53-1004236-01
February 2016

Campus Fabric

Solution Design Guide

Contents

Preface

Overview

A typical campus or large branch network includes several buildings with multiple floors and dozens of access switches. Those switches connect devices like IP phones, PCs, and wireless access points to the network. As new technologies and changing demands test the limits of traditional networks, administrators must meet their current needs and address future ones by implementing network infrastructures that will adapt to their changing needs.

Brocade Campus Fabric is a solution that cuts unnecessary network layers to create large management domains that eliminate individual switch touch points, reducing maintenance time and costs. This solution enables a single point of control, configuration, and management across distribution and access layer switches, intensely simplifying design, deployment, and operation of enterprise campus networks. It creates a single network touch point and single configuration across distribution and access layer switches, ultimately driving simplified operations, distribution layer features at the access layer with no additional licenses, in turn driving down total cost of ownership (TCO). This document discusses the campus fabric architecture, components, packet walks, and value proposition.

This solution design guide provides design guidance for network professionals who are looking for a flexible and robust campus infrastructure with a solution that simplifies the network by providing provisioning and operational simplicity.

Purpose of This Document

This document highlights purpose-built features, components, and the architecture of the Brocade Campus Fabric solution, which is intended to simplify enterprise network operations and management.

Audience

This document is written for network designers, network architects, and network engineers who are looking for architectural reference information about the Brocade Campus Fabric solution.

Objectives

The objective of this document is to provide design guidance that can apply to a variety of enterprise campus networks. Enterprise campus networks can span diverse physical configurations, from small networks to wide-area networks with multiple locations. We'll focus on the requirements of the campus, which, unlike the data center, must support a variety of devices across a wider geographic area. The objective is to give customers a solution that provides a simplified network infrastructure and centralized control and data management.

Related Documents

- Campus Fabric SPX Demo Video
- Transforming the Network with Brocade Campus Fabric: At a Glance
- Brocade FastIron Switch Port Extender Deployment Guide
- Switch Port Extender Configuration Guide (under the FI 08.0.40 product page)
- Campus Fabric FAQ (under the FI 08.0.40 product page)

Acronyms

Acronym	Description
CB	control bridge
PE	port extender
SPX	Switch Port Extender
ECID	E-Channel Identifier
QoS	Quality of Service
ACL	access control list
STP	Spanning Tree Protocol
VLAN	virtual LAN

About Brocade

Brocade networking solutions help the world's leading organizations transition smoothly to a world where applications and information reside anywhere. This vision is realized through the Brocade One™ strategy, which is designed to deliver key business benefits such as unmatched simplicity, non-stop networking, application optimization, and investment protection.

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

To help ensure a complete solution, Brocade partners with world-class IT companies and provides comprehensive education, support, and professional services offerings.

To learn more, visit www.brocade.com.

Introduction

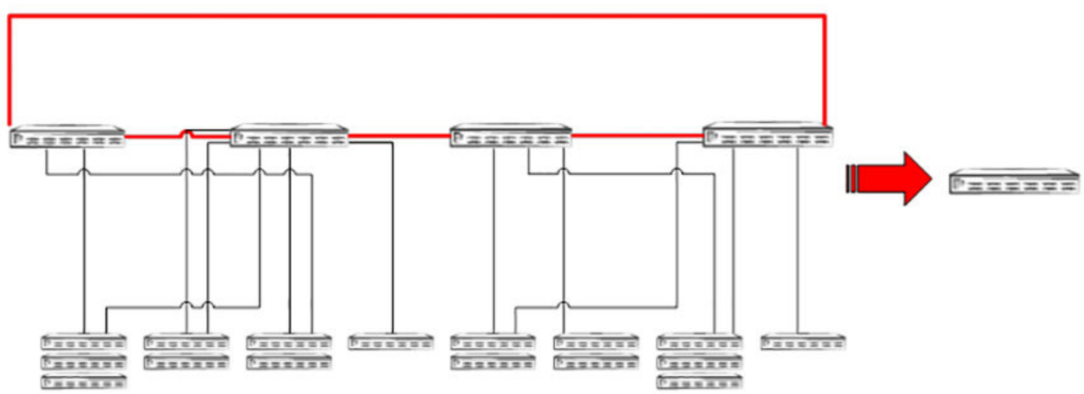
Brocade Campus Fabric provides a solution to encompass multiple network layers into a single logical device, flattening the network and eliminating deployment complexity and arbitrary network segmentation between office floors, buildings, and other enterprise locations. The solution is based on open standards: IEEE 802.1BR - Bridge Port Extension technology, internally termed as Switch Port Extender. Switch Port Extender technology integrates premium, mid-range, and entry-level switches to create a distributed chassis that collapses the network access, aggregation, and core layers into a single domain that shares services. It significantly reduces management touch points and network hops across the entire campus network.

The Brocade Campus Fabric solution provides the following benefits that impact Total Cost of Ownership (TCO):

- Single network touch point for configuration and management
- STP-free Layer 2 design
- Policy and feature inheritance
- Rich and consistent ICX 7xxx Series feature set across distribution and access layers
- No license required to run SPX
- Standards-based (IEEE 802.1BR)

The following figure shows a single point of management and control for a 16-access-switch distribution block.

FIGURE 1 Centralized Point of Control and Data Management



With the Brocade FastIron 08.0.40 release, the Campus Fabric solution supports:

- 768 ports across 16 access clients (16 X 48 X 1G ports)
- Up to 4 core/distribution switches in a stack (4 X 48 X 10G + 12 X 40G ports)

Comparison Between Traditional Campus Design and Campus Fabric Design

Consider the topology outlined in the figure "Traditional Campus Deployment." The topology includes a 1008-port traditional campus network with 16 access switches and a bulky chassis at the core/distribution layer.

This campus requires:

- 6 devices for configuration management
- 6 devices for image management
- 6 separate configurations, including SNMP, NTP, VLAN database, management IP, gateway, and host name
- An expensive chassis

As shown in the figure "Campus Fabric Deployment," with Brocade Campus Fabric, the same 1008-port campus requires only:

- 1 device to manage
- A distributed architecture with chassis-like performance
- No image management at the access switches
- A single configuration for SNMP, NTP, VLAN database, management IP, gateway, and host name

FIGURE 2 Traditional Campus Deployment

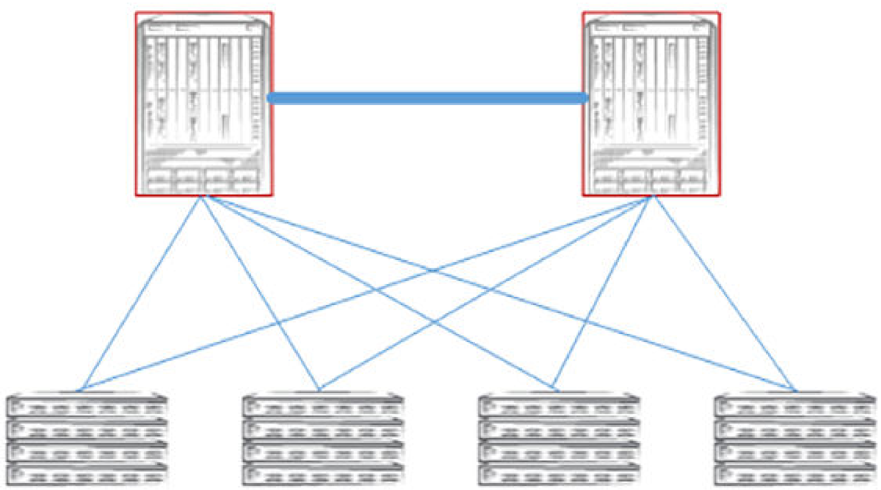
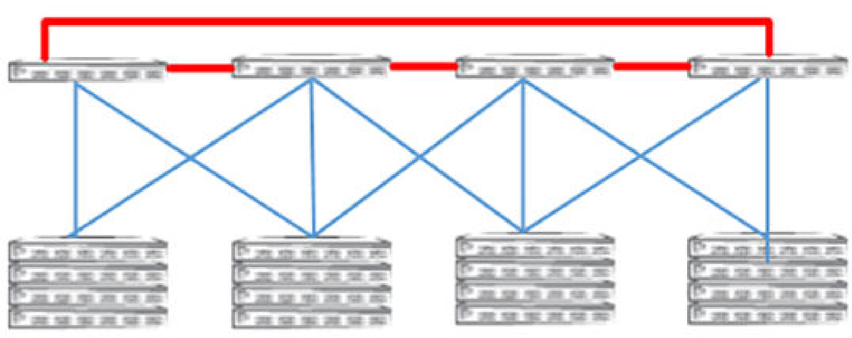


FIGURE 3 Campus Fabric Deployment



Building Blocks

The Brocade Campus Fabric solution has two components: a control bridge and port extenders.

Control Bridge

The control bridge in the Brocade Campus Fabric is an ICX 7750 switch operating in standalone or stacking mode. Brocade FastIron 8.0.40 supports up to four ICX 7750 switches in a stack. The ICX 7750 is premium high-density hardware with 10G and 40G ports. Detailed product information can be found here.

The control bridge is the brain of the complete Switch Port Extender topology. The active unit of the control bridge stack is the point of management and control for the complete 1008-port network. The data and control packets from all distribution and access switches are forwarded to the control bridge and are then processed for further action.

The power of a "distributed chassis" is now extended to the Switch Port Extender, allowing the control bridge to manage all access clients from one location despite the geographical distribution of the switches. Competitive chassis-based solutions require a significant up-front investment because the large chassis-based control bridge, which represents the core of the solution, is expensive to acquire and maintain. Brocade takes the architecture to the next level by offering a distributed chassis-based solution as the aggregation/core control bridge, including a "pay as you grow" model that allows customers to start small and upgrade as needs grow.

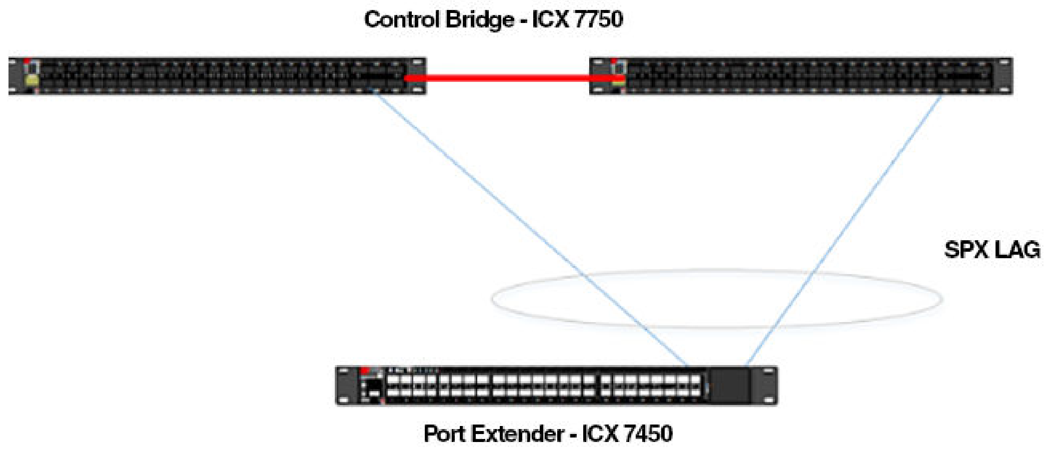
Port Extender

The port extender (PE) is the access switch in the Brocade Campus Fabric solution. Brocade FastIron 8.0.40 supports the Brocade ICX 7450 Switch as a port extender unit. The switches can be directly connected to the control bridge, or they can be connected in chain. The maximum number of chained PE units is 4 (in FI 8.0.40). The ICX 7450 is a stackable switch that can operate in both traditional and port extender modes. The ICX 7450 delivers the performance, flexibility, and scalability required for enterprise Gigabit Ethernet (GbE) access deployment. Detailed product information can be found here.

The ICX 7450 switches in port extender mode connect to the control bridge using 10G or 40G ports. The ICX 7450 in port extender mode can be managed through the ICX 7750 control bridge with centralized packet switching on the control bridge only.

The ICX 7450 can operate in traditional switching mode, and it can also be configured as a Switch Port Extender client switch. As seen in the figure that follows, the switches can be connected in a chain. The hosts connect to the base/access PE. A PE that is not an access PE aggregates transmissions from downstream PEs and is called a *transit PE*. The downstream ports on the PE units are called *virtual ports (VPs)*.

FIGURE 4 Building Blocks of Brocade Campus Fabric



Brocade Campus Fabric Architecture

A control bridge (CB) and a port extender (PE) are the building blocks of a Campus Fabric; and an ICX 7750 stack or an ICX 7750 standalone unit serves as the IEEE 802.1BR CB for attached ICX 7450 units configured as PE units. The PE units provide connectivity to PCs, laptops, IP phones, and other access devices. The CB communicates with the attached PE units downstream using protocols defined in the IEEE 802.1BR standards. PE units in the extended topology tag packets from attached user devices and send the packets upstream to the CB for switching and network management.

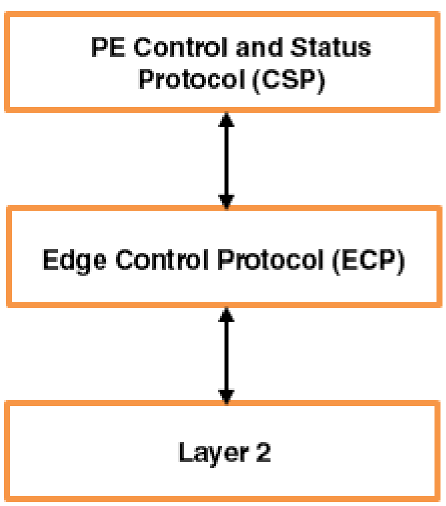
The following are the main components of the Switch Port Extender architecture:

Link Layer Discovery Protocol (LLDP)—The CB uses LLDP to discover PE units. When the CB discovers a PE unit, it connects to the PE unit and creates a control plane using the Control and Status Protocol (CSP) over the uplink/cascade port. Each PE port is managed as a virtual port from the CB perspective. The CB sets up each PE unit for traffic forwarding and creates multicast and unicast forwarding tables through CSP.

Control and Status Protocol (CSP)—CSP runs between the CB and attached PE units; it is used to bring the PE units up or down. PE CSP executes as an upper layer protocol over the Edge Control Protocol (ECP). CSP handles configuration management, metrics, and status of port extender switches.

Edge Control Protocol (ECP)—Port Extender Control and Status Protocol is transported over Edge Control Protocol (ECP). ECP runs on top of LLDP at Layer 2 and provides ACK and Retransmit responses. Port Extender Control and Status Protocol packets are prioritized, enabling repeatability if command or response is lost.

FIGURE 5 Switch Port Extender Protocol Hierarchy



E-tag—802.1BR adds an E-tag to every packet that traverses between the port extender and the control bridge. The E-tag header enables the port extender switch to behave like a remote switch, allowing client host ports to appear as logical interfaces at the control bridge switch. The communication is on a bidirectional path between the external virtual port and the corresponding internal virtual port. E-channels are identified by an E-Channel ID (ECID) in the E-tag (ranges from 0x0001 to 0x3FFF). E-channels can be point-to-point, point-to-multipoint, or multipoint-to-point.

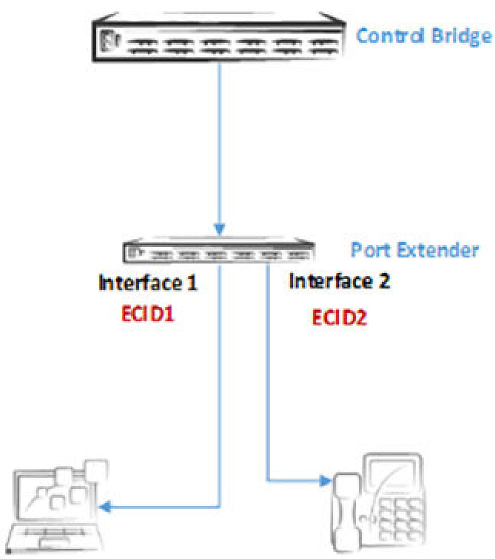
FIGURE 6 ECID Frame

<table>
<tr><td colspan="4">Ethertype
(16 bits)</td></tr>
<tr><td colspan="2">PCP
(3 bits)</td><td>DEI</td><td>Ingress ECID
(12 bits)</td></tr>
<tr><td>Resv
(2 bits)</td><td colspan="3">ECID
(14 bits)</td></tr>
<tr><td colspan="4">Reserved
(16 bits)</td></tr>
</table>

- PCP and DEI are used for traffic class selection.
- The source ECID contains the identifier of the port extender port that sourced this frame. The port extender filters the frame from this port.
- The ECID indicates the E-channel on which this frame is transmitted.
- ECIDs are 14 bits. The first 4k of the range is reserved for E-channels that contain a single virtual port used for the default ECID of the port. Thus the Ingress ECID field requires only 12 bits.

As shown in the figure that follows, a unique ECID is added to each virtual port during initialization. The packet traversing each virtual port is identified by the unique ECID on the control bridge. The transit PE does not modify the ECID on the packet; it is modified only at the control bridge.

FIGURE 7 ECID Assignment



E-tag	Virtual Port
ECID 1	Interface 1
ECID 2	Interface 2

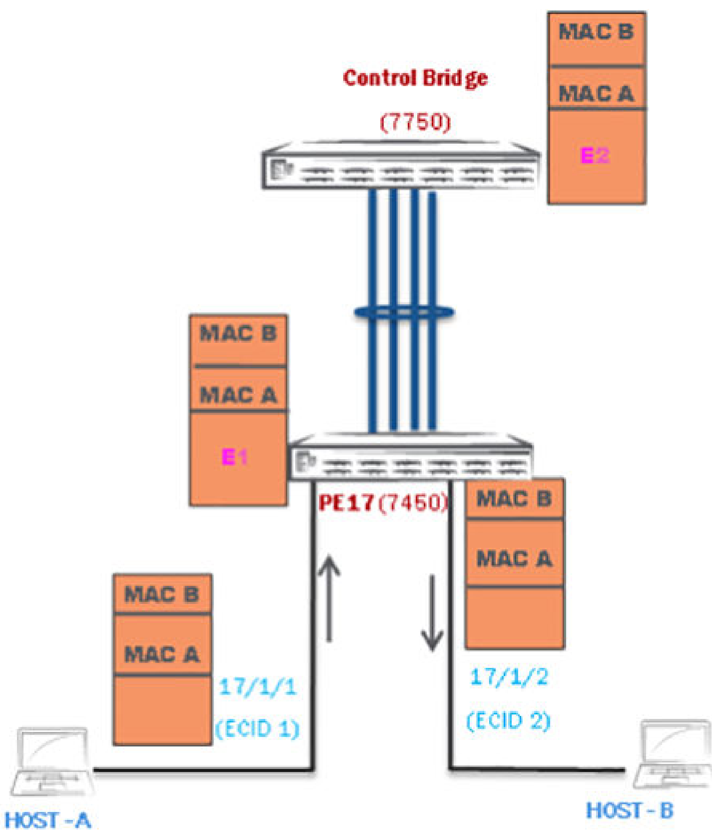
- Automatically Assigned
- One Unique ECID to Each Host Port

Packet Walkthrough

To understand the data forwarding in the Brocade Campus Fabric solution, the following is an example of a packet walk. In this example, we assume that Host A pings Host B.

1. A regular Ethernet frame arrives from Host A to port extender unit number 17 on virtual port 17/1/1.
2. The ingress Ethernet frame is encapsulated with an E-tag header with assigned ECID 1.
3. A packet with the E-tag header arrives at the SPX port at the control bridge and is decapsulated of the header. The MAC learning happens at the control bridge after E-tag decapsulation. The control bridge looks up the destination port and encapsulates the packet with ECID 2 for destination port 17/1/2.
4. The packet then forwards to the port extender unit, which checks for the destination port and removes ECID 2 from the packet.
5. The packet reaches Host B without any E-tag encapsulation.

FIGURE 8 Data Forwarding in a Switch Port Extender Topology

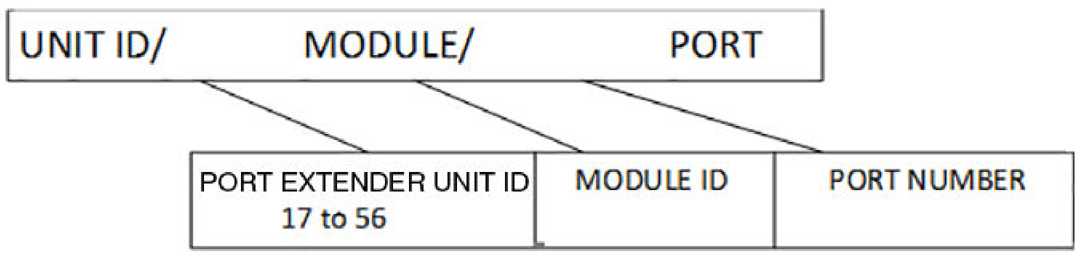


Campus Fabric Solution Capabilities

Virtual Interface Numbering

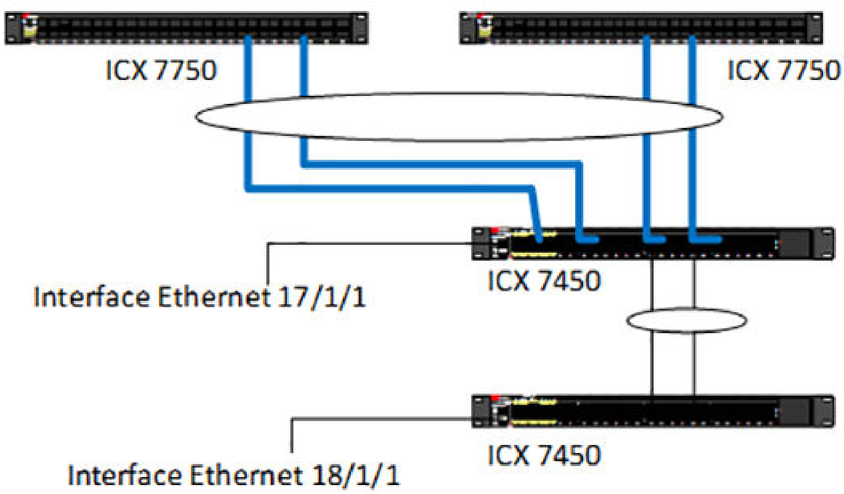
The Campus Fabric solution provides a single point of control and data management. The port number assignment for a virtual port is very consistent with the existing stacking interface numbering in ICX products. In the FastIron 08.0.40 release, the port extender units are assigned a unit ID from 17 to 56. Unit IDs 1 through 16 are reserved for the control bridge stack units.

FIGURE 9 Virtual Port Interface Numbering



For example, as indicated in the figure that follows, the interface on ICX 7450 in port extender mode is configured as 17/1/1. The port on PE chain unit 18 is numbered as 18/1/1.

FIGURE 10 Interface on Port Extender Units



Each physical port on a port extender unit is a logical interface that can be managed and controlled by the control bridge.

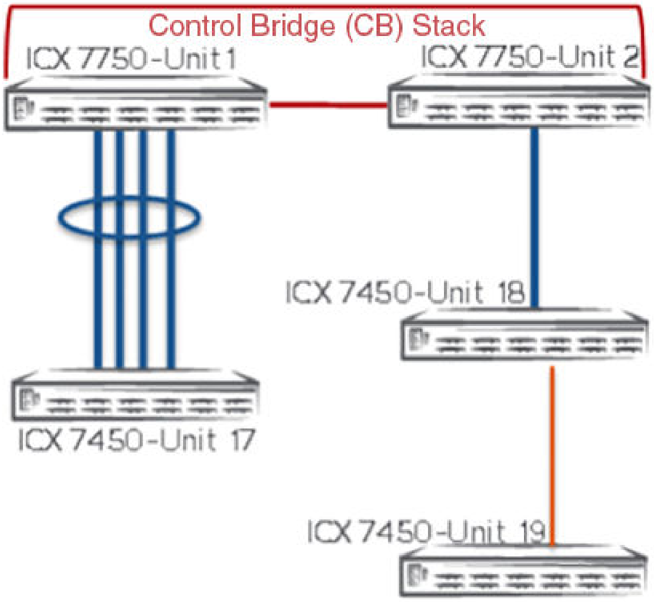
```
ICX7750-48F Router(config)# show interface ethernet 17/1/1
GigabitEthernet17/1/1 is Up, line protocol is Up
  Port Up for 26 day(s) 23 hour(s) 35 minute(s) 28 second(s)
  Hardware is GigabitEthernet, address is cc4e.2489.b088 (bia cc4e.2489.b088)
  Configured speed auto, actual unknown, configured duplex fdx, actual unknown
  Configured mdi mode AUTO, actual unknown
  Member of L2 VLAN ID 1, port is untagged, port state is BLOCKING
  BPDU guard is Disabled, ROOT protect is Disabled, Designated protect is Disabled
  Link Error Dampening is Disabled

  STP configured to ON, priority is level0, mac-learning is enabled
  Openflow is Disabled, Openflow Hybrid mode is Disabled, Flow Control is config
disabled, oper disabled
  Mirror disabled, Monitor disabled
  Mac-notification is disabled
  Not member of any active trunks
  Not member of any configured trunks
  No port name
  IPG MII 96 bits-time, IPG GMII 96 bits-time
  MTU 1500 bytes, encapsulation ethernet
  MMU Mode is Cut-through
  300 second input rate: 0 bits/sec, 0 packets/sec, 0.00% utilization
  300 second output rate: 0 bits/sec, 0 packets/sec, 0.00% utilization
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 multicasts, 0 unicasts
  0 input errors, 0 CRC, 0 frame, 0 ignored
  0 runts, 0 giants
  0 packets output, 0 bytes, 0 underruns
  Transmitted 0 broadcasts, 0 multicasts, 0 unicasts
  0 output errors, 0 collisions
  Relay Agent Information option: Disabled
UC Egress queues:
Queue counters    Queued packets    Dropped Packets
         0                 0                  0
         1                 0                  0
         2                 0                  0
         3                 0                  0
         4                 0                  0
         5                 0                  0
         6                 0                  0
         7                 0                  0
MC Egress queues:
Queue counters    Queued packets    Dropped Packets
         0                 0                  0
         1                 0                  0
         2                 0                  0
         3                 0                  0
```

Operational Simplicity

Similar to traditional stacking, the complete topology can be derived using the **show spx** command. The following output from this command shows that PE unit ID 17 is connected to the unit 1 control bridge and that unit 18 and unit 19 are connected in a chain to unit 2 of the control bridge stack.

FIGURE 11 Operational Simplicity with Campus Fabric




```
ICX7750-48F Router(config)# show spx
T=26d23h46m20.1: alone: standalone, D: dynamic cfg, S: static
ID   Type          Role    Mac Address    Pri State   Comment
1   S ICX7750-48XGF active  cc4e.246d.4980 128 local   Ready
2   S ICX7750-48XGC standby cc4e.2438.6f00 128 remote  Ready
17 S ICX7450-48P    spx-pe  cc4e.2489.b088 N/A remote  Ready
18 S ICX7450-48GF   spx-pe  cc4e.2489.c448 N/A remote  Ready
19 S ICX7450-24P    spx-pe  cc4e.2489.d570 N/A remote  Ready

   standby      active
   +---+        +---+
2/4| 2 |2/1--2/1| 1 |2/4
   +---+        +---+

            +----+
 1/1/48--2/1| 17 |
            +----+

            +----+        +----+
  2/3/1--4/1| 18 |2/3--2/3| 19 |2/1-
            +----+        +----+
```

For easier administration and monitoring, the user can assign a name to the cascade port that is connected to a PE unit or PE chain. The system can print the unit details based on the assigned name.

```
ICX7750-48F Router(config)# spx cb-configure
ICX7750-48F Router(config-spx-cb)# spx-port 2/3/1 pe-group PE-CHAIN-18-19
ICX7750-48F Router(config-spx-cb)# show spx pe-group PE-CHAIN-18-19
Show PEs attached to pe-group PE-CHAIN-18-19 (port 2/3/1)
T=26d23h56m51.6: alone: standalone, D: dynamic cfg, S: static
ID   Type          Role    Mac Address    Pri State   Comment
1   S ICX7750-48XGF active  cc4e.246d.4980 128 local   Ready
2   S ICX7750-48XGC standby cc4e.2438.6f00 128 remote  Ready
18 S ICX7450-48GF   spx-pe  cc4e.2489.c448 N/A remote  Ready
19 S ICX7450-24P    spx-pe  cc4e.2489.d570 N/A remote  Ready

    standby      active
    +---+        +---+
  2/4| 2 |2/1--2/1| 1 |2/4
    +---+        +---+
            +----+        +----+
  2/3/1--4/1| 18 |2/3--2/3| 19 |2/1-
            +----+        +----+
```

Pre-provisioning of Port Extender Switches

Pre-provisioning the Switch Port Extender switch configuration before physical installation is supported. Once a PE switch is connected, the pre-provisioned configurations are applied to the port extender host ports automatically, further simplifying deployment. A network administrator can pre-provision port extender switches from the network distribution layer and have the PE switches installed and cabled locally by anyone who does not need to be networking savvy.

The following is an example where PE unit 20 is added to the control bridge configuration without physically connecting it.

```
ICX7750-48F Router(config-spx-cb)# spx unit 20
ICX7750-48F Router(config-spx-unit-20)# module
  DECIMAL   Module number
ICX7750-48F Router(config-spx-unit-20)# module 1 icx7450-24p-poe-port-management-
module
ICX7750-48F Router(config-spx-unit-20)# module 2 icx7400-xgf-4port-40g-module
ICX7750-48F Router(config-spx-unit-20)# module 3 icx7400-qsfp-1port-40g-module
ICX7750-48F Router(config-spx-unit-20)# module 4 icx7400-qsfp-1port-40g-module
ICX7750-48F Router(config-spx-unit-20)# spx-port 20/2/1
ICX7750-48F Router(config-spx-unit-20)# spx-port 20/2/3
```

As soon as the switch is pre-provisioned, the virtual ports show up in the running configuration, which can be applied without physically connecting them.

```
ICX7750-48F Router(config)# vlan 200
ICX7750-48F Router(config-vlan-200)# tagged e 20/1/1

SYSLOG: <14> Jan 28 00:22:09 VLAN: Id 200 added by un-authenticated user from
console session.
Added tagged port(s) ethe 20/1/1 to port-vlan 200.
ICX7750-48F Router(config-vlan-200)# vlan 201
ICX7750-48F Router(config-vlan-201)# tagged e 20/1/2

SYSLOG: <14> Jan 28 00:22:19 VLAN: Id 201 added by un-authenticated user from
console session.
Added tagged port(s) ethe 20/1/2 to port-vlan 201.


ICX7750-48F Router(config-vlan-201)# show run
Current configuration:
!
!
vlan 200 by port
 tagged ethernet 20/1/1
 no spanning-tree
!
vlan 201 by port
 tagged ethernet 20/1/2
 no spanning-tree
```

When the user physically connects the device to the topology, the host port configuration automatically applies to all host ports that were pre-provisioned, making the deployment smooth and error-proof.

Scalability with the Campus Fabric Solution

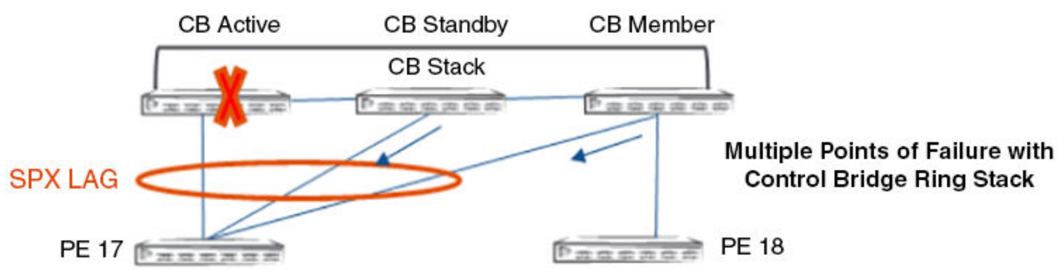
The Brocade Campus Fabric solution released in FastIron 08.0.40. The following table describes the hardware and software scalability for FastIron 08.0.40.

Scalability Parameter	Scalability Limit	Notes
Number of virtual ports	768	16 X 48-port ICX 7450.
Maximum number of port extender units	16	
Maximum PE unit chain length	4	
Maximum number of control bridge stack units	4	
Maximum VLANs for virtual ports	4 (including default VLAN)	Flexible mode to support 16 VLANs for 128 ports.
Maximum Layer 2 IGMP groups	512	
Maximum number of directly attached PEs to the CB	8	PE can connect in chain to support a maximum of 16 PE units per Campus Fabric network.

High Availability

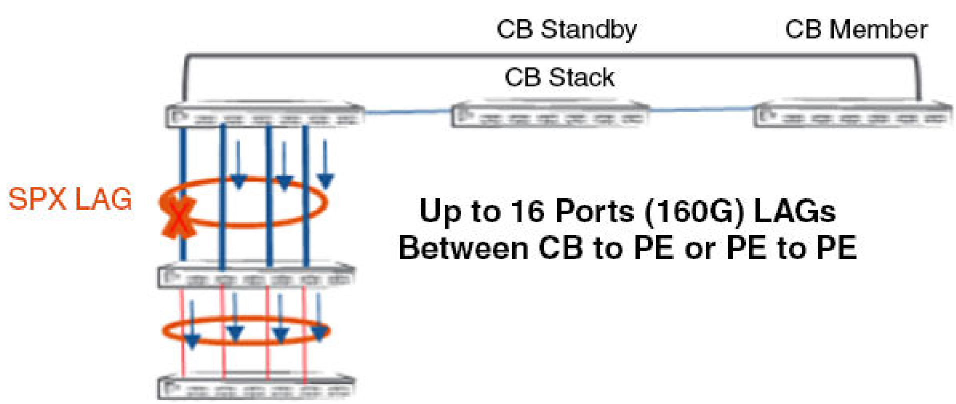
The Campus Fabric solution provides multiple levels of resiliency. At the distribution/core level, the control bridge supports Brocade FastIron stacking, providing multiple levels of high availability. With the control bridge's four stack units, the port extender should be multihomed, connected to CB units in a LAG to provide high availability and load balancing. The control bridge stack units also support a ring topology for hitless failover in case of physical failure.

FIGURE 12 High Availability with CB Ring Stack and SPX LAG



The port extender units can be connected in a chain, and each chained unit can be connected via a 16-port LAG. The SPX LAG provides resiliency and load balancing for the data traffic from the host devices.

FIGURE 13 High Availability for PE Chain Units with LAG



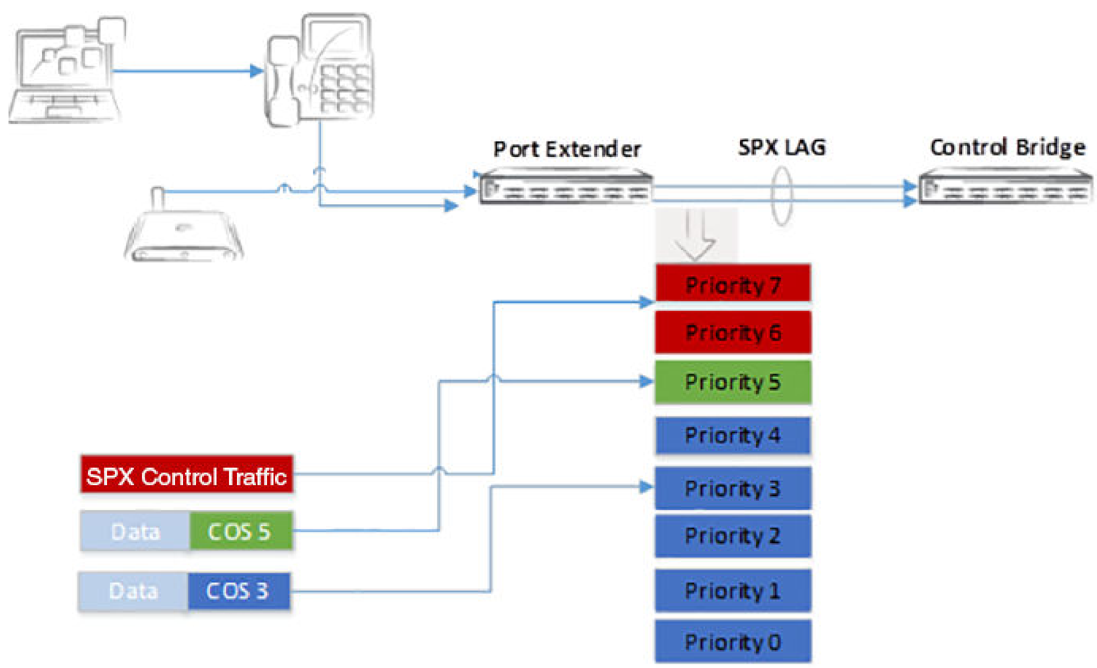
Quality of Service

A Switch Port Extender client supports up to eight traffic classes per port with values from 0 to 7. Packets with higher priority classifications are given precedence for forwarding.

Port extender ports (virtual ports) are capable of supporting interface classification based on Class of Service (CoS), Differentiated Services Code Point (DSCP), and port priority. Quality of Service (QoS) over the SPX link is strictly based on the DSCP/CoS values of the ingress packets. The control bridge and port extender maintain a default DSCP-to-Queue map and CoS-to-Queue map, which are the basis of queuing packets appropriately over the priority queue or the standard queue on SPX interfaces.

As the following figure shows, any IP packet marked with COS=5 is queued to priority queue 5, and any IP packet marked with COS=3 is queued to standard queue 3. All SPX control traffic is sent over the priority queue 6 or 7 to ensure that communication between the control bridge and port extender switch is not lost due to congestion.

FIGURE 14 Quality of Service at Campus Fabric



Security Features

The Switch Port Extender solution in the FastIron 08.0.40 release supports the following security features:

- Layer 2 access control lists
  - MAC filters
- Layer 3 access control lists
  - IPv4 ingress ACLs
  - IPv6 ingress ACLs
  - IPv4 outbound ACLs
  - IPv6 outbound ACLs
- Outbound ACLs for CPU traffic
- DSCP remarking
- PCP remarking

Port extender ports are capable of supporting ACL classifications based on packet headers. The classification by port extender edges is carried in the E-tag across the cascading and uplink links. ACL-based QoS marking is supported at the port extender host port level and is honored by the CB forwarding engine.

Auto Image Download and Upgrade

Auto image download and upgrade for the Switch Port Extender switches is supported in a Campus Fabric solution. Similar to the support in FastIron stacking switches, when a Switch Port Extender switch connects to the control bridge directly or through a PE chain, the control bridge's active unit checks for the image details and automatically upgrades the switch with the latest image version running on the control bridge stacking units.

This mechanism is already supported on the stacking units for the patch upgrades between major releases, and the support is now extended to the Campus Fabric solution.

Automatic Execution of Commands in Batches

The batch file create and execute feature has been added to the FastIron feature set in the 08.0.40 release. This feature is supported in the Campus Fabric solution as well. A batch file is a container of configurations or policies that can be applied to the switch. All batch templates are customizable and easily modified. Users can create multiple templates and assign them to a device to run instantly or at a specific time based on the NTP clock. Detailed information about this feature can be found here.

Batch file templates are easy to use, as demonstrated in the following output. They can be statically applied using the Batch <buffer> <execute> command in the CLI.

```
Brocade(config)# batch buffer 1 &
Enter TEXT message, End with the character '&'.
show memory
show users
show version
show cpu
show memory
show flash
show version
show memory
show users
show memory
show users
ICX(config)# execute batch <id> <now> <after> <at> <cancel> <Begin>

Brocade# execute batch 1 now
   To execute batch id 1 at a particular time:
Brocade# execute batch 1 at  04:05:00 04-22-15
   To execute batch id 1 after a particular time period:
Brocade# execute batch 1 after 03:07:04
   To cancel the scheduled execution of commands on batch id 1:
Brocade# execute batch 1 cancel
```

Consistent and Reliable Feature Set

The following are the software features supported on the Brocade Campus Fabric solution in FastIron release 08.0.40.

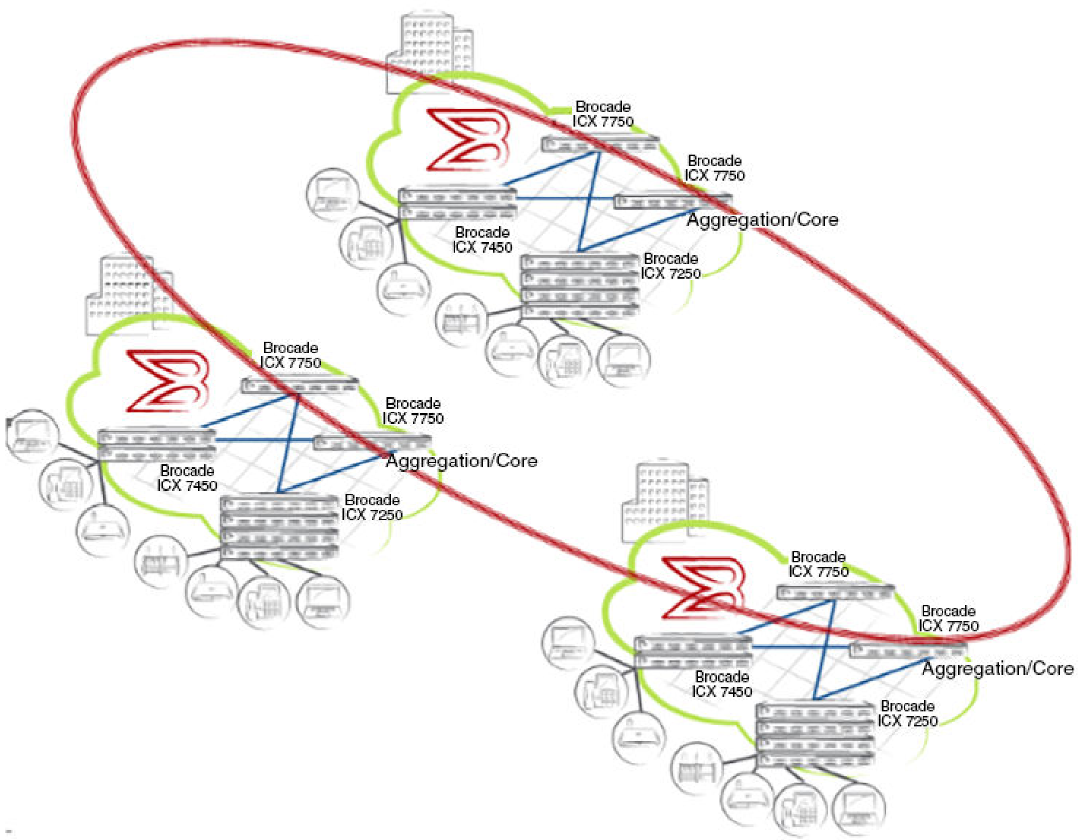
Technology	Details
Administration	Software features (port name, speed, NTP, etc.), FDP, CDP, LLDP, network monitoring, operations, administration, maintenance, PoE, SNMP, syslog, image management.
Layer 2	VLAN, rapid STP, BPDU guard, root guard, dynamic MAC learning, static MAC, L2 jumbo, static LAG, dynamic LAG (LACP), port mirroring and monitoring, error disable and recovery.
Layer 3	Static routing, IPv4, IPv6, etc., static ARP, route loop prevention, route only support, routing protocols like BGP, OSPF, RIP, VRRP/VRRP-E.
Multicast	IGMP v1, v2, v3, IGMPv3 fast leave, IGMP proxy, static multicast routes and groups, IP multicast reduction, MLD snooping.
Security	MAC filter, IPv4/v6 ACLs, rules-based IP ACLs (inbound, outbound), security access, SSH2, and SCP.
SPX Infrastructure	Unit ID assignment, topology validation, spx-lag.
Traffic Management (QoS)	QoS (.1p, diffServ, strict priority, WRR) (on PE ports), user-configurable scheduler profiles, ACL statistics, CPU rate limiting.

Conclusion

The Brocade Campus Fabric solution centralizes the data, control, and management planes, making the network easier to manage and troubleshoot. The solution also provides rich and premium software features.

Mission-critical client applications require multiple data ports with high bandwidth, high availability, and premium software support. A Campus Fabric architecture with centralized configuration and management for multiple devices at the access layer provides a scalable model to keep up with a growing campus topology over time.

FIGURE 15 Brocade Effortless Campus Network with the Campus Fabric Solution



To summarize a few benefits of Campus Fabric:

- Centralized point of configuration and management
- Consistent and reliable features across distribution and access
- Distributed architecture with "pay as your grow" model
- Standards-based solution (802.1BR)

The Campus Fabric solution enables customers to build and expand robust, cost-effective, and business-optimized campus networks that meet both current and future corporate requirements. Auto image management and operational simplicity provide a seamless network deployment at a great value.