** on FA Proxy and FA Server devices to support FA Clients that do not support the required authentication procedure. Disabling FA message authentication on FA Proxy and FA Service devices

means that FA Element TLV authentication is not performed. In this scenario the FA Client does not need to compute the digest. If FA communication is occurring between non-secure systems, the HMAC-SHA256 Digest data should always be zero and the digest data, regardless of the value, is ignored.

A number of FA Element Type values, including the primary FA Proxy, FA Server and several FA Client element types, are currently defined. The list of supported element types will expand as additional devices incorporate FA signaling.

Currently supported Fabric Attach Element Type values:

- FA Element Type - Other (1)
- FA Server (2)
- FA Proxy (3)
- FA Server No Authentication (4)
- FA Proxy No Authentication (5)
- FA Client - Wireless Access Point Type 1 (6) [wireless clients get direct network attachment]
- FA Client - Wireless Access Point Type 2 (7) [wireless clients get tunneled to a controller]
- FA Client - Switch (8)
- FA Client - Router (9)
- FA Client - IP Phone (10)
- **FA Client - IP Camera (11)**
- FA Client - IP Video (12)
- FA Client - Security Device (13) [FW, IPS/IDS, etc.]
- FA Client – Virtual Switch (14)
- FA Client – Server/Endpoint (15)
- FA Client – ONA SDN(16)
- FA Client – ONA SPB-over-IP(17)
- FA Proxy ISW RingV2 (18)
- FA Client – Building security/access (19)
- FA Client – PDU/battery backup (20)
- FA Client – PoE lighting (21)
- FA Client – Nutanix server solution (22)
- FA Client – Placeholder 1 (23)
- FA Client – Placeholder 2 (24)

- FA Client Unknown (63)

The FA Element Type indicates the capabilities of the advertising agent. A FA Proxy is a non-SPBM device that supports I-SID/VLAN assignment definition and, if connectivity permits, has the ability to advertise these assignments for possible use by a FA Server. A FA Server is a SPBM device that potentially accepts externally generated I-SID/VLAN assignments that can be used for automated configuration purposes.

A FA Client is a non-SPBM device that may support some form of I-SID/VLAN service request (i.e., binding) definition and, if connectivity permits, has the ability to advertise this data to a directly connected FA Proxy (providing an external client proxy service) or FA Server. Tagged (i.e., all traffic is tagged) and untagged (i.e., a mix of tagged and untagged traffic may be generated) FA Client connections are supported.

> Note: IoT FA Client types such as Cameras do not have to signal VLAN/I-SID bindings to the FA-Server, but the FA-Server can instead leverage the Zero-Touch-Client functionality which by default assigns a FA-client to a VLAN/ISID based on its Client type. This ensures that all FA clients of the same type are joining the same broadcast domain enabling a zero-touch deployment.

FA Element TLV State field settings indicate FA Client link tagging requirements in FA Client-sourced frames and current provisioning mode information in FA Proxy and FA Server-sourced messages (bits are numbered left to right):

- Link VLAN Tagging Requirements (bit 1)
  - 0 – All traffic tagged on link
    - Egress tagging mode on connected FA Proxy/FA Server set to ‘tagAll’
  - 1 – Tagged and untagged traffic on link
    - Egress tagging mode on connected FA Proxy/FA Server set to ‘untagPvidOnly’
- Automatic Provisioning Mode (bits 2/3)
  - 0 – Automatic provisioning disabled
  - 1 – SPB provisioning

- 2 – VLAN provisioning

Management VLAN data can be included in FA Server and FA Proxy-sourced frames to support management VLAN auto-configuration on downstream FA Client devices.

The FA Element System ID conveys connection information that the TLV recipient can use for multi-factor authentication purposes and to enforce connectivity restrictions. This 10 octet system/connection identifier is formatted as follows:

- System MAC Address (6 octets)
  - Chassis MAC (standalone/stack)
  - Virtual BMAC (SPB/SMLT configuration)
- Connection Type Indication (3 bits)
  - 0 – Unit/Port, 1 – MLT, 3 – SMLT, 4 - IfIndex
- Connection ID (29 bits - right-justified value)
  - Unit (0/standalone, 1..8/stack [1 octet]), Port (1..MaxPort [1 octet])
  - MLT/SMLT ID
  - IfIndex

The FA Element TLV can only exist once in a LLDPDU. The FA Element TLV length is fixed at 52 bytes.

Extreme Networks FA I-SID/VLAN Assignment TLV (not required for IOT devices)

This Extreme Networks proprietary TLV is used by a FA Client to advertise service requests (i.e., I-SID/VLAN assignments) that it would like supported by a FA Proxy and/or by a FA Server. It is also used by the complementary FA entity (i.e., directly connected FA Proxy/Server) to export status data pertaining to the I-SID/VLAN assignments that it has considered for installation.

TLV format:

TLV Type **[127]**	TLV Length **[41-506 octets]**	Extreme OUI **[00-04-0D]**	Subtype **[12]**	HMAC-SHA Digest	Assignment Status	VLAN	I-SID
7 bits	9 bits	3 octets	1 octet	32 octets	4 bits	12 bits	3 octets

I-SID/VLAN Assignment TLV data integrity and source validation is supported through the use of the HMAC-SHA256 message authentication algorithm. The HMAC-SHA256 generated digest size is 32 octets and the FA I-SID/VLAN Assignment TLV includes a field to support the digest exchange between source and destination parties. Symmetric private keys are used for digest generation.

The FA I-SID/VLAN Assignment TLV can only exist once in a LLDPDU. It is only included in a LLDPDU when complementary FA element (i.e., FA Server/Proxy/Client) devices are directly connected. Per-port TLV transmission flags must be enabled on the communicating devices as well. The FA Element TLV must also be present in the LLDPDU for the FA I-SID/VLAN Assignment TLV to be processed. The TLV will not exceed the LLDP 511 byte TLV size limit, which implies a maximum of 94 I-SID/VLAN assignments in a LLDPDU.

The HMAC-SHA256 digest is computed for the series (1 – 94) of I-SID/VLAN assignments (i.e., data for the digest computation starts at [0-based] byte 38 of the TLV). The digest is then placed in the HMAC-SHA256 Digest field in the TLV prior to transmission. Upon receipt, the digest is again computed for the series (1 – 94) of I-SID/VLAN assignments in the received TLV and the resulting digest is compared against the received digest. If the received digest is the same as the newly computed digest, the TLV is considered valid and processing can commence. If the comparison fails, the TLV is discarded and processing is terminated.

If FA communication is occurring between non-secure systems, the HMAC-SHA256 Digest data should always be zero and the digest data, regardless of the value, is ignored. A misconfiguration can occur with one system operating in secure mode and the other operating in non-secure mode. In this scenario, the I-SID/VLAN Assignment TLV will always be discarded prior to processing by the system operating in secure mode.

Fabric Attach Client Service Request Status Processing

All I-SID/VLAN assignments in service requests generated by a FA Client start in the ‘pending’ state (status value ‘pending(1)’). This state is updated based on the results of upstream FA device request processing. If an assignment is accepted, its state is updated to ‘accepted’ (status value ‘accepted(2)’). A service request may also be rejected. In this case, the assignment state is updated to ‘rejected’ (status value ‘rejected(3)’ or greater). This request status information is used by the FA Client to drive processing of service request (i.e., I-SID/VLAN Assignment TLV) responses received by the FA Client from the upstream FA Proxy/Server.

Fabric Attach Client Variants

Four FA Client variants are defined, each of which have different implementation requirements and support different levels of FA connectivity.

Basic FA Client (use case IoT/Camera)

The basic FA Client supports only FA Element TLV processing and does not support FA signaling authentication. Support for I-SID/VLAN binding configuration or download (i.e., from a management entity) is not required.

Requirements/capabilities:

- Must generate a well-formed FA Element TLV containing
    - Valid FA Element type data
    - Valid FA state information (e.g., traffic tagging requirements)
    - A System ID containing the device MAC address
- May process received FA Element TLV data including
    - Connected FA element device type/operational mode (FA Proxy/FA Server)
    - Upstream FA management VLAN data

A basic FA Client is suitable for environments in which port security, specifically source authentication, is not a priority and where FA device service requirements (i.e., required I-SID/VLAN associations) are controlled by upstream devices. Implementation requirements are minimal.

Basic Secured FA Client

The basic secured FA Client supports only FA Element TLV processing and does support FA signaling authentication. Support for I-SID/VLAN binding configuration or download (i.e., from a management entity) is not required.

Requirements/capabilities:

- Must generate a well-formed FA Element TLV containing
    - Valid FA Element type data
    - Valid FA state information (e.g., traffic tagging requirements)
    - A System ID containing the device MAC address
- Must support generation of a HMAC-SHA256 digest using message authentication key material and out-bound FA Element TLV data
- May process received FA Element TLV data including
    - Connected FA element device type/operational mode (FA Proxy/FA Server)
    - Upstream FA management VLAN data
- May support message authentication key configuration and in-bound TLV authentication

A basic secured FA Client is suitable for environments in which port security, specifically source authentication and possibly data integrity, is a priority. Security support is required on the FA Client. Otherwise the implementation requirements are minimal.

Advanced FA Client

An advanced FA Client supports both the FA Element TLV and the FA I-SID/VLAN Assignment TLV. Support for FA signaling authentication is not available. Support for I-SID/VLAN binding configuration or download (i.e., from a management entity) is likely required. The ability to initiate actions based on received status information related to advertised service requests (i.e., I-SID/VLAN bindings) is also expected, though is not mandatory.

Requirements/capabilities:

- Must generate a well-formed FA Element TLV containing

    - Valid FA Element type data
    - Valid FA state information (e.g., traffic tagging requirements)
    - A System ID containing the device MAC address
- Must generate a well-formed FA I-SID/VLAN Assignment TLV based on hardcoded or configured service request data (i.e., I-SID/VLAN bindings)
- May process received FA Element TLV data including
    - Connected FA element device type/operational mode (FA Proxy/FA Server)
    - Upstream FA management VLAN data
- May process received FA I-SID/VLAN service request response data by
    - Configuring networks settings due to service request acceptance
    - Reporting/logging upstream service request processing issues

An advanced FA Client is suitable for environments in which port security, specifically source authentication and data validation, is not a priority. The targeted deployment environment does require the FA Client have the ability to signal service requirements to upstream FA Proxy and FA Server devices. Advanced FA Clients represent a step-up in terms of implementation complexity when compared to basic FA Clients.

Advanced Secured FA Client

An advanced secured FA Client supports both the FA Element TLV and the FA I-SID/VLAN Assignment TLV. Support for FA signaling authentication is available as well. Support for I-SID/VLAN binding configuration or download (i.e., from a management entity) is likely required. The ability to initiate actions based on received status information related to advertised service requests (i.e., I-SID/VLAN bindings) is also expected, though is not mandatory.

Requirements/capabilities:

- Must generate a well-formed FA Element TLV containing
    - Valid FA Element type data
    - Valid FA state information (e.g., traffic tagging requirements)
    - A System ID containing the device MAC address
- Must generate a well-formed FA I-SID/VLAN Assignment TLV based on hardcoded or configured service request data (i.e., I-SID/VLAN bindings)
- Must support generation of a HMAC-SHA256 digest using authentication key material and
    - Out-bound FA Element TLV data
    - Out-bound FA I-SID/VLAN Assignment TLV data
- May process received FA Element TLV data including
    - Connected FA element device type/operational mode (FA Proxy/FA Server)
    - Upstream FA management VLAN data
- May process received FA I-SID/VLAN service request response data by
    - Configuring networks settings due to service request acceptance
    - Reporting/logging upstream service request processing issues
- May support message authentication key configuration and in-bound TLV authentication

An advanced secured FA Client is suitable for environments in which port security, specifically source authentication and data integrity, is a priority. The targeted deployment environment also requires the FA Client have the ability to signal service requirements to upstream FA Proxy and FA Server devices. Security support is required on the FA Client.

- **Message authentication and integrity protection**

Message authentication is supported for all FA TLV exchanges through the use of a keyed-hash message authentication code (HMAC) that is computed for, and transmitted with, the FA TLV data. The standard HMAC-SHA256 algorithm is used to calculate the message authentication code (i.e., digest) involving a cryptographic hash function (SHA-256) in combination with a shared secret key.

When FA message authentication is enabled, the (pre) configured FA key is used to generate a HMAC digest that is included in the FA TLVs. 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 silently ignored (FA I-SID/VLAN Assignment TLV) or processed but marked “authentication-failed” (FA Element TLV).

For convenience, element type data, exported in the FA Element TLV, is updated to reflect the message authentication status (e.g., enable/disabled) to allow attached FA Clients to determine whether or not message authentication is required for communication with the source FA Proxy or FA Server.

A symmetric key (i.e., a key known by both source and destination parties) is required to support this functionality. A default key is defined such that secure communication is available out-of-the-box. Both the FA secure communication setting (i.e., enabled/disabled if the option is available) and the symmetric key are administrator-configurable. This data is maintained across resets and restored during FA initialization.

In addition to FA device data authentication using multiple keys, authentication failure processing is enhanced to provide greater visibility and flexibility with regard to handling authentication failure scenarios. Information related to authentication failures is passed to the EAP/NEAP agent for forwarding to a FA policy server for potential processing if:

- The interface on which the FA Client is discovered is EAP/NEAP enabled or
- 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 are provided for additional upstream client processing, if desired.

Glossary

Glossary

FA – Fabric Attach
HMAC – Hash-based Message Authentication Code
I-SID – Backbone Service Instance Identifier [IEEE 802.1ah]
LLDP – Link Layer Discovery Protocol
LLDPDU – Link Layer Discovery Protocol Data Unit
MAC-in-MAC – MAC-in-MAC frame encapsulation
SHA – Secure Hash Algorithm
SPB – Shortest Path Bridging
SPBM – Shortest Path Bridging MAC-in-MAC