Active Fabric Manager
Deployment Guide 1.5

2013 - 05

Rev. A0X

Contents

1 Introduction

Active Fabric Manager (AFM) is a graphical user interface (GUI) based network automation and orchestration tool that allows you to design, build, deploy, and optimize a Layer 3 distributed core and Layer 2 Virtual Link Trunking (VLT) fabric for your current and future capacity requirements. This tool helps you simplify network operations, automate tasks, and improve efficiency in the data center. AFM supports Dell Networking S4810, S4820T, S55, S60, MXL blade, and Z9000 switches.

Problem: Challenges to Build a Fabric in the Data Center

- How do you design the fabric?
- What kind of switch do you buy?
- Who is going to use Visio to manually document the fabric (which switch ports connect to another switch).
- Who is going to draw the cables?
- How will I ensure that this fabric design is accurate?
- Who is going to update the fabric design as I change it or expand it?
- Who is going to configure every switch in the fabric and what kind of errors can happen because this is manually performed?
- How do I keep track of software versions on each switch?
- Who is going to validate every switch in the fabric to verify that they have the correct version of software and configuration and are physically connected to the right switch.

Solution: Active Fabric Manager

Automated Fabric Design	Automated Configuration	Automated Deployment	Automated Validation
• Design Templates • Capacity Planner • Automated fabric expansion • Auto documentation (PDF) • Draws fabric topology • Draws table of switch port connections	• No CLI commands. • No need to manually configure each switch. • Automatically configures every switch in the fabric.	Automatically deploys each switch in the fabric based on the design.	• Automatically validates each switch in fabric. • Accelerates data center deployment.

2

About AFM

Active Fabric Manager (AFM) is a graphical user interface (GUI) based network automation and orchestration tool that allows you to design, build, deploy, and optimize a Layer 3 distributed core and Layer 2 VLT fabric for your current and future capacity requirements. This tool helps you simplify network operations, automate tasks, and improve efficiency in the data center.

NOTE: Before you begin, review the Getting Started page. For information about the AFM workflow, see Flowchart for Designing and Deploying a Fabric. To learn how to install the AFM, including instructions on completing the Initial Setup, see the *Active Fabric Manager Installation Guide*.

- Getting Started
- Fabric Designer Wizard
- Pre-deployment Wizard
- Deploying the Fabric
- Alerts
- Administration
- Performance Management

3

Getting Started

This section contains the following topics:

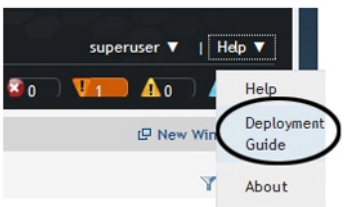
- Designing and Deploying the Fabric
- Flowchart for Designing and Deploying a Fabric

Related links:

- Supported Fabrics
- Designing the Fabric
- AFM Site Map

NOTE:

You can view the *Active Fabric Manager Deployment Guide* in the AFM by selecting the **Deployment Guide** option from the **Help** pull-down menu in the upper right of the screen.



Designing and Deploying a Fabric

This section provides an overview of the steps required to design and deploy a fabric, including the information you need before you begin.

After you complete the basic installation of the Active Fabric Manager (AFM), you must configure it. This is done using the **Getting Started** configuration wizard at the **Home** > **Getting Started** screen. After you complete the installation process, the AFM automatically launches this wizard. The **Getting Started** configuration wizard provides launch points for designing, pre-deploying, and deploying the fabric. Review the steps in the wizard and the online help or (*AFM Deployment Guide*) before you begin. With this wizard, you can also edit and expand an existing fabric design and import an existing design.

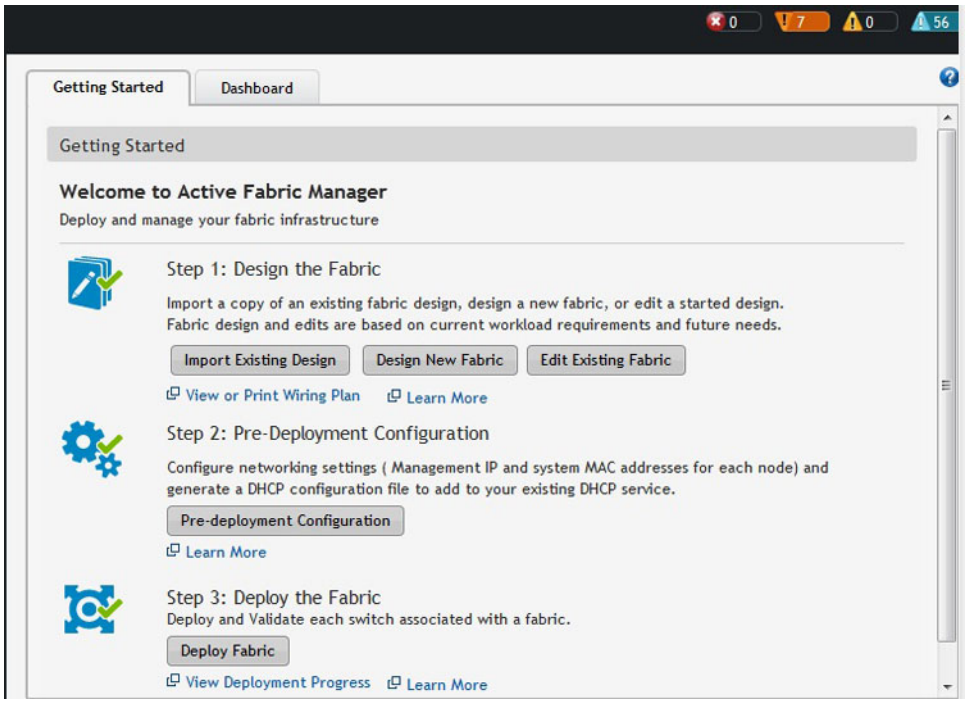


Figure 1. Getting Started Wizard

To design and deploy a Layer 2 VLT or layer 3 distributed core fabric.

1. Gather useful information.

   Related links.

   - Gather Useful Information for Layer 2 VLT Fabric
   - Gathering Useful Information for a Layer 3 Distributed Core Fabric.

2. Design the fabric.

   Related links designing a Layer 2 VLT fabric:

   - Overview of VLT
   - Key Considerations fo Designing a VLT Fabric
   - Selecting a VLT Fabric

   Related links for designing a Layer 3 distributed core fabric:

   - Overview of a Distributed Core
   - Terminology
   - Designing a Distributed Core
   - Selecting a Distributed Core Design

3. Build the physical network.
4. Configure the following settings:

   - TFTP/FTP

  - SNMP
  - CLI Credentials
5. Prepare the Fabric for Deployment
6. Deploy and Validate the Fabric
7. Validate the deployed fabric against the fabric design.
8. Monitor the fabric health and performance. See Performance Management.

NOTE: To provision the fabric, enter the Dell Networking operating system (FTOS) CLI user's Credentials and enable the configuration credential for all the switches in the fabric. For information about this topic, see CLI Credentials.

CAUTION: If you are using a switch that has already been deployed, reset its factory settings in the fabric. The switch must be in Bare Metal Provision (BMP) mode.

Designing and Deploying a Fabric Flowchart

The following flowchart shows how to design and deploy a new fabric.

Figure 2. Designing and Deploying a Fabric Flowchart

4

AFM Site Map

To help you navigate the AFM user interface use the following site map.

Home	Getting Started Wizard Step 1: Design the Fabric Step 2: Pre-Deployment Configuration Step 3: Deploy the Fabric	Dashboard			
Network Level	Summary Map Network View Graphical and Tabular View	Alerts and Events Current Historical	Performance Average Bandwidth Utilization Link Usage Switch Statistics	Design Fabric New Fabric Edit Fabric Delete Fabric View Wiring Plan	
Fabric Level	Summary Fabric View	Alerts and Events Current Historical	Performance Average Bandwidth Utilization Link Usage Switch Statistics	Maintenance Software Updates Backup and Restore	Configure and Deploy Fabric **Deploy Fabric** Pre-deployment Configuration Deploy and Validate View DHCP Configuration Errors CLI Configuration View DHCP configuration files Manage Templates Associate Templates Custom Configuration View Custom Configuration History View Wiring Plan
Switch Level	Summary Device View Graphical and Tabular View	Alerts and Events Current Historical	Performance Switch and Port Real-time and Historical data	Troubleshooting Ping SSH Traceroute Telnet	Replace a Switch Decommission Switch Pre-deployment Replacement Deploy Replacement

Jobs	Job Results	Schedule Jobs Backup Switch Configuration Files Update switch software Active Software	Data Collection Schedule data collection Edit threshold	Reports Create Edit Delete Duplicate Run	
Administration	Audit Log	Administration CLI Credentials Client Settings Data Retention Settings DHCP Server Settings NTP Server Settings Email Settings Syslog IP Addresses SNMP Configuration System Information TFTP/FTP Settings	User Accounts Add User Delete User Edit User Unlocking User	User Sessions Display active AFM users Terminate users' sessions	AFM Server Upgrade AFM Server Upgrade AFM Server Backup

5

Supported Fabric Types

The fabric design wizard templates define the basic configuration for a Layer 3 distributed core or Layer 2 VLT fabric.

- Use the Layer 3 distributed core fabric for large fabric deployments. For information about distributed core fabrics, see Conventional Core Versus Distributed Core and Selecting a Layer 3 Distributed Core Fabric Design.
- Use the Layer 2 VLT fabric for workload migration over virtualized environments. For information about Layer 2 fabrics, see VLT and Selecting a VLT Fabric Design.

To design a fabric based on the capacity requirements for your current and future needs, use the fabric design wizard at the **Network > Configure Fabric > Design New Fabric** screen. When you first start the AFM, it starts the **Getting Started** configuration wizard in the **Welcome to Active Fabric Manager** screen.

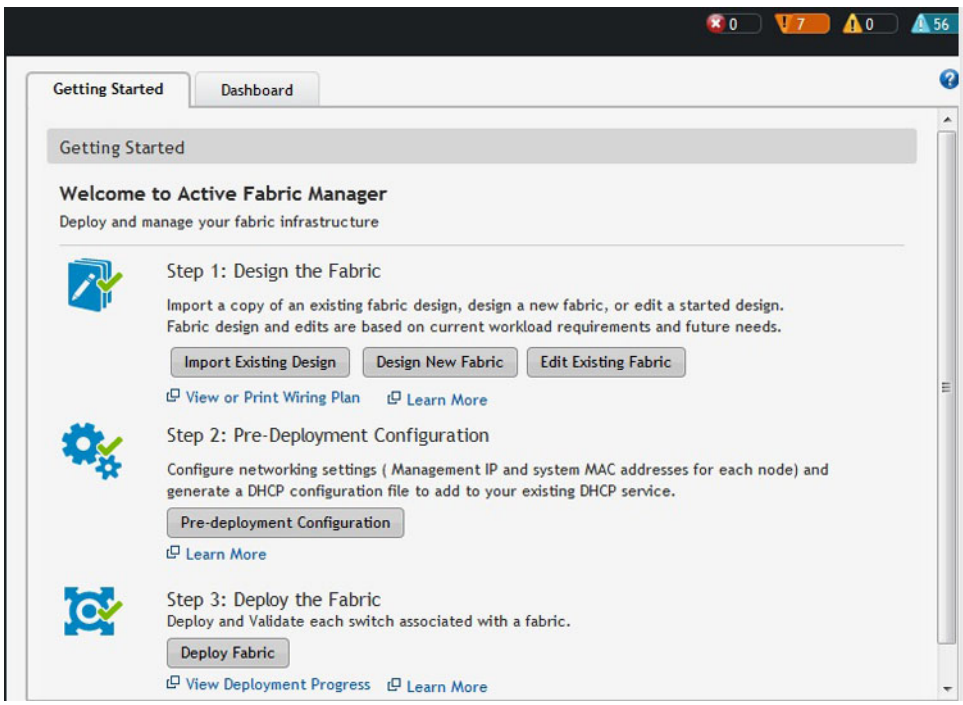


Figure 3. Getting Started: Welcome to Active Fabric Manager Screen

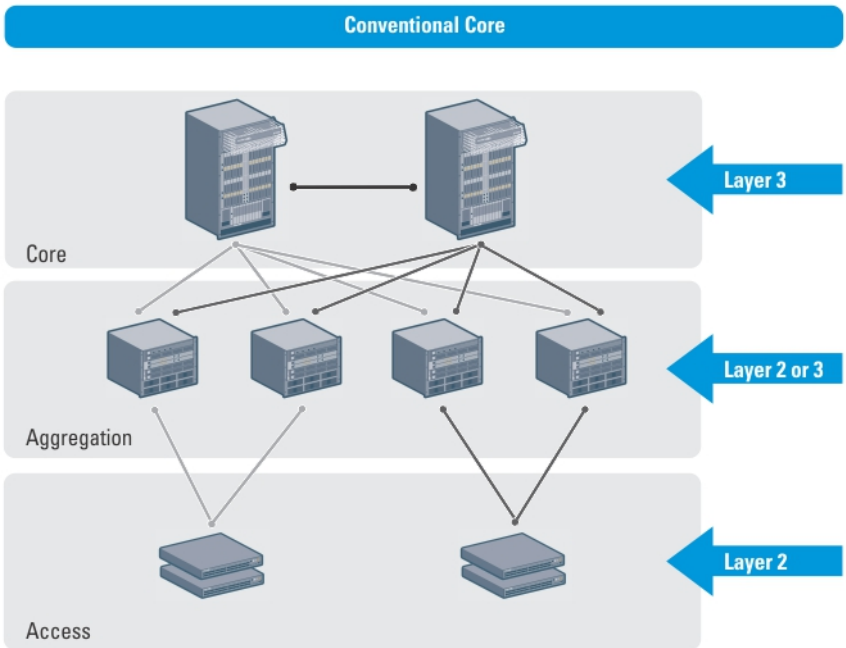
Conventional Core Versus Distributed Core

This section describes the differences between a conventional core and a distributed core.

Conventional Core

A conventional core is a three-tier network that is typically chassis based and is composed of the following:

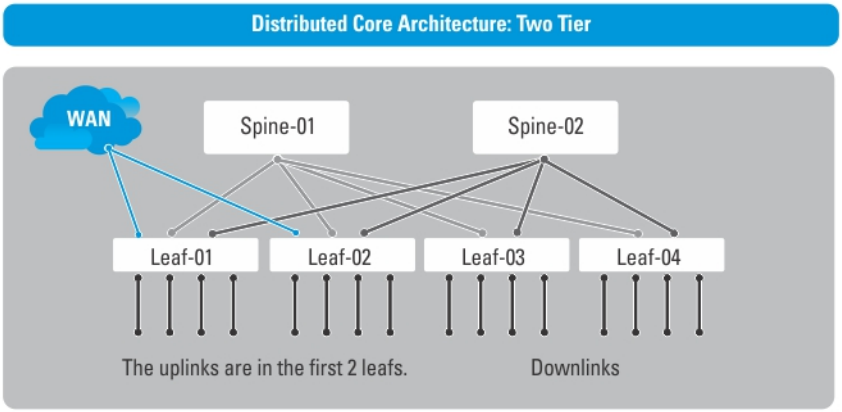
- Core — The core layer routes traffic to and from the internet and the extranet. Redundancy and resiliency are the main factors for high availability, which requires chassis-based core routers.
- Aggregation layer — The aggregation layer connects with top of rack (ToR) switches and aggregates the traffic into fewer high-density interfaces such as 10GbE or 40GbE. This layer aggregates the traffic to the core layer.
- Access layer (ToR) — The access layer typically contains ToRs. A ToR is a small form-factor switch that sits on top of the rack and allows all the servers in the rack to be cabled into the switch. A ToR has a small 1 to 2 rack unit (RU) form factor.



Distributed Core

A distributed core is a two-tier architecture composed of multiple switches interconnected to provide a scalable, high-performance network that replaces the traditional and aggregation layers in a conventional core. Switches are arranged as spines and leaves; the spines interlink (connect) the leaves together using a routing protocol. The leaves' edge ports connect to the switches, ToR switches, servers, other devices, and the WAN. The spines move traffic between the leaves bi-directionally, providing redundancy and load balancing. Together, the spine and leaf architecture forms the distribute core fabric.

This two-tier network design allows traffic to move more efficiently in the core at a higher bandwidth with lower latencies than most traditional three-tier networks. Because there is no single point of failure that can disrupt the entire fabric, the distributed core architecture is more resilient and as a result, there is less negative impact on the network when there is a link or node failure. The AFM views the distributed core as one logical switch.



NOTE: There are no uplinks on the spines. All the leaves have downlinks. The uplink should be configured in the first two leaves.

Key Advantages

The key advantages of a distributed core architecture are:

- Simplified fabric
- Higher bandwidth
- Highly resilient
- Higher availability
- Low power consumption
- Less cooling
- Lower latency
- Lower cost
- Less rack space
- Easier to scale

Distributed Core Terminology

The following terms are unique to the design and deployment of a Layer 3 distributed core fabric.

- Leaf — A switch that connects switch, servers, storage devices, or top-of-rack (TOR) elements. The role of the leaf switch is to provide access to the fabric. The leaf switch connects to all of spines above it in the fabric.
- Spine — A switch that connects to leaf switches. The role of the spine is to provide an interconnect to all the leaf switches. All the ports on the spine switches are used to connect the leaves, various racks together. The spines provides load balancing and redundancy in the distributed core. There are no uplinks on the spines.
- Edge ports — The uplinks and downlinks on the leaves.
- Uplinks — An edge port link on the first two leaves in the distributed core fabric that connects to the edge WAN, which typically connects to an internet server provider (ISP). Uplinks are always 10 GbE.

- Downlinks — An edge port link that connects the leaves to the data access layer; for example, servers or ToR elements. Downlinks are always 10 GbE.

  NOTE: Specify an even number of uplinks. The minimum number of uplinks is **2**. One uplink is for redundancy.

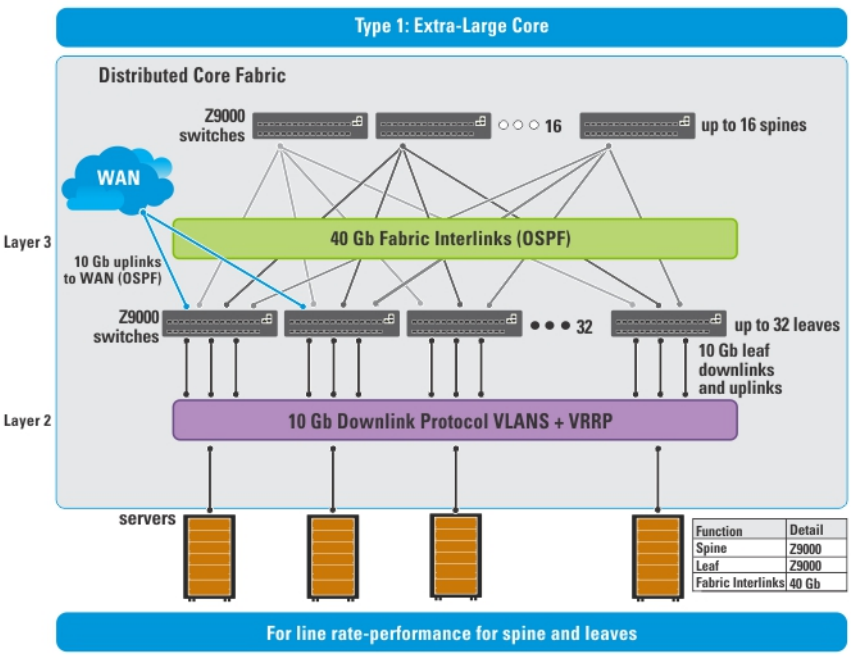
- Fabric Interlinks — Links that connect the spines to the leaves. The fabric interlink bandwidth is fixed: 40 GbE or 10 GbE.

- Fabric over-subscription ratio — Varies the maximum number of available interconnect links. This ratio determines the number of fabric interlinks (the number of communication links between the spine and leaf devices). The ratio that you specify depends on the bandwidth, throughput, and edge port requirements. The interlink over-oversubscription ratio does **not** come off the edge port downlinks.

  As you increase the fabric over-subscription ratio:

  - The total number of ports for the downlinks increases.
  - The number of interconnect links from the leaves to the spines decreases.
  - The maximum number of available ports increases.

  For non-blocking, line rate between the leaves and spines, use the 1:1 fabric over-subscription ratio. When you require a lot of bandwidth and not a lot of ports, use this ratio. The following image illustrates a distributed core fabric.



NOTE: The AFM does not configure or manage anything beyond the distributed core fabric.

Important: In a single distributed fabric, all the leafs can act as non-ToR or as a ToR, not both at the same time.

Key Considerations for Designing a Distributed Core

When designing the Layer 3 distributed core fabric, consider the following:

- You can deploy up to 10 fabrics. However, the fabrics do not communicate with each other.
- AFM manages Dell S4810 and Z9000 switches.

CAUTION: If you are already using a deployed switch, reset the factory settings. The switch must be in BMP mode.

For information on BMP, see Pre-Deployment – Step 7: DHCP Integration and the *FTOS Configuration Guide* for either the S4810 or Z9000 at https://www.force10networks.com/CSPortal20/KnowledgeBase/Documentation.aspx.

The number and type of spines and leaves (switches) in a distributed core fabric are based on the following:

- The type of distributed core fabric design:
  - Type 1: Extra Large Core
  - Type 2: Large Core
  - Type 3: Medium Core
  - Type 4: Small Core
- The number of current uplinks and downlinks for the leaves.
- The number of planned edge ports (future uplinks and downlinks) for the leaves.
- Whether you require non-blocking (line rate) performance.
- Whether the leaves act as a ToR or are connecting to a server.
- Fabric interlink bandwidth (the links between the spines and leaves).
- Uplinks and downlinks, which are always 10 GbE.
- When the Open Shortest Path First (OSPF) is selected for both uplinks and interlinks, one of the uplinks or interlinks must be in area 0. If one uplink is in area 0 then the interlinks must not be in area 0.
- The fabric over-subscription ratio.
- Fixed fabric interlink bandwidth that is based on the fabric type: 10 GbE or 40 GbE.

CAUTION: If you do not specify additional links in the fabric design for future expansion in the Port Specification screen:

- Any future expansion requires rewiring the hardware.
- IP addresses are not reserved.
- You might have to bring down the current switches to expand the fabric. For information about how to expand a fabric, see Editing and Expanding an Existing Fabric Design.

Gathering Useful Information for a Distributed Core

To gather the following useful information for a Layer 3 distributed core fabric before you begin:

- Obtain the .CSV file that contains the system MAC addresses, service tag, and serial numbers for each switch provided from Dell manufacturing or manually enter this information.
- Obtain the location of the switches, including the rack and row number from your network administrator or network operator.

- Obtain the Remote Trivial File Transfer Protocol (TFTP) / File Transfer Protocol (FTP) address from your network administrator or network operator.
- Download the software image for each type of switch in the fabric: S4810 or Z9000. Each type of switch must use the same version of the software image within the fabric. Place the software images on the TFTP/FTP site so that the switches can install the appropriate FTOS software image and configuration file. The AFM automatically copies the minimum configuration into the specified TFTP/FTP location. To specify a TFTP/FTP site, go to **Administration** > **Settings** screen. For information about which software packages to use, see the Release Notes.
- Obtain the Dynamic Host Configuration Protocol (DHCP) server address to be used for the fabric from your DHCP network administrator or network operator. If a remote DHCP server is not available, AFM also provides a local DHCP. The DHCP server must be in the same subnet where the switches are located. After you power cycle the switches, the switches communicate with the DHCP server to obtain a management IP address based on the system MAC address. The DHCP server contains information about where to load the correct software image configuration file for each type of switch from the TFTP/FTP site during BMP. For information about BMP, see Pre-Deployment – Step 7: DHCP Integration.
- Obtain pool of IP addresses for the management port for each switch in the fabric.
- Obtain IP addresses (2-8 addresses, must be an even number) for the uplink configuration from the ISP service.
- Obtain IP addresses for the downlink configuration for connecting to the server or ToR.
- Obtain IP addresses for the Fabric Interlink Configuration for the spine and leaf switches.
- Gather protocol configuration for uplinks, downlinks and fabric interlink configuration

Selecting a Layer 3 Distributed Core Fabric Design

For large fabric deployments, use the Layer 3 distributed core fabric. AFM supports the following distributed core fabric designs:

- Type 1: Extra Large Core Fabric
- Type 2: Large Distributed Core Fabric
- Type 3: Medium Distributed Core Fabric
- Type 4: Small Distributed Core Fabric

To select the appropriate Layer 3 distributed core fabric design, use the following table as a guide. For more information about a Layer 3 distributed core, see Overview of a Distributed Core and Key Considerations for Designing a Distributed Core Fabric. See also the Flowchart for Designing and Deploying a Fabric.

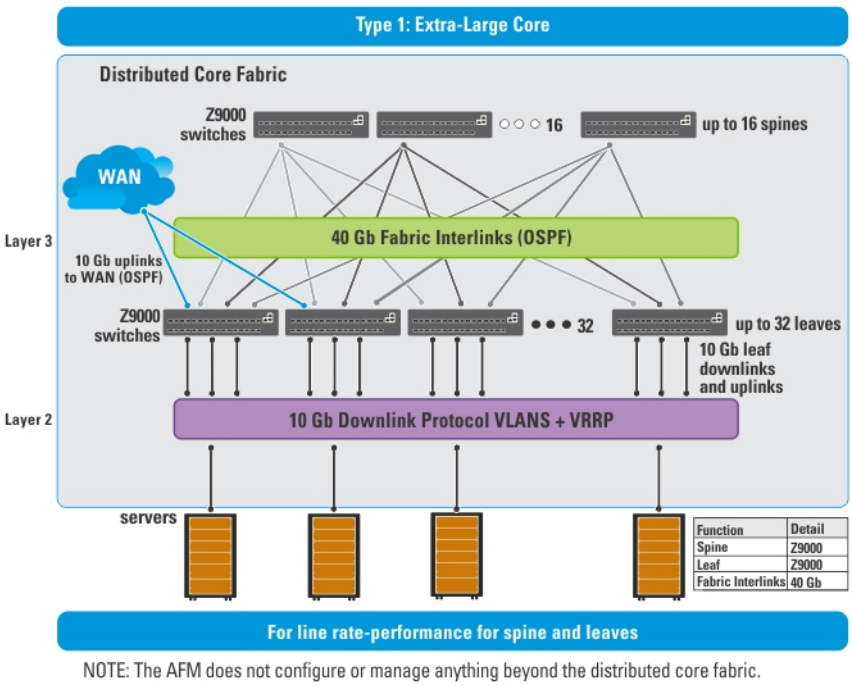
Table 1. Layer 3 Distributed Core Design Fabric Designs

Distributed Core Fabrics	Type 1-Extra Large Core	Type 2-Large Core	Type 3-Medium Core	Type 4-Small Core
Spine device	Z9000	S4810	Z9000	S4810
Leaf device	Z9000	S4810	S4810	S4810
fabric over-subscription (OS) ratio	1:1 (line rate)	1:1 (line rate)	3:1 (default) 4:1	3:1 (default) 5:1
Max # of spine devices	16	32	4 spines with a fabric OS ratio of 3:1	2 or 4

			3 spines with a fabric OS ratio of 4:1	
Max # of leaf devices	32	64	32	8 or 16
Fabric interlink bandwidth	1 x 40 GbE link	1 x 10 GbE link	1 x 40 GbE link	1 x 10 GbE link
Max # of ports (10g) based on fabric OS ratio.	2048 or 2040 with 2 * 10 GbE uplinks	2048	3:1 – 832 (for 4 spines) 4:1 – 1664	For fabric with 2 spines and 8 leaves: 3: 1 – 384 5: 1 – 432 For a fabric with 4 spines and 16 leaves: 3:1 – 768 5:1 – 896

Type 1: Extra Large Distributed Core Fabric

With a Type 1: Extra Large Distributed Core fabric design, the Z9000 spines connect to the Z9000 leaves at a fixed 40 GbE line rate. The maximum number of leaves is based on the maximum number of ports on the spine, 32 ports for the Z9000, as shown in the following figure.



NOTE: The AFM does not configure or manage anything beyond the distributed core fabric.

Figure 4. Type 1: Extra Large Distributed Core Fabric Design

Use the Type 1: Extra Large Distributed Core fabric design when:

- The line rate-performance with a fabric oversubscription ratio of 1:1 between the spines and leaves.
- The current and future planned uplinks and downlinks on the leaves for the distributed core is less than or equal to 2048 ports.

For redundancy, each leaf in a large core design can connect 2 to 16 spines. The Type 1: Extra Large Distributed Core Design uses a 1:2 spine-to-leaf ratio. As a result, the maximum number of spines for this design is 16 and the maximum number of leaves is 32.

Each Z9000 leaf for the Type 1: Extra Large Distributed Core design has the following:

- Six hundred forty Gigabit of fabric interlink maximum capacity to the Spine (16 x 40 Gb)
- Forty-eight 10 GbE ports for server connectivity and WAN connectivity

Type 2: Large Distributed Core Fabric

Use the Type 2: Large Distributed Core fabric design when:

- You require a fabric interlink bandwidth between the spines and leaves of 10 GbE is required.
- The current and future planned uplinks and downlinks on the leaves for the fabric is less than or equal to 2048 ports.
- The leaves act as a switch or ToR-leaf switch. Within the ToR, the downlink protocol can be either **VLAN** or **VLAN and LAG**.

With a Type 2: Large Distributed Core fabric design, the S4810 spines connect to the S4810 leaves at a fixed 10 GbE. The maximum number of spines is 32 and the maximum number of leaves is 64, as shown in the following figure.

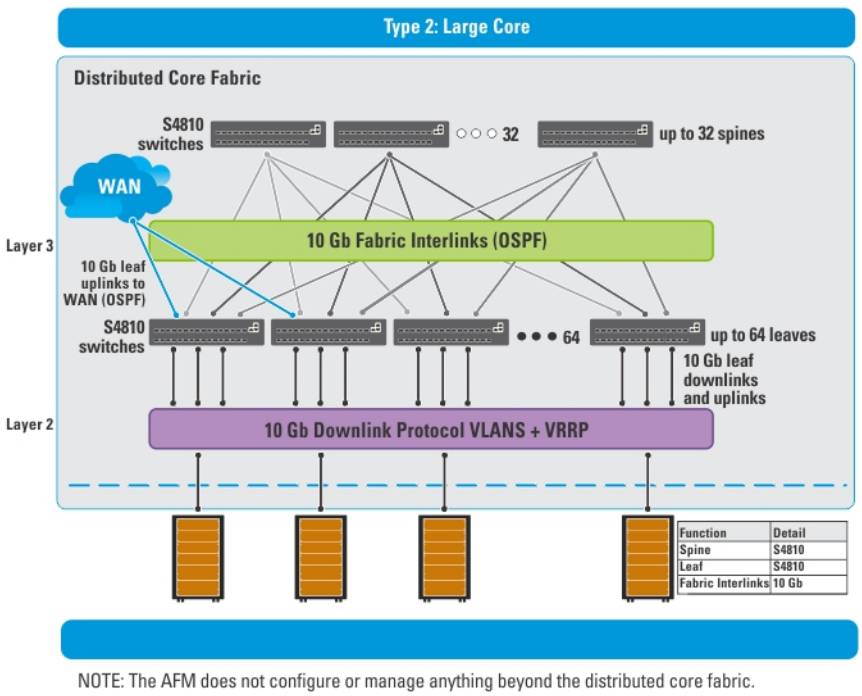


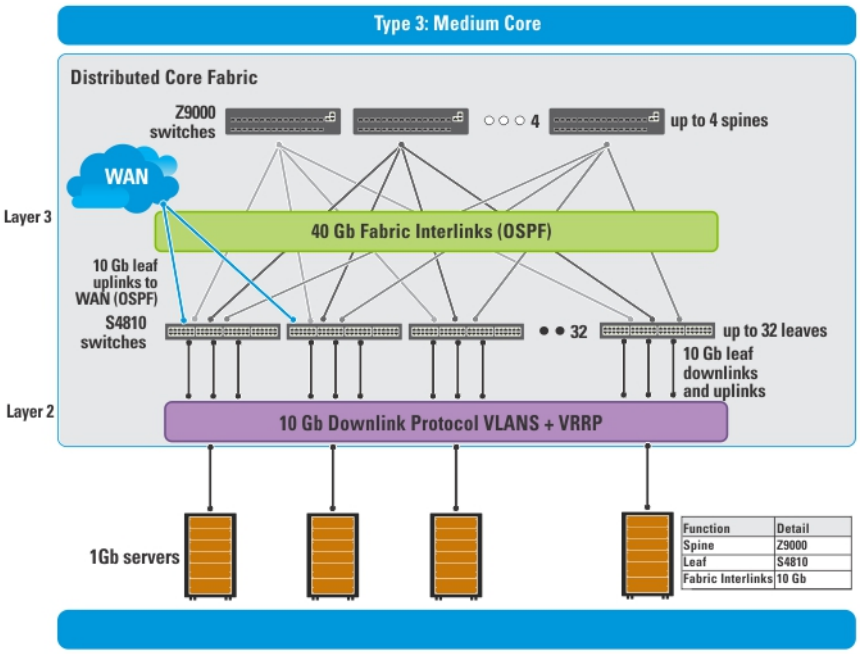
Figure 5. Type 2: Large Distributed Core Fabric Design

Each S4810 leaf for the Type 2: Large Distributed Core fabric design has the following:

- Forty gigabit of fabric interlink maximum capacity to the spine (4x 10 Gb)
- Thirty-two 10 Gigabit ports will be used for fabric interlink and thirty–two 10 Gb ports are used for the downlinks

Type 3: Medium Distributed Core Fabric

With a Type 3: Medium Distributed Core design, the Z9000 spines connect to the S4810 leaves at a fixed 40 GbE line rate as shown in the following figure. The maximum number of leaves is based on the maximum number of ports on the spine, 32 ports for the Z9000. The maximum number of spines is 16 and the maximum number of leaves is 32, as shown in the following illustration. This illustration shows a networking system architecture in a data center are a distributed core fabric containing a set of ToRs to which servers, storage devices, and network appliances (such as load balancers or network security appliances) are connected. You can run application services, network services, and network security services either on physical machines or virtual machines.



NOTE: The AFM does not configure or manage anything beyond the distributed core fabric.

Figure 6. Type 3: Medium Distributed Core Fabric Design

Use the Type 3: Medium Distributed Core design when:

- You require a fabric interlink bandwidth between the spines and leaves at a 40 GbE line rate.
- The current and future planned uplinks and downlinks on the leaves for your distributed core fabric is less than or equal to 1536 ports.
- The leaves act as a switch or ToR-leaf switch. Within the ToR, the protocol can be either **VLAN** or **VLAN and LAG**.

Each Z9000 spine for the Type 3: Medium Distributed Core design has the following:

- Six hundred and forty Gigabit of interlink maximum capacity to the spine (16 x 40 Gig)
- Six hundred and forty 10 Gig Ethernet ports for WAN connectivity

Each S4810 leaf for the Type 3: Medium Distributed Core design has the following:

- One hundred and sixty Gigabit of interlink maximum capacity to the spine (4x 40 Gig)
- Forty–eight 10 Gig Ethernet ports for WAN connectivity

Type 4: Small Distributed Core Fabric

Use the Type 4: Small Distributed Core design when:

- You require a fabric interlink bandwidth between the spines and leaves of 10 GbE.
- The current and future planned uplinks and downlinks on the leaves for your core is less than or equal to 960 ports.
- The maximum port count for a Type 4: Small Distributed Core fabric with an OS ratio of 3:1 is 768. For an OS ratio of 5:1, the maximum port count is 896.
- The leaves act as a switch or ToR-leaf switch. Within the ToR, the downlink protocol can be either **VLAN** or **VLAN and LAG**.

With a Type 4: Small Distributed Core fabric design, the S4810 spines connect to the S4810 leaves at a fixed 10 GbE. The maximum number of spines is 4 and the maximum number of leaves is 16, as show in the following figure.

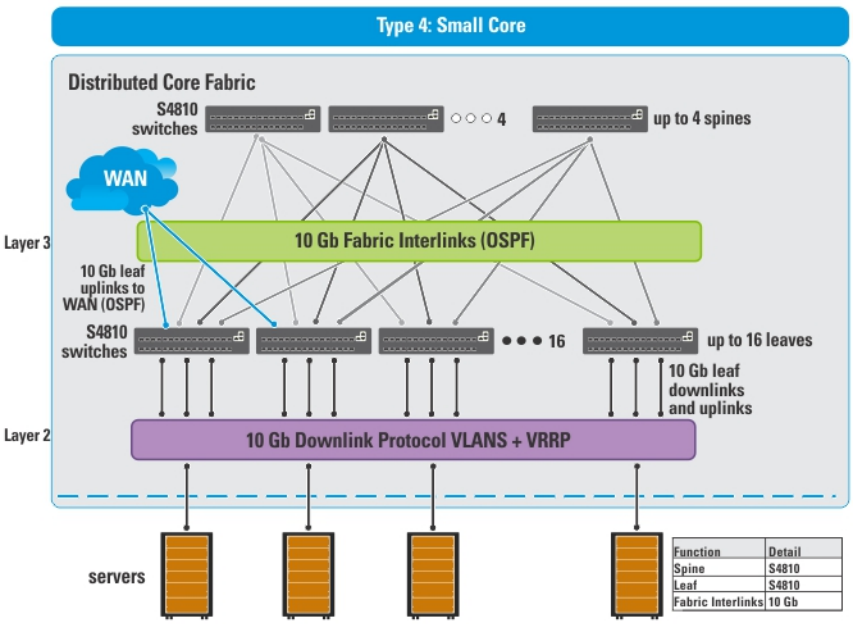


Figure 7. Type 4: Small Distributed Core Fabric Design

Each S4810 leaf for the Type 4: Small Distributed Core design has the following:

- Sixteen 10 Gigabit of fabric interlink port capacity to the spine
- Forty–eight 10 Gig Ethernet downlinks
- Sixty 10 Gig Ethernet ports for servers per node and WAN connectivity

VLT

Virtual link trunking (VLT) allows physical links between two chassis to appear as a single virtual link to the network core or other switches such as Edge, Access or Top of Rack (ToR). VLT reduces the role of Spanning Tree protocols by allowing LAG terminations on two separate distribution or core switches, and by supporting a loop free topology. (A Spanning Tree protocol is still needed to prevent the initial loop that may occur prior to VLT being established. After VLT is established, RSTP may be used to prevent loops from forming with new links that are incorrectly connected and

outside the VLT domain.) VLT provides Layer 2 multipathing, creating redundancy through increased bandwidth, enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.

For information about VLT, see the FTOS Configuration Guide for either the S4810 or the Z9000 at https://www.force10networks.com/CSPortal20/KnowledgeBase/Documentation.aspx. For more information about VLT, see Selecting a VLT Fabric Design.

Virtual link trunking offers the following benefits:

- Allows a single device to use a LAG across two upstream devices
- Eliminates Spanning Tree protocol (STP) - blocked ports
- Provides a loop-free topology
- Uses all available uplink bandwidth
- Provides fast convergence if either the link or a device fails
- Optimized forwarding with Virtual Router Redundancy Protocol (VRRP)
- Provides link-level resiliency
- Assures high availability

CAUTION:

Dell Networking recommends not enabling Stacking and VLT simultaneously.

If both are enabled at the same time, unexpected behavior occurs.

Multi-domain VLT

An multi-domain VLT (mVLT) configuration allows two different VLT domains connected by a standard Link Aggregation Control protocol (LACP) LAG to form a loop-free Layer 2 topology in the aggregation layer. This configuration supports a maximum of 4 units, increasing the number of available ports and allowing for dual redundancy of the VLT. For more information about mVLT deployments, see Selecting a Layer 2 VLT Fabric Design.

VLT Terminology

The following are key VLT terms.

- **Virtual link trunk (VLT)** — The combined port channel between an attached device and the VLT peer switches.
- **VLT backup link** — The backup link monitors the health of VLT peer switches. The backup link sends configurable, periodic keep alive messages between VLT peer switches.
- **VLT interconnect (VLTi)** — The link used to synchronize states between the VLT peer switches. Both ends must be on 10G or 40G interfaces.
- **VLT domain** — This domain includes both VLT peer devices, the VLT interconnect, and all of the port channels in the VLT connected to the attached devices. It is also associated to the configuration mode that must be used to assign VLT global parameters.
- **VLT peer device** — One of a pair of devices that are connected with the special port channel known as the VLT interconnect (VLTi).

VLT peer switches have independent management planes. A VLT interconnect between the VLT chassis maintains synchronization of Layer 2/ Layer 3 control planes across the two VLT peer switches. The VLT interconnect uses either 10G or 40G user ports on the switch.

A separate backup link maintains heartbeat messages across an out-of-band (OOB) management network. The backup link ensures that node failure conditions are correctly detected and are not confused with failures of the VLT

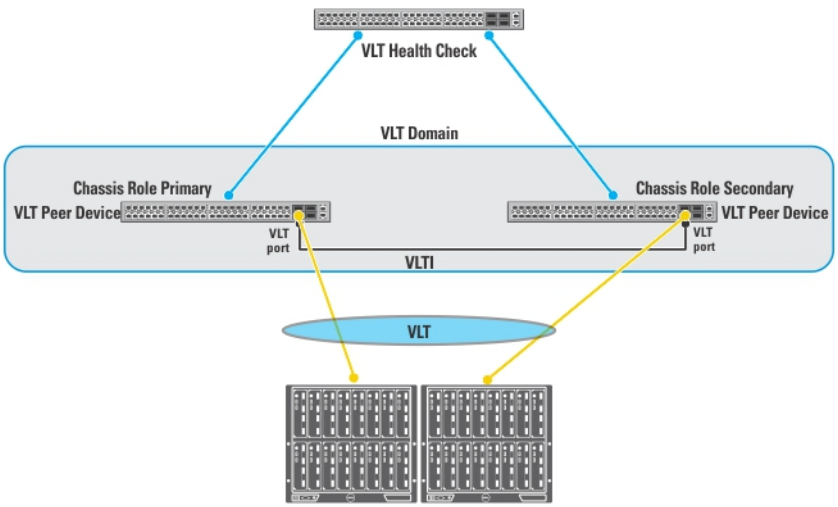
interconnect. VLT ensures that local traffic on a chassis does not traverse the VLTi and takes the shortest path to the destination via directly attached links.

VLT Fabric Terminology

The following terms are unique to the design and deployment of a Layer 2 VLT fabric.

- **Leaf** — A switch that connects switch, servers, storage devices, or top-of-rack (TOR) elements. The role of the leaf switch is to provide access to the fabric. The leaf switch connects to all of spines above it in the fabric.
- **Spine** — A switch that connects to leaf switches. The role of the spine is to provide an interconnect to all the leaf switches. All the ports on the spine switches are used to connect the leaves, various racks together. The spines provides load balancing and redundancy in the distributed core. There are no uplinks on the spines.
- **Edge ports** — The uplinks on the spines and downlinks on the leaves.
- **Uplinks** — An edge port link on the first two spines in the VLT fabric that connects to outside the fabric.
- **Downlinks** — An edge port link that connects the leaves to the data access layer. For example, servers or ToR elements. Downlinks are always 1 Gb or 10 Gb. You must specify an even number of uplinks. The minimum number of uplinks is **2**. One uplink is for redundancy.
- **Fabric Interlinks** — Links that connect the spines to the leaves. The fabric interlink bandwidth is fixed: 40 Gb or 10 Gb.

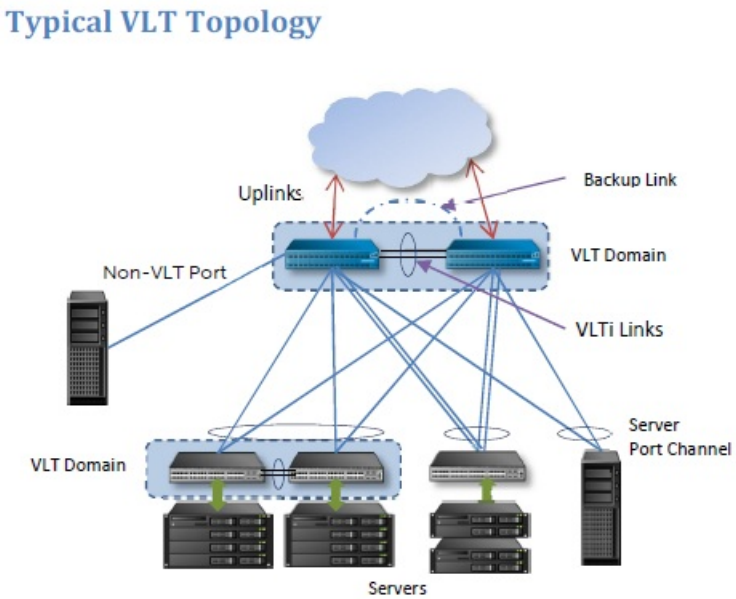
VLT Components



Typical VLT Topology

The VLT domain has VLTi (ICL) links connecting between VLT peers and VLT port-channels connecting to a single access switch, to a switch stack, a server supporting LACP on its NIC, or to another VLT domain as shown in the following illustration. The backup-link connected through the out-of-band (OOB) management network. Some hosts can

connect through the non-VLT ports.



Key Considerations for Designing a Layer 2 VLT Fabric

Use the Layer 2 VLT fabric for workload migration over virtualized environments. When designing the Layer 2 VLT fabric, consider the following:

- You can deploy up to 10 fabrics. However, the fabric do not communicate with each other.
- For a VLT fabric, the AFM manages Dell Networking S4810, S4820T, S55, S60, Z9000, and MXL Blade switches.

CAUTION: If you are already using a deployed switch, you must reset the factory settings. The switch must be in BMP mode.

For more information on BMP, see Pre-Deployment – Step 7: DHCP Integration and the *FTOS Configuration Guide* for the Dell Networking S4810, S4820T, S55, S60, Z9000, and MXL switches at https://www.force10networks.com/CSPortal20/KnowledgeBase/Documentation.aspx.

The number and type of spines and leaves (switches) in a VLT fabric are based on the following:

- The type of VLT fabric design:

VLT Fabric Type	Use Case	Stacking
Type 1 – 1 Gb ToR	For a ToR deployment (S60 or S55 switches) that require 1 Gb downlinks. The leaves must the same type of switch.	Yes
Type 2 – 10 Gb Blade Switch (MXL)	Have an MXL switch that requires 10 Gb uplinks.	Yes
Type 3 – 10 Gb ToR	For a ToR deployment that requires 40 Gb uplinks and 10 Gb downlinks and mVLT	No

- The number of current uplinks and downlinks for the leaves.
- The number of planned edge ports (future uplinks and downlinks) for the leaves.
- Whether the leaves need to act as a ToR or access layer.

- Fabric interlink bandwidth (the links between the spines and leaves).
- Downlinks, 1 Gb or 10 Gb.
- The fabric interlink bandwidth, 10 Gb or 40 Gb, is fixed and based on the fabric type.

CAUTION: If you do not specify additional links in the fabric design for future expansion in the Port Specification screen:

- Any future expansion requires rewiring the hardware.
- IP addresses are not reserved.
- You might have to bring down current switches to expand the fabric. For information on how to expand a fabric, see Editing and Expanding an Existing Fabric Design.

Gathering Useful Information for a Layer 2 VLT Fabric

To gather useful information for a layer 2 VLT fabric before you begin:

- Obtain the **.csv** file that contains the system MAC addresses, service tag and serial numbers for each switch provided from Dell manufacturing or manually enter this information.
- Obtain the location of the switches, including the rack and row number from your network administrator or network operator.
- Obtain the remote Trivial File Transfer Protocol (TFTP) / File Transfer Protocol (FTP) address from your network administrator or network operator.
- Download the software image for each type of switch in the fabric: S4810, S4820T, S55, S60, Z9000, or MXL blades. Each type of switch must use the same version of the software image within the fabric. Place the software images on the TFTP/FTP site so that the switches can install the appropriate FTOS software image and configuration file. The AFM automatically copies the minimum configuration into the specified TFTP/FTP location. To specify a TFTP/FTP site, go to **Administration** > **Settings** screen. For information about which software packages to use, see the Release Notes.
- Obtain the Dynamic Host Configuration Protocol (DHCP) server address to use for the fabric from your DHCP network administrator or network operator. If a remote DHCP server is not available, AFM also provides a local DHCP. The DHCP server must be in the same subnet where the switches are located. After you power cycle the switches, the switches communicate with the DHCP server to obtain a management IP Address based on the system MAC Address. The DHCP server contains information about where to load the correct software image configuration file for each type of switch from the TFTP/FTP site during BMP. For information about BMP, see Pre-Deployment – Step 7: DHCP Integration.
- Obtain the pool of IP addresses for the management port for each switch in the fabric.
- Obtain IP addresses (2-8 addresses, must be an even number) for the uplink configuration from the ISP service.
- Obtain IP addresses for the downlink configuration for connecting to the server or ToR.
- Gather protocol configuration for uplinks and downlinks.

Selecting a Layer 2 VLT Fabric Design

For workload migration over virtualized environments, use a Layer 2 VLT fabric design.

The AFM supports the following Layer 2 VLT fabric designs:

- Type 1: 1 Gb Top of Rack Deployment

- Type 2: 10 Gb Blade Switch (MXL)
- Type 3: 10 Gb Top of Rack Deployment (mVLT)

For more information about VLT, see Overview of VLT, and Key Core Design Considerations for VLT. See also Getting Started.

Use the following table as guideline to select the appropriate Layer 2 VLT fabric design.

NOTE: With a Layer 2 VLT fabric, the uplinks come from the first two spines.

Table 2. Layer 2 VLT Fabric Designs

Function	Type 1: 1 Gb ToR	Type 2: 10 Gb Blade Switch (MXL)	Type 3: 10 Gb ToR (mVLT)
Spine device	S4810	S4810	Z9000
Leaf device	S60 or S55	MXL switch	S4810 or S4820T
Max # of spines	2	2	2
Max number of leafs	44	11 (without stacking) and 10 (with stacking)	26
Uplink ports	4 x 40 Gb	8 x 40 Gb	8 x 40 Gb
Interlink ports	88 x 10 Gb	80 x 10 Gb	52 x 40 Gb
Max number of leaf ports	2304 (1Gb ports) 48 * 48 ports = 2304	240 (10 Gb ports) ports per expansion * 2 expansion blade = 8 ports 8 ports + 40Gb (4 * 10GB) = 12 ports 12 ports per MXL * 2= 24 ports per chassis 10 chassis * 24 ports= 240 ports.	1248 (10 Gb ports) 26 Leaf devices * 48 ports = 1248 From each leaf (S4810/ S4820-T) two 40G ports are used as VLTi connections and two 40G are used as fabric links. The remaining forty–eight 10G ports are used as downlinks.

Type 1: 1 Gb ToR VLT Deployment

With a Type 1: 1 Gb ToR VLT Deployment fabric design, the S4810 spines connect to leaves (S60 or S55) at fixed 10 Gb. The maximum number of spines is 2 and the maximum number of leaves is 44. Use this type for a ToR deployment that requires 1 Gb downlinks and stacking. On S60 or S55 leaf switches, the leaves must the same type of switch.

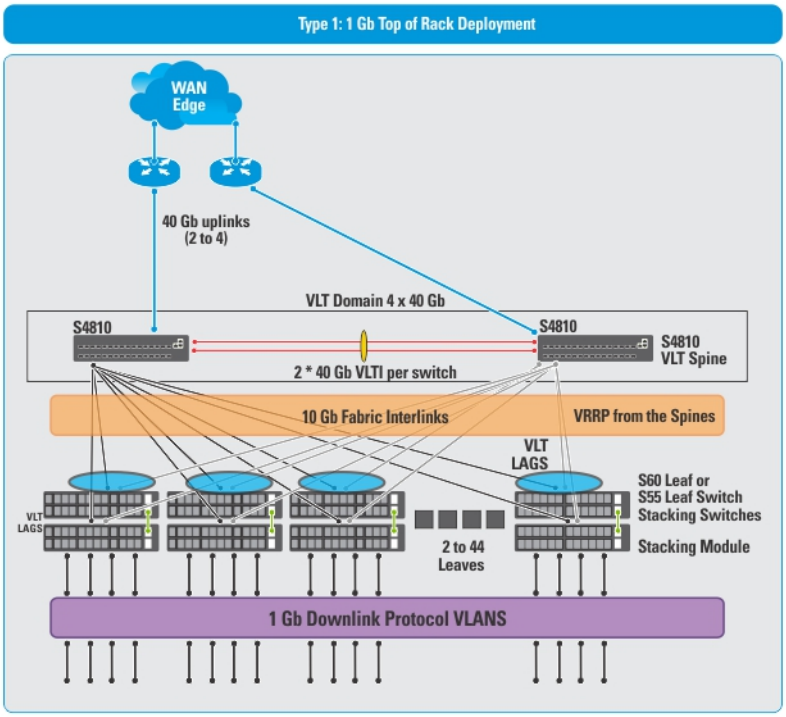


Figure 8. Type 1: 1 Gb ToR VLT Deployment

Important: All the spines must be same type: S4810. On the leaves, all the switches must be same type of switch: S60 or S55.

Table 3. Type 1: 1 Gb ToR VLT Deployment Port Types

Port Type	Max # of Ports	Min # Ports
Downlink ports (48 Switches x 48 Ports)	2304 x 1Gb	96 x 1Gb
Uplink ports	4 x 40 Gb	2 x 40Gb
Fabric (Interlink) ports (VLT Spine to Leaf)	96 x 10Gb	4 x 10Gb
VLTi Ports (Spine 2 links)	4 x 40Gb	4 x 40Gb
Stack Ports (2 Leaf stack Max)	2 x 12 Gb	2 x 12 Gb

Type 2: 10 Gb Blade Switch (MXL) VLT

Use the Type 2: 10 Gb MXL Blade Deployment when you require a 10 Gb downlinks, stacking, and have an MXL switch.

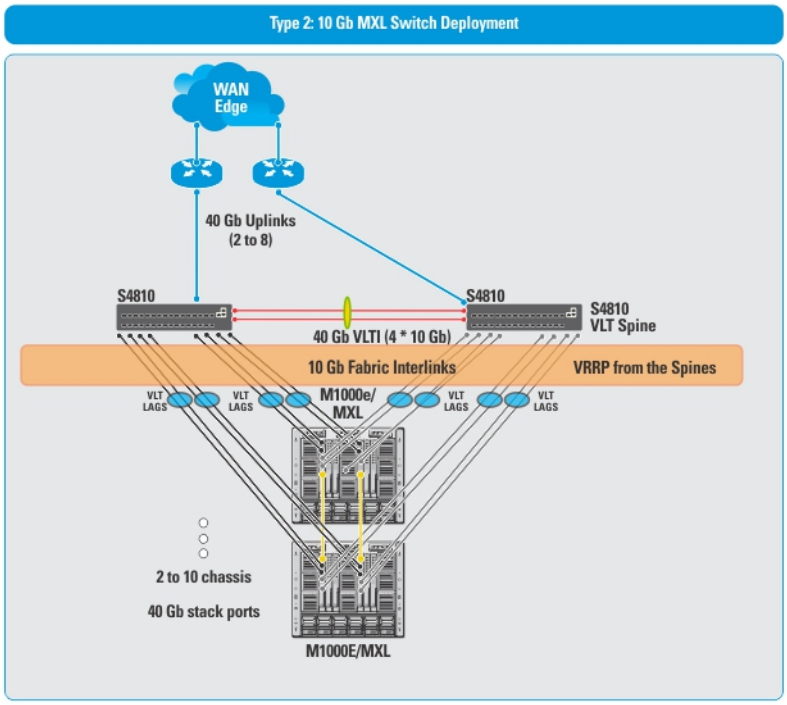


Figure 9. Type 2: 10 Gb Blade Switch (MXL) VLT Deployment

Table 4. Type 2: 10 Gb Blade Switch (MXL) VLT Deployment Port Types

Port Type	Max # of Ports
MXL Available ports (10 Chassis * 24)	240 * 10 Gb
Uplink ports	8 * 40 Gb
Fabric Interlink ports	88 * 10 Gb
VLTi Ports (Spine)	The maximum number of VLTi ports is 8 * 10 Gb. The ports and maximum VLTi links have a 4 * 10 Gb capacity.
Stack Ports (Leaf)	40 * 40 Gb

NOTE: With a Type 2: 10 Gb Blade Switch (MXL) VLT deployment, there are no downlinks.

Type 3: 10 Gb ToR (mVLT)

Use the Type 3: 10 GbE ToR Deployment (mVLT) when you require 10 Gb downlinks for a ToR. For information about mVLT, see Multi-domain VLT.

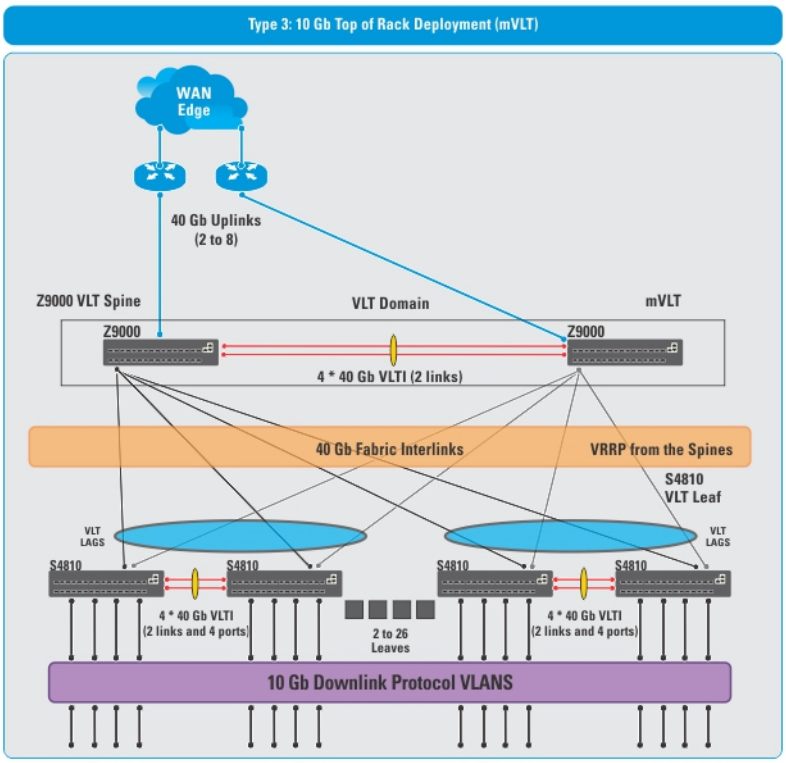


Figure 10. Type 3: 10 Gb ToR VLT Deployment (mVLT)

Important: All the spines must be Z9000. On the leaves, all the switches must be same type of switch: either S4810 or S4820T.

Table 5. Type 3: 10 Gb ToR mVLT Deployment Port Types

Port Type	Max # of Ports	Min # Ports
Downlink ports (26*48 or 2*48)	1248 * 10Gb	96 * 10Gb
Uplink ports	8 * 40 Gb	2 * 40 Gb
Fabric (Interlink) ports Spine (2 * Z9000)	52 * 40Gb	4 * 40Gb
Fabric (Interlink) ports Leaf (13 S4810 VLT pairs)	52 * 40Gb	4 * 40Gb
VLTi Ports (Spine 2 links)	4 * 40Gb	2 * 40Gb
VLTi Ports (Leaf 26 links)	26 * 40Gb	2 * 40GB

6

Designing the Fabric

To design a Layer 3 two-tier distributed core fabric or Layer 2 VLT fabric based on your capacity planning for your current and future needs, use the **Fabric Design Wizard** at the **Network > Design Fabric > New Fabric** screen. The design consists of a wiring plan, network topology information, summary of the inventory requirement, and a design specification. See also Network Deployment Summary.

This screen allows you to perform the following tasks:

- Create a fabric
- Editing and Expanding an Existing Fabric
- Deleting the Fabric
- Import an Existing Fabric Design
- Viewing the Wiring Diagram
- Display the status of the fabric design (whether the design, pre-deployment, deployment, and validation has been successfully completed.
- Display detailed information about the fabric

Before you begin, review the Getting Started section.

To design a fabric, complete the following tasks using the **Fabric Design Wizard**.

1. Fabric Design – Step 1: Fabric Name, Type, and Description
2. Fabric Design – Step 2: Bandwidth
3. Fabric Design – Step 3: Port Specification
4. Fabric Design – Step 4: Deployment Type
5. Fabric Design – Step 5: Output
6. Fabric Design – Step 6: Summary

NOTE: After you finish designing the fabric, prepare it for deployment. For more information, see Preparing the Fabric for Deployment.

Network Deployment Summary

AFM allows you to design a fabric, make changes to the pre-deployment configuration, deploy the fabric, and validate the fabric designed with the discovered fabric. AFM provides up-to-date status during each phase of the fabric from design to validate. AFM displays any pending steps required that you needed to ensure the fabric is fully functional for each fabric design.

Fabric Configuration Phases and States

The following table describes the four fabric phases displayed on the **Network** > *Fabric Name* > **Configure and Deploy** > **Deploy** screen. To correct the fabric design and pre-deployment configuration before and after you deploy the fabric, use this information.

Table 6. Fabric Configuration Phases and States

Phase	State	State Description
Design	Incomplete	Indicates that not all required information to complete the design was provided. **Note**: This state is applicable only during the initial design; after a design is completed it never reverts back to this state.
	Complete	Indicates that all required input was provided to complete the design.
Pre-deployment Configuration	Required	Indicates that not all required Pre-deployment Configuration information for any of the switches was provided. **NOTE:** The Pre-deployment Configuration state for all switches is in state Required.
	Error	Indicates that deployment error(s) exist for one or more switches.
	Partial Complete	Indicates that Pre-deployment was successfully completed for one or more switches but not for all switches per design. It provides information about the count of switches successfully deployment versus the count of total switches per design. **NOTE:** Information provided is sufficient to proceed with deployment of the subset of switches.
	Complete	Indicates that Pre-deployment Configuration information is complete for all switches.
Deployment	Required	Indicates that the Deployment state for all switches is in the Required state.
	In-progress	Indicates that Deployment is In-progress (the progress bar displays in the UI) on one or more switches. It also provides information about the count of switches successfully deployment versus the count of total switches per design (the based current port count, doesn't include the future port count).
	Error	Indicates that deployment error(s) exist for one or more switches.
	Partial Complete	Indicates that Deployment was successfully completed for one or more switches but not for all switches per design. It provides information about count of switches successfully deployment vs. count of total switches per design. **NOTE:** Deployment on any of the switches is not in-progress during this state.Note
	Complete	Indicates that deployment was successful for the switch.
Validation	Required	Indicates that the validation state for all switches is in state Required.
	In-progress	Indicates that validation is In-progress (progress bar to be displayed in UI) on one or more switches. It provides information about count of switches successfully validated vs. count of total switches per design (based current port count, doesn't include future port count).
	Error	Indicates that validation error(s) exist for one or more switches.

	Partial Complete	Indicates that validation was successfully completed for one or more switches but not all switches per design. It provides information about the count of switches successfully validated versus the count of total switches per design. NOTE: Validation of any of the switches is not in-progress during this state.
	Complete	Indicates that validation was successful for all switches.

Switch Configuration Phases and States

This section describes the phases and possible states for a switch.

Table 7. Switch Configuration Phases and States

Phase	State	State Description
Design	Complete	Indicates that design is complete for the switch. NOTE: At switch level, design Partial Complete will not be tracked. Partial Complete will only be tracked at the fabric level.
Pre-deployment Configuration	Required	Indicates that not all required Pre-deployment Configuration information was provided.
	Error	Indicates that an error occurred during file transfer (transfer of minimum configuration file) to FTP/TFTP server or an error occurred during automatic DHCP integration for local DHCP server. NOTE: In case of remote DHCP server, no errors will be reported for DHCP integration step as it is not an automated step from AFM; user is responsible for manual DHCP integration in this case.
	Complete	Indicates that Pre-deployment Configuration information is complete for the switch.
Deployment	Required	Indicates that deployment was never initiated for the switch or the Deployment state was reset due to Design/Pre-deployment Configuration change. NOTE: Deployment can be initiated/re-initiated only if Pre-deployment Configuration is in state Complete
	In-progress	Indicates that Deployment is in-progress and also provides the latest percentage complete information.
	Error	Indicates that deployment error exists.
	Complete	Indicates that deployment was successful for the switch.
Validation	Required	Indicates that validation was never initiated for the switch or the validation state was reset due to Design/Pre-deployment Configuration/Deployment change. NOTE: Validation can be initiated only if Deployment is in state Complete.
	In-progress	Indicates that deployment is in-progress and also provides the latest percentage complete information.
	Error	Indicates that one or more validation error exists.
	Complete	Indicates that validation was successful for the switch.

Using the Fabric Design Wizard

Use the Fabric Design Wizard at the **Network > Design Fabric** > **New Fabric** screen to design a Layer 3 distributed core fabric or Layer 2 VLT fabric based on your workload requirements for your current and future needs. This screen allows you to create, edit, delete, and view the fabric.

Use the following screens to design a fabric:

1. **Fabric Name and Type** — Displays the fabric name, type, and description.
2. **Bandwidth** — Displays the downlink and uplink bandwidth based on the fabric type.
3. **Port Specification** — Displays the fabric over-subscription ratio (distributed core fabric only), the number of edge port uplinks to the WAN connection, and downlinks (for example, to servers or ToRs) required for the initial deployment as well as for future expansion.
4. **Deployment Type** — Displays the deployment type for a Layer 3 distributed core fabric or Layer 2 VLT fabric.
5. **Output** — Displays the fabric in the following formats: graphical wiring plan, tabular wiring plan, and network topology.
6. **Summary** — Displays a summary of the fabric design.

Fabric Design – Step 1: Fabric Name and Type

To design a Layer 3 distributed core fabric or Layer 2 VLT fabric based on the your current and future capacity requirements, use the **Fabric Design Wizard**. To simplify and automate the design process, the AFM provides a fabric design wizard to help you design the fabric. See Designing the Fabric, Using the Fabric Design Wizard, and Supported Fabric Types.

To generate a physical wiring diagram for the fabric during the design phase, enter your data center capacity requirements. The wiring diagram is typically given to the network operator who uses it to build the physical network. For information about designing a fabric, see Selecting Distributed Core and Selecting a VLT Fabric Design.

To configure the fabric name, type and description:

1. Navigate to the **Fabric Design Wizard** at the **Network > Design Fabric** screen.
2. Click the **New Fabric** link.

   The Introduction screen is displayed.
3. Review the introduction and click the **Next** button.

   The **Fabric Name and Type** screen displays.
4. Enter the name of the fabric in the **Fabric Name** field.

   The fabric name must be a unique name. It can have from 1 to 21 characters. Valid characters are as follows:

   - alphanumeric
   - underscore (_)
   - **@**
   - **+**

   When you specify the name of the fabric,AFM automatically names the switches (spines and leaves) in the fabric with the fabric name as the prefix. For example, if the name of the fabric is **EastFabric**, the switch names assigned are **EastFabric-Spine-1** and **EastFabric-Leaf1**.
5. (Optional) In the **Description** field, enter the description of the fabric.

   There is no character restriction. The length of the description can be from 1 and 128 characters.

6. In the **Fabric Type** area, select one of the following options:
   a) **Layer 2 Fabric - Virtual Link Trunking (VLT)** — Use the Layer 2 VLT fabric for workload migration over virtualized environments. See Selecting a VLT Fabric Design.

      If you are designing a Layer 2 VLT fabric, select one of the following options:

      * **Top of Rack Deployment**
      * **Blade switch (MXL) deployment**

   b) **Layer 3 Fabric - Distributed Core** — Use the Layer 3 distributed core fabric for large fabric deployments. See Selecting Distributed Core Fabric.
7. Click **Next** to go to the **Bandwidth** screen to review the uplink and downlink bandwidth settings.

   Uplinks connect from the fabric up to the next upstream tier of devices towards the core of the network. Downlinks connect from the fabric down to the next tier of devices or servers towards the edge of the network.

Fabric Design – Step 2: Bandwidth

The **bandwidth** screen displays the default values for the fabric uplinks and downlinks. Uplinks connect from the fabric up to the next upstream tier of devices toward the core of the network. Downlinks connect from the fabric down to the next tier of devices or servers towards the edge of the network. These values (1 Gb, 10 Gb, or 40 Gb) are based on the fabric you have selected in the **Fabric Name and Type** screen.

For Layer 3 Distributed Core fabric, the downlinks and uplinks are always 10GbE. For a Layer 2 VLT fabric that has the leaves acting as a ToR, you can design it to have 1 GbE or 10 GbE downlinks using the **Downlinks Bandwidth** pull-down menu.

Review the values and then click the **Next** button to go to the **Port Specification** screen. For more information about uplinks and downlinks, see VLT Fabric Terminology and Distributed Core Terminology.

Fabric Design – Step 3: Port Specification

This section describes how to configure the port specification for a Layer 3 distributed core fabric and Layer 2 VLT fabric.

- Fabric Design — Step 3: Port Specification for a Layer 3 Distributed Core Fabric
- Fabric Design — Step 3: Port Specification for Type 2 — MXL Blade (Layer 2 VLT Fabric))
- Fabric Design — Step 3: Port Specification for 1 Gb and 10 ToR Port Specification (Layer 2 VLT Fabric)

Fabric Design – Step 3: Port Specification for a Layer 3 Distributed Core

To enter the number of edge port uplinks and downlinks required for the initial deployment and future expansion, use the **Port Specification** screen.

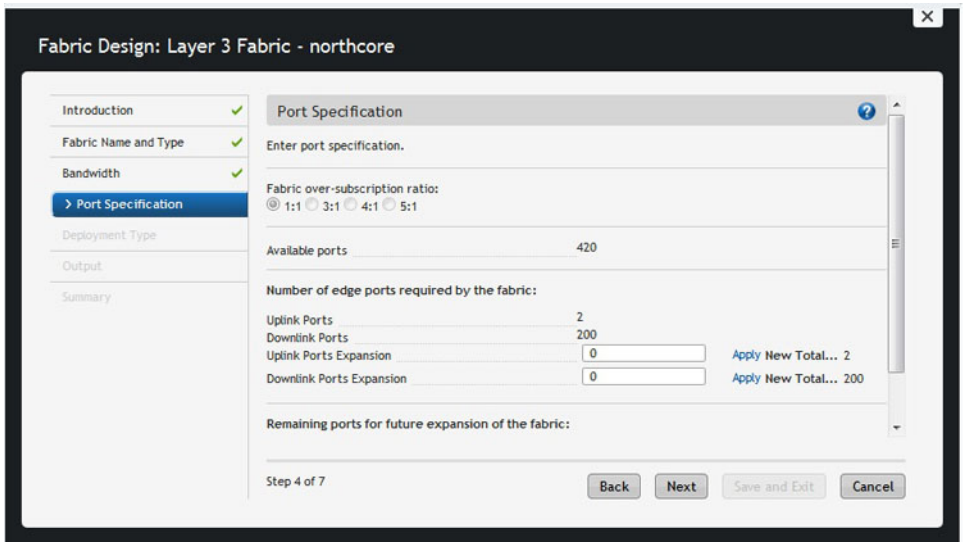


Figure 11. Layer 3 Port Specification

For information about how to expand the fabric, see Editing and Expanding the Fabric.

To configure a Layer 3 distributed core fabric port specification:

1. Navigate to the **Network > Configure and Deploy > Design New Fabric > Port Specification** screen.
2. Select one of the following **Fabric over-subscription ratio** options:
   a) **1:1** (default) — Use the 1:1 fabric over-subscription rate for the non-blocking, line rate between the leaves and spines. Use this option when you require a lot of bandwidth and not a lot of ports.
   b) **3:1**
   c) **4:1**
   d) **5:1**

   The fabric over-subscription rate varies the maximum number of available fabric interlinks. The ratio you specify depends on the bandwidth, throughput, and available edge port requirements. The fabric over-subscription does not come off the edge port downlinks. As you increase the interlink over-subscription ratio:

   – The total number of ports for the uplinks and downlinks increases.
   – The total number interconnect links from the leaves to the spines decreases.
   – The maximum number of available ports increases.
3. In the **Number of edge ports required by the fabric**:
   a) Enter an even number (2 to 32) of uplink ports (connections to the WAN) required by the fabric for initial deployment.
   b) Enter an even number of downlink ports (2 to the maximum number of available ports) required by the fabric for initial deployment. The available number of ports is specified in the **Fabric Name and Typ**e screen. The default is 2 downlinks.
4. In the **Number of additional edge ports for future expansion of the fabric:**
   a) Enter an even number of uplink ports (connections to the WAN) required by the fabric for future deployment.
   b) Enter an even number of downlink ports (connections to the servers, switches, or ToR) required by the fabric for future deployment.
5. Click **Next** to go the **Deployment Type** screen.

Port Specification for MXL (Layer 2 VLT Fabric)

The port specification screen displays the following MXL options when you select the **Type 2: 10 Gb Blade Switch (MXL)** option for a Layer 2 VLT fabric.

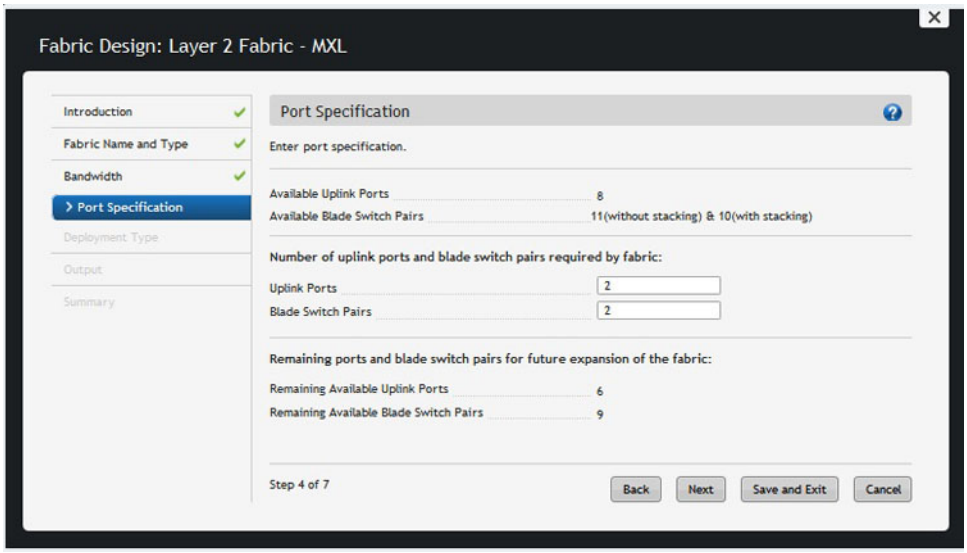


Figure 12. Layer 2 Port Specification for a MXL Blade

Table 8. MXL Blade Port Specification Options

Option	Description
Available Uplink Ports	Displays the maximum available uplink ports. Read-only field.
Maximum Available Blade Switch Pairs	Displays the maximum available blade switch pairs. Read-only field.
Uplink Ports	Enter the uplink ports based on the current requirements. Values: from 2 to 8 **Default**: 2
Blade Switch Pairs	Enter the blade switch pairs based on the current requirements. Values: • from 2 to 11 — without stacking • from 2 to 10 — with stacking **Default**: 2
Remaining Available Uplink Ports	Displays the difference between the Maximum Available Uplink Ports and Current Planned Uplink Ports. Read-only field.
Remaining Available Blade Switch Pairs	Displays the difference between the Maximum Available Blade Switch Pairs and Current Planned Blade Switch Pairs. Read-only field. It is automatically populated. **Default**: Automatically populated.

To specify the port specification for an MXL switch:

1. Navigate to the **Number of uplink ports and blade switch pairs required by fabric** section.
2. In the **Uplinks** field, specify the number of uplinks (from 2 to 8) for the VLT fabric.
3. In the **Blade Switch Pairs** field, specify the number of blade pairs:
   a) from 2 to 11 — without stacking
   b) from 2 to 10 — with stacking
4. Click the **Next** button to go to the **Deployment Type** screen.

Port Specification for ToRs (Layer 2 VLT Fabric)

This section describes how to configure the port specification for the following Layer 2 VLT ToR deployments:

- 1 Gb ToR Deployment
- 10 Gb ToR Deployment

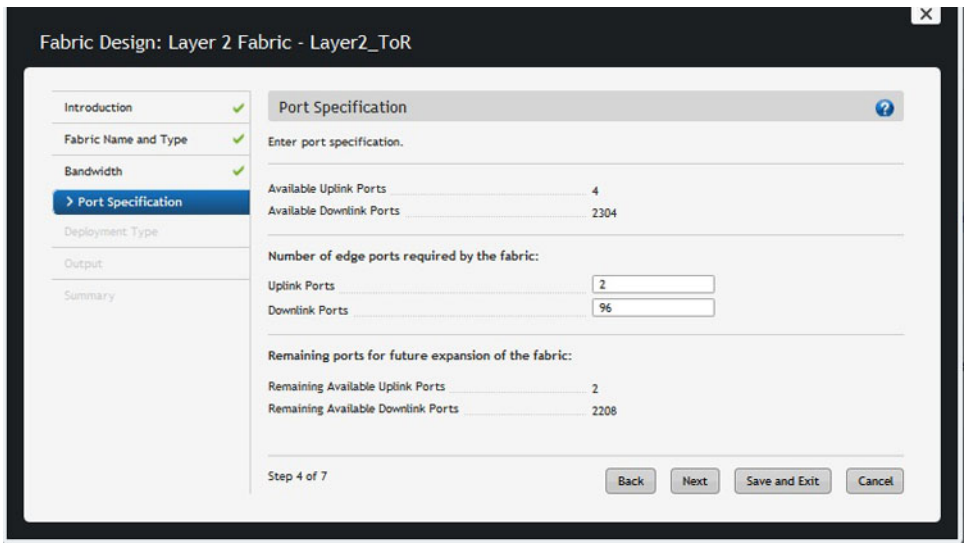


Figure 13. Layer 2 VLT ToR Port Specification

Table 9. Layer 2 VLT ToR Port Specification

Option	Description
Available Uplink/Downlink Ports	Displays the maximum available ports. This value is determined by what is specified in the previous screens. Validation Criteria: This is a read-only field and pre-populated. **Default**: Pre-populated value
Uplink Ports	Enter the uplink ports based on the current requirements. Validation Criteria: • For a Type 1 – 1 Gb ToR deployment the uplink value is from 2 to 4 . • For a Type 3 – 10 Gb ToR deployment the uplink value is from 2 to 8. **Default**: 2
Downlink Ports	Enter the downlink ports based on the current requirements.

	Validation Criteria: 96 to the maximum available ports **Default**: 96
Remaining Available Uplink Ports	Displays the difference between the Maximum Available Uplink Ports and the Current Planned Uplink Ports. Validation Criteria: his is a read-only field and pre-populated. **Default**: It is automatically populated.
Remaining Available Downlink Ports	Displays the difference between the Maximum Available Downlink Ports and the Current Planned Downlink Ports. Validation Criteria: This is a read-only field and pre-populated. **Default**: It is automatically populated.

To configure the port specification for a Layer 2 VLT ToR deployment:

1. Navigate to the **Number of edge ports required by the fabric** section.
2. In the **Uplink Ports** field, specify the number of uplink ports:
   a) For a Type 1 -1 Gb ToR Deployment the uplink value is from 2 to 4.
   b) For a Type 3 -10 Gb ToR Deployment the uplink value is from 2 to 8.
3. In the **Downlinks Ports** field, specify the number downlink ports (96 to the maximum available ports).
4. Click the **Next** button.

Fabric Design – Step 4: Deployment Type

The AFM displays deployment-type options based on what type of fabric you select in the **Fabric Name and Type** and **Port Specification** screens.

When you select a Layer 3 distributed core fabric, the following deployment types are available:

- Type 1: Extra Large Fabric
- Type 2: Large Fabric
- Type 3: Medium Fabric
- Type 4: Small Fabric

When you select a Layer 2 VLT fabric, the following options are available:

- Type 1: 1 Gb Top of Rack
  - **Stack leaf switches** (High Stream Buffering or Deploy using stacking)
- Type 2: 10 Gb Blade Switch (MXL)
  - **Deploying Using Stacking**
- Type 3: 10 Gb Top of Rack
  - **SFP+ (Switch: Model S4810)**
  - **RJ-45 (Switch Model: S4820T)**

To configure the fabric deployment type:

1. Navigate to the **Network** > **Design Fabric** > **New Fabric** > **Deployment Type** screen.
2. Select the deployment type and the options that are appropriate for your fabric.

3. For a Layer 2 VLT fabric, select whether you require stacking.

4. For a Layer 2 VLT Type 1: 1 Gb Top of Rack deployment, select one of the following options:
   a) **High Stream Buffering** — The fabric uses S60 switches in the leaves. When you uncheck this option, the fabric uses S55 switches in the leaves.
   b) **Deploy using stacking** — Deploys stacked S60 and S55 leaves in the fabric.

5. For a Layer 2 VLT Type 3: 10 Gb ToR fabric, select one of the following cabling options:
   a) **SFP+ (Switch: Model S4810)**
   b) **RJ-45 (Switch Model: S4820T)**

6. Click the **Next** button to go to the **Output** screen.

Fabric Design – Step 5: Output

To view the graphical wiring, tabular wiring, and network topology wiring plans for your fabric design, use the **Output** screen. Use the wiring plan as a guide for installing your equipment into the Layer 3 distributed core fabric or Layer 2 VLT fabric. Based on the configuration, the AFM calculates the number of leaf and spine switches required for the design and displays the physical wiring plan which you can export and print in PDF or Visio®. The wiring plans display the cabling maps (the connections between the spines and leaves) the switches and links for future expansion. Review the wiring plans and then export them to a file.

Typically, after the fabric design is approved, the wiring plan is given to your data center operator who uses this information to build the physical network according to the fabric design.

The fabric design is displayed in the following formats:

- **Graphical Wiring Plan** — Displays information about how the spines and leaves (switches) are connected graphically as shown below.

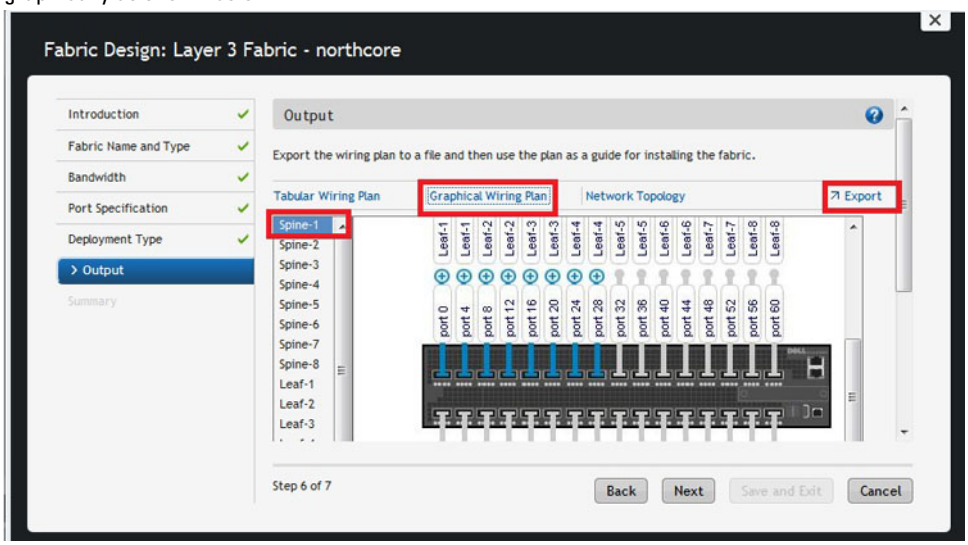


Figure 14. Graphical Wiring Plan

- **Network Topology** — Displays information about how the spines and leaves are connected physically using a topology map. By default, no links are displayed in the fabric. Click on a switch to display the links in the fabric. When you select a spine or leaf switch , all the fabric interconnect links are displayed. When you select a spine switch, the links to the leaf switches are displayed. Similarly, when you select a leaf switch, the links to the spine switches are displayed.

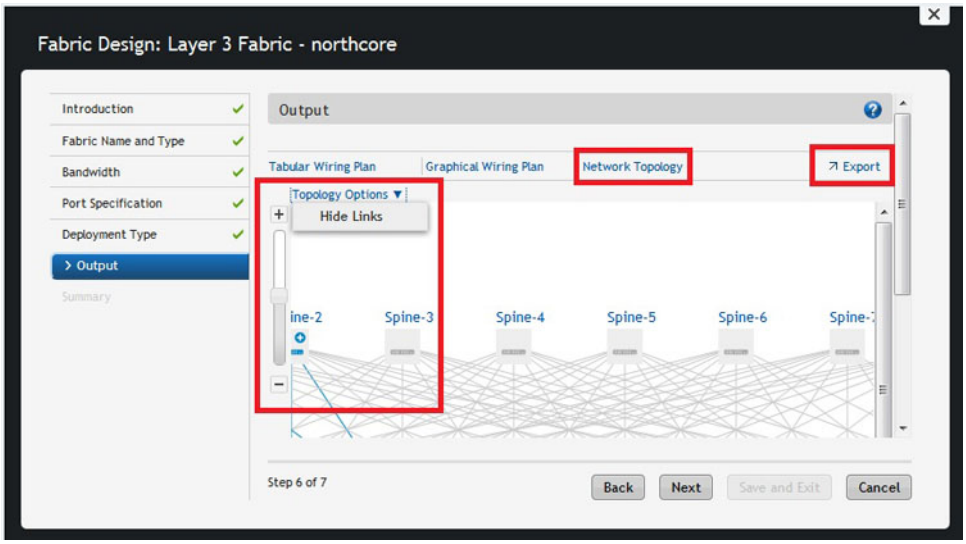


Figure 15. Network Topology

- **Tabular Wiring Plan** — Displays information about how the spines and leaves are connected in the distributed core design in a tabular format, as shown below. The tabular wiring plan contains a list of switches along with their names and ports which connect to the ports on the other switches.

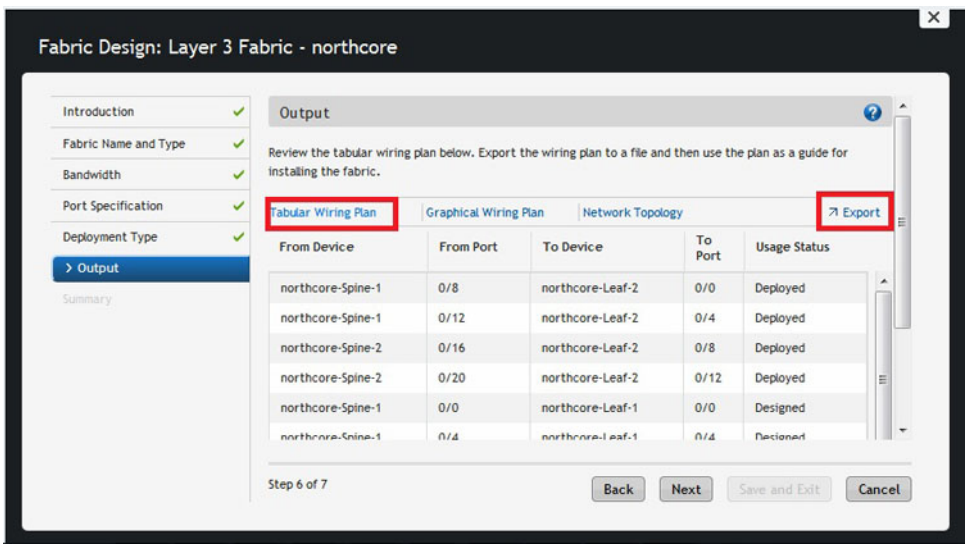


Figure 16. Tabular Wiring Plan

Table 10. Tabular Wiring Plan Output Descriptions

Field Name	Description
From Port	Displays the port number on the spine — from the side.
From Spine	Displays the name of the spine — from the side.
To Leaf	Displays the name of the leaf — to the side.
To Port	Displays the port number on the leaf — to the side.

Usage Status	• Current — Represents the links based on your current needs. • Future — Represents links based on the fabric's future needs. • Displays usage status: Current / Expansion.

To review and export the fabric wiring plan:

1. Navigate to the **Network > Design Fabric > New Fabric > Output** screen.
2. Click on the type of wiring plan that you want to export: **Tabular Wiring Plan**, **Graphical Wiring Plan**, or **Network Topology**.
3. Click the **Export** link.

   The **Generate Wiring Plan** window displays.
4. Specify the following export options.
   a) **PDF** — **Table Data**, **Graphical Wiring Plan**, or **Both.**
   b) **Visio** — **Network Topology**

Fabric Design – Step 6: Summary

The **Summary** screen displays a summary of your fabric design. You can export the fabric design by click the **Export** link in the upper right of the screen, select a format PDF (**Table Data**, **Graphical Wiring Plan**, **Both**) or **Visio**, then click the **Generate** button. Carefully review the design before you commit the changes.

To commit the changes, click **Finish**.

Next Steps

After you have designed the fabric, do the following to prepare it for deployment:

1. Check with your system administrator for the TFTP or FTP IP address. To stage the switch software images, use this address. When you prepare the software images:
   a) Make sure the software version is the same for each type of switch across the fabric.
   b) Download the software image for each type of Dell Networking switch.
   c) Stage the software images on the TFTP or FTP site.
2. Obtain a pool of management IP addresses from the lab or system administrator to use for the switches in the fabric.
3. Prepare the DHCP server so that the switches can be assigned a management IP address.
4. Download the comma separate values (.csv) file that contains the switch system MAC address, if available. If not available, consult Dell customer support.
5. Use the wiring plan to rack and cable the hardware according to the fabric design wiring plan.
6. Document the location of the switches, including the rack and row.
7. Document the system MAC address and name of the switches in the fabric so that you can map the address to the appropriate switch.
8. Select the fabric you are performing pre-deployment on at the **Network >** *Fabric Name* > **Configure and Deploy** > **Pre-deployment Configuration** screen.

Importing an Existing Fabric Design

To import an existing fabric design:

1. Navigate to the **Home** > **Getting Started** screen.
2. Click the **Importing Existing Design** option.

The **Import Existing Design** screen displays.

3. In the **Fabric XML file** area, click the **Browse** button and locate the fabric XML design file (the XML design that you have exported from the AFM design wizard).
4. Click the **Upload** button.

Editing and Expanding an Existing Fabric Design

You can edit or expand an existing fabric from the **Getting Started** screen. After you initiated the pre-deployment configuration, you can only update the fabric description and port count for expanding uplinks and downlinks.

1. Navigate to the **Home** > **Getting Started** screen.
2. Click the **Edit Existing Fabric** button.

   The **Select a Fabric** screen displays.
3. Select a fabric to edit and then click the **OK** button.

   The **Fabric Designer** wizard displays.
4. Edit the fabric.

Deleting the Fabric

To delete a fabric:

1. Navigate to the **Network** > *Fabric Name* > Configure screen.
2. Select the fabric to delete.
3. Click the **Delete** button.

Viewing the Wiring Diagram

To view and export the wiring diagram of the fabric:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. Click the **View Wiring Plan** link.
3. If you want to display future switches and links, click the **Display future switches/links** option.
4. Click one of the following options:
   a) **Tabular Wiring Plan**
   b) **Graphical Wiring Plan**
   c) **Network Topology Plan**
5. Click the **Export** link to export the wiring plan.

7

Configuring and Deploying the Fabric

After you create a fabric at the **Network** > **Design Fabric** > **New Fabric** screen, you can configure and deploy the fabric at the **Network** > *Fabric Name* > **Configure and Deploy** screen. This screen contains the following options:

- **Deploy Fabric** — Prepares the fabric for deployment and deploys the fabric.
  - Pre-deployment Configuration
  - Deploying and Validate
  - View DHCP Configuration
- **Errors** — Displays errors in the fabric

  Related Links:
  - Deployment and Validation Errors

    Troubleshooting
- **CLI Configuration** — Template and custom configuration using the FTOS CLI commands.
  - Manage Templates
  - Associate Templates
  - Custom Configuration
  - Viewing Custom Configuration History
- **View Wiring Plan** — Displays the wiring plan in tabular, network topology, and graphical formats, which can be exported.

Related Links:

- Pre-deployment Configuration
- Using the Pre-deployment Configuration Wizard

Fabric Deployment Summary

Switch Configuration Phases and States

Table 11. Switch Configuration Phases and States

Phase	State	State Description
Design	Complete	Indicates that the design is complete for the switch. **NOTE:** At switch level, design Partial Complete is not tracked. Partial Complete is only tracked at the fabric level.

Pre-deployment Configuration	Required	Indicates that not all required Pre-deployment Configuration information was provided.
	Error	Indicates that an error occurred during file transfer (transfer of a minimum configuration file) to the FTP/TFTP server or an error occurred during automatic DHCP integration for the local DHCP server. **NOTE:** In a case of remote the DHCP server, no errors are reported for the DHCP integration step because it is not an automated step from the AFM; you are responsible for manually integrating the DHCP configuration.
	Complete	Indicates that Pre-deployment Configuration information is complete for the switch.
Deployment	Required	Indicates that deployment was never initiated for the switch or the Deployment state was reset due to a Design/Pre-deployment Configuration change. **NOTE:** Deployment can be initiated/re-initiated only if Pre-deployment Configuration is in a Complete state.
	In-progress	Indicates that deployment is in-progress and also provides the latest percentage complete information.
	Error	Indicates that deployment error exists.
	Complete	Indicates that deployment was successful for the switch.
Validation	Required	Indicates that validation was never initiated for the switch or the Validation state was reset due to a Design/Pre-deployment Configuration/Deployment change. **NOTE:** Validation can be initiated only if deployment is in a Complete state.
	In-progress	Indicates that deployment is in-progress and provides the latest percentage complete information.
	Error	Indicates that one or more validation errors exist.
	Complete	Indicates that validation was successful for the switch.

Operations Allowed in Each Fabric State

To determine which operations are allowed during the design, pre-deployment configuration, deployment, and validation states, use the following table.

Table 12. Operations Allowed in Each Fabric State

Design State	Pre-Deploy Configuration State	Deployment State	Validation State	Operation Allowed
Incomplete	Not Started	Not Started	Not Started	• Edit Fabric • Delete Fabric
Complete	Not Started	Not Started	Not Started	• View Wiring Plan • Edit Fabric (All fabric attributes) • Pre-deployment Configuration • Delete Fabric

Complete	Incomplete. The system MAC and IP address are not configured for the switches.	Not Started	Not Started	• View Wiring Plan • Edit Fabric (All fabric attributes except fabric name) • Pre-deployment Configuration • Delete Fabric
Complete	Partial Complete / Complete–Partial complete indicates that at least 1 switch has its system MAC and IP address configured.	Not Started	Not Started	• View Wiring Plan • Edit Fabric (All fabric attributes except fabric name) • Pre-deployment Configuration • View DHCP Configuration • Deploy and Validate Fabric • View Deployment and Validation Status • Delete Fabric
Complete	Partial Complete / Complete	In-progress	Not Started / In-progress / Stopped / Error / Complete	• View Wiring Plan • View DHCP Configuration • View Deployment and Validation Status • Delete Fabric
Complete	Partial Complete / Complete	Incomplete / Partial Complete / Complete Incomplete indicates that the AFM is in the middle of deploying the switches. Complete indicates all the switches in the distributed fabric are deployed.	Not Started / In-progress / Stopped / Error / Complete	• View Wiring Plan • Edit Fabric—Allow editing of all fabric attributes except fabric name, fabric type interlink over-subscription, port count, and expand fabric. • Expand Fabric—Port Count and uplink Configuration (allow additions in Configure Protocol Setting) • Pre-deployment Configuration • View DHCP Configuration • Deploy and Validate Fabric – Validation is only allowed when deployment is

				partial or fully complete • View Deployment and Validation Status • Delete Fabric

Using the Pre-deployment Wizard

Layer 2 VLT Fabric Pre-deployment

To prepare the Layer 2 VLT fabric for deployment, complete the following tasks using the **Pre-deployment Configuration** wizard.

1. Pre-deployment - Step 1: Uplink Configuration
2. Pre-deployment - Step 2: Configuring a VLT VLAN
3. Pre-deployment – Step 3: VLT Downlink Port Configuration
4. Pre-deployment – Step 4: Assign Switch Identities
5. Pre-deployment – Step 5: Management IP
6. Pre-deployment – Step 6: Software Images
7. Pre-deployment – Step 7: DHCP Integration
8. Pre-deployment – Step 8: Advance Configuration
9. Pre-deployment – Step 9: Output
10. Pre-deployment – Step 10: Summary

Layer 3 Distributed Core Fabric Pre-deployment

To prepare the Layer 3 Distributed Core fabric for deployment, complete the following tasks using the **Pre-deployment Configuration** wizard.

1. Pre-deployment – Step 1: Fabric Interlink Configuration
2. Pre-deployment – Step 2: Uplink Configuration
3. Pre-deployment – Step 3: Downlink Configuration
4. Pre-deployment – Step 4: Assign Switch Identities
5. Pre-deployment – Step 5: Management IP
6. Pre-deployment – Step 6: Software Images
7. Pre-deployment – Step 7: DHCP Integration
8. Pre-deployment – Step 8: Advance Configuration
9. Pre-deployment – Step 9: Output
10. Pre-deployment – Step 10: Summary

Pre-Deployment Configuration

To prepare the fabric for deployment, use the **Pre-deployment Configuration Wizard**. After you initiate the pre-deployment configuration, you can only update the fabric description and port count for expanding uplinks and downlinks.

Prerequisites

Before you begin:

1. Rack the equipment in the fabric.

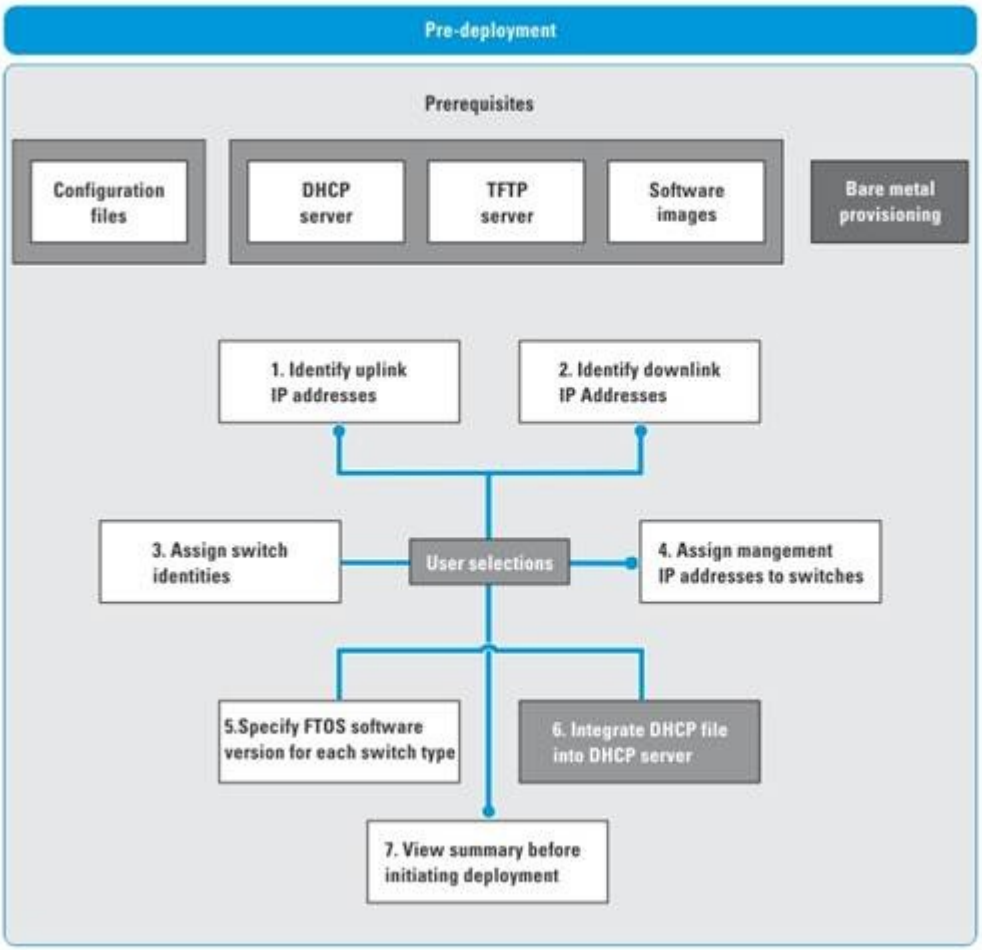
   NOTE: Before racking the switches, make sure that you have the **csv.** file that contains the system MAC addresses for each switch in the fabric. If you do not have this file, record the system addresses before you rack the switches.

2. Power off the switches in the fabric.

Gather the useful information listed in Gathering Useful Information for a Layer 3 Distributed Core Fabric or Gather Useful Information for a Layer 2 VLT Fabric.

Use the following pre-deployment flowchart as a guide to prepare the fabric for deployment.

Pre-Deployment Flowchart



NOTE: The pre-deployment flowchart does not list all the prerequisites. This flowchart does not include obtaining the fabric interlink and loop back IP address groups. For more information, see Pre-requisites.

Pre-Deployment Screens

To provide the fabric the minimum configuration to the switches, use the following **Pre-deployment** screens. These screens automate the deployment process.

- **Fabric Interlink Configuration** — (for a Layer 3 Distributed Core Fabric only) Configures options for the spine and leaf to communicate in the fabric.
- **Uplink Configuration** — Specify an even number of uplinks. The minimum number of uplinks is 2. One uplink is for redundancy.
  - For Layer 3 distributed core, an edge port link on the first two leaves that connects to the edge WAN, which typically connects to an internet service provider (ISP).
  - For a Layer 2 VLT fabric, an edge port link (uplinks) on the first two spines that connect outside the fabric.

- **Downlink Port Configuration** — (for a Layer 2 VLT fabric only) Associates each of the ports of a leaf (on a per leaf basis) to one or more VLANs. You can associated one or more tagged VLANs one and for untagged VLAN only one is allowed.
- **VLT VLAN Configuration** — (for a Layer 2 VLT fabric only) Specify a VLT VLAN to be applied to the Layer 2 fabric. Include at least one VLAN configuration.
- **Downlink Configuration** — An edge port that connects to the access layer; for example, servers or a ToR.
- **Assign Switch Identities**— Assigns a system MAC address to each switch in the fabric. You can optionally assign serial numbers and service tags to each switch.
- **Management IP** — Specifies a management IP address to each switch.
- **Software Images** — Specifies the TFTP or FTP address (local or remote server) and the path of the FTOS software image download to each type of switch. To stage the software, use this address.
- **DHCP Integration** — Creates a **dhcp.cfg** file that loads the correct software image and then a configuration file for each type of switch. The DHCP server also uses this file to assign a management IP address to each switch.

  NOTE: Install the DHCP configuration file on the DHCP server before you deploy the fabric.
- **Output** — Displays the uplink and downlink configuration on the leaves. Verify that this information is correct before deploying the switches.
- **Summary** — Displays the fabric name, location of the software image, and DHCP configuration file.

Protocol Configuration — Layer 3 Distributed Core Fabric: Step 1 — 3

To configure the pre-deployment protocol configuration for a Layer 3 distributed core fabric, complete the following tasks:

1. Pre-deployment – Step 1: Fabric Interlink Configuration
2. Pre-deployment – Step 2: Uplink Configuration
3. Pre-deployment – Step 3 Downlink Configuration

NOTE: For pre-deployment, the Layer 2 VLT and Layer 3 Distributed Core fabrics use the same pre-deployment configuration screens from step 4 through step 10. See also Using the Pre-deployment Configuration Wizard.

Pre-deployment – Step 1: Distributed Core Fabric Interlink Configuration

To configure the links that connect the leaves and spines for a Layer 3 distributed core fabric using the OSPF routing protocol, use the **Fabric Interlink Configuration** screen. The port bandwidth (a read-only field) is automatically determined by the selected fabric type and fabric oversubscription ratio (Layer 3 distributed core fabric only). To automate the pre-deployment process, AFM automatically populates the starting IP address range/prefix, loop IP address/prefix based on the fabric design, and sets the area ID for OSPF to "0". Review these settings. You can modify the IP address range and loopback address. The start prefix for both types of addresses must be from 8 to 29 and the loopback prefix from 8 to 26. Before you begin, review the Using the Pre-Deployment Wizard and Pre-deployment Wizard: Introduction sections.

For information about how to configure a Layer 2 VLT Fabric Interlink Configuration, see Pre-deployment – Step 1: VLT Fabric Interlink Configuration

CAUTION: The area ID for the interconnect link must not be the same as the area ID specified for the uplink.

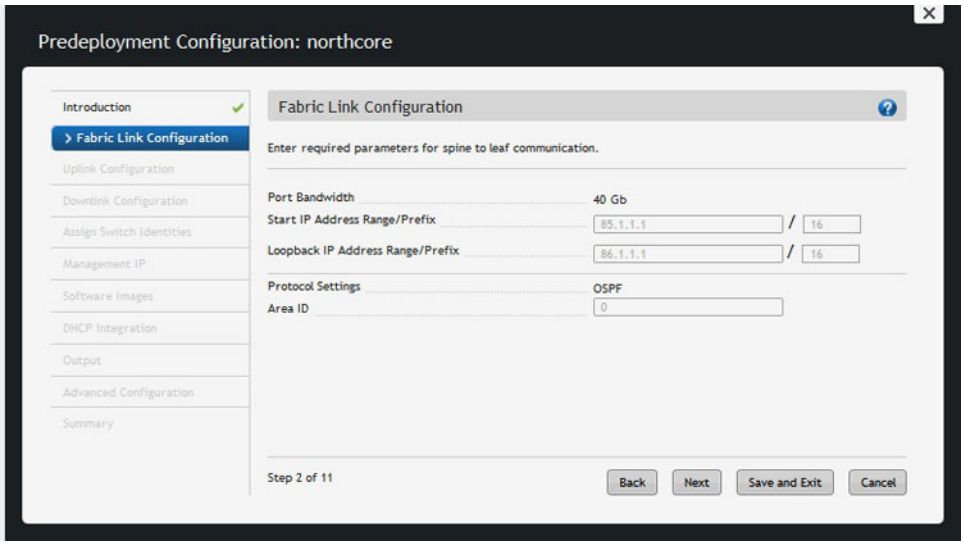


Figure 17. Fabric Link Configuration

To configure the Fabric Link Configuration for a Layer 3 distributed core fabric:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **Deploy Fabric** pull-down menu, select the **Pre-Deployment Configuration** option.
   The **Introduction** screen displays.
3. Review the **Introduction** screen and gather the useful information to prepare your fabric for deployment.
4. Click the **Next** button.
   The **Fabric Link Configuration screen** displays.
5. In the **Start IP Address Range/Prefix** area, enter the starting IP address and prefix.
   The prefix must be from 8 to 29.
6. In the **Loopback IP Address Range/Prefix** area, enter the loopback address range and prefix.
   The prefix must be from 8 to 26.
7. In the **Area ID** field, use the default setting of "0" or enter the area ID.
   The area ID is a value from 0 and 65535. The uplinks or interlinks must be in area 0 for OSPF.

Pre-deployment – Step 2: Uplink Configuration (Distributed Core Fabric)

The **Uplink Configuration** page displays the port bandwidth and the number of specified ports (read-only fields) entered on the **Fabric Name and Type** and **Port Specification** screens. To configure the uplink protocol for the edge port uplinks to the WAN, use the **Uplink Configuration** screen. For information about for a uplinks for a Layer 3 distributed core fabric, see Distributed Core Terminology.

NOTE: When the Open Shortest Path First (OSPF) is selected for both uplinks and interlinks, one of uplinks or interlinks must be in area 0.

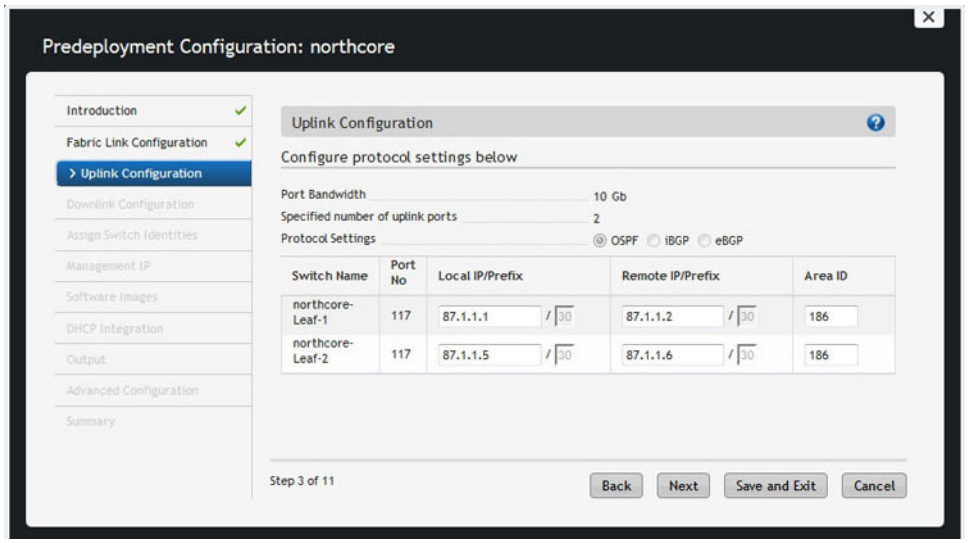


Figure 18. Layer 3 Uplink Configuration

To configure the uplink protocol for the edge port uplinks to the WAN for a Layer 3 distributed core fabric:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **Deploy Fabric** pull-down menu, select the **Pre-deployment Configuration** option.
3. Navigate to the **Uplink Configuration** screen.
4. In the **Protocol Settings**, select a routing protocol (OSPF, IBGP, or eBGP) for the edge port uplinks. The number of uplinks is specified in the **Port Specification** screen.

   The AFM automatically populates the range of IP addresses belong to the **/30** subnet.

   a) For OSPF, for each specified uplink, enter the local IP address, remote neighbor IP address, and area ID. A valid area ID area is from 0 to 65535.
   b) For iBGP, for each specified uplink, enter the local IP address, remote neighbor IP address, local AS number. For the AS number, enter a value from 1 to 4294967295.
   c) For eBGP, for each specified uplink, enter the local IP, remote neighbor IP address, local AS number, and remote AS number. For the AS number, enter a value from 1 to 4294967295.
5. Click **Next** to go the **Downlink Configuration** screen.

Pre-deployment – Step 3: Downlink Configuration

Downlinks are edge port links which connect to servers, switches, or ToRs. When you enable the ToR configuration, the leaves function as a ToR. When you disable the ToR configuration, the leaves function as a switch. The port bandwidth for the downlinks is 1 GbE or 10 GbE (a read-only field). For more information about downlinks, see Distributed Core Terminology and VLT Terminology.

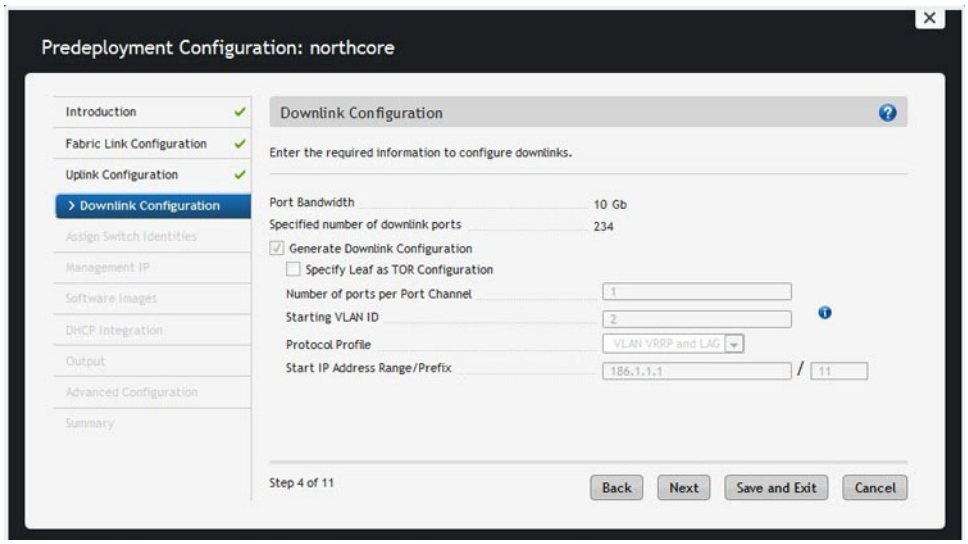


Figure 19. Downlink Configuration for Layer 3 Distributed Core Fabric

To configure the downlinks for a Layer 3 distributed core fabric:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **Deploy Fabric** pull-down menu, select the **Pre-deployment Configuration** option.
3. Navigate to the **Downlink Configuration** screen.
4. Select the **Specify Leaf as ToR** option if you want to the leaves to act as a ToR.
5. Manually configure the downlinks, or to automatically generate the downlink configuration, uncheck the **Generate Downlink Configuration** option.
6. In the **Start IP Address Range/Prefix** field, enter the starting IP address and prefix.

   Enter a valid IP address and a prefix from 8 to 23.
7. In the **Number of ports per port channel**, enter the number of ports assigned to a port channel for a particular VLAN ID.

   Range: from 1 to 16.
8. In the **Starting VLAN ID** field, enter a starting VLAN ID.

   Range: from 2 and 4094.
9. From the **Protocol Profile** pull-down menu, when the leaves are acting as a leaf switch (the switches are directly connected to the server), select the **Downlink VLAN and VRRP and LAG** protocol setting. The default setting is **Downlink VLAN**.
10. Click **Next** to go the Pre-deployment Configuration – Step 4: Assign Switch Identities screen.

Protocol Configuration — Layer 2 VLT Fabric: Step 1 – 3

The pre-deployment protocol configuration for VLT consists of the following tasks:

- Pre-deployment – Step 1: Uplink Configuration (VLT)
- Pre-deployment – Step 2: VLT VLAN Configuration
- Pre-deployment – Step 3:VLT Downlink Port Configuration

NOTE: For pre-deployment, the Layer 2 VLT and Layer 3 Distributed Core fabrics use the same pre-deployment configuration screens from step 4 through step 10.

Pre-deployment – Step 1: Uplink Configuration (VLT)

The **Uplink Configuration** page displays the port bandwidth and the number of specified ports (read-only fields) entered on the **Fabric Name and Type** and **Port Specification** screens. To configure the uplink protocol for the edge port uplinks to the WAN, use the **Uplink Configuration** screen. For information about uplinks, see VLT Terminology.

NOTE: For OSPF, the uplinks or interlinks must be in area 0.

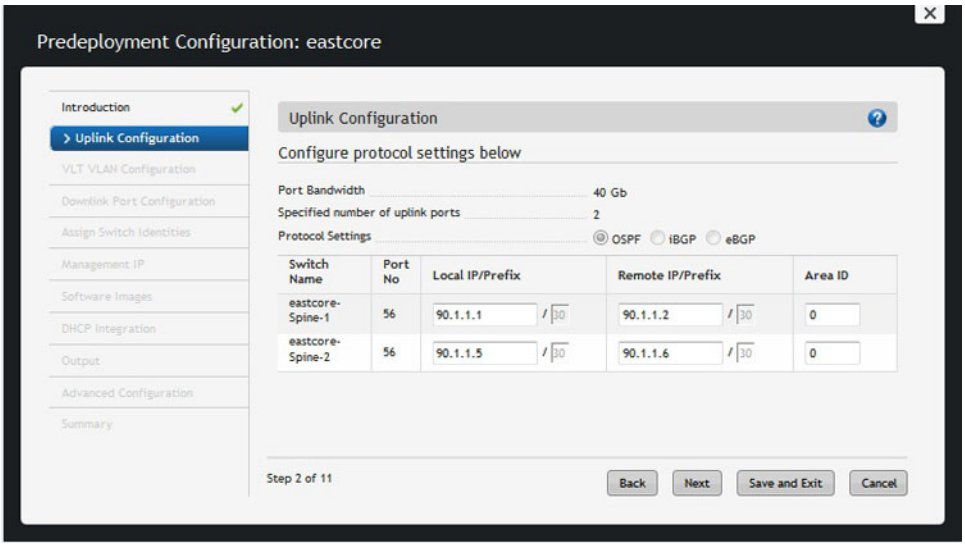


Figure 20. Layer 2 VLT Uplink Configuration

To configure the uplink protocol for the edge port uplinks to the WAN:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **Deploy Fabric** pull-down menu, select the **Pre-deployment Configuration** option.
3. Navigate to the **Uplink Configuration** screen.
4. In the **Protocol Settings**, select a routing protocol (OSPF, IBGP, or eBGP) for the edge port uplinks. The **Port Specification** screen specifies the number of uplinks.

   The range of IP addresses belong to the **/30** subnet is automatically populated by the AFM.

   - For OSPF, for each specified uplink, enter the local IP address, remote neighbor IP address, and area ID. A valid area ID area is 0 to 65535.
   - For iBGP, for each specified uplink, enter the local IP address, remote neighbor IP address, local AS number. For the AS number, enter a value from 1 to 4294967295.
   - For eBGP, for each specified uplink, enter the local IP, remote neighbor IP address, local AS number, and remote AS number. For the AS number, enter a value from 1 to 4294967295.
5. Click **Next** to go the **VLT VLAN Configuration** screen.

Pre-deployment - Step 2: Configuring a VLT VLAN

To specify a VLT VLAN to be applied to the Layer 2 fabric, use this screen. Specify at least **one** VLAN configuration.

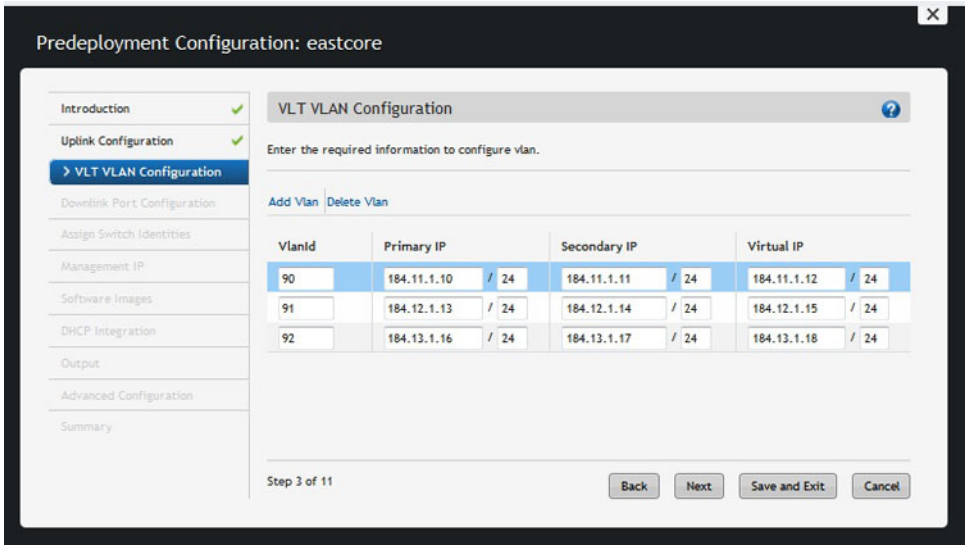


Figure 21. VLT VLAN Configuration

Table 13. VLT VLAN Configuration Options

Field Name	Description
VLAN Id	Enter the VLAN Id. Range: from 1 to 4094 **Default**: <Blank>
Primary IP	Enter the primary IP address. The prefix is auto-populated. Validation Criteria for Primary IP: Valid IP Prefix Range: from 8 to 29 **Default** Primary IP: <Blank> **Default** Prefix: 24
Secondary IP	Enter the secondary IP address. The prefix is auto-populated. Address for Secondary IP: Valid IP Prefix range: from 8 to 29 **Default** Secondary IP: <Blank> **Default** Prefix: 24
Virtual IP	Enter the virtual IP address. The prefix is auto-populated. Address for Virtual IP: Valid IP Prefix range: from 8 to 29 **Default** Virtual IP: <Blank> **Default** Prefix: 24

To configure a VLT VLAN:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **Deploy Fabric** pull-down menu, select the **Pre-deployment Configuration** option.
3. Navigate to the **VLT VLAN Configuration** screen.
4. Click the **Add Vlan** link.

5. In the **VlanId** field, enter the VLAN ID.
6. In the **Primary IP addre**ss field, enter the primary IP address.
7. In the **Seconday IP** address field, enter the secondary IP address.
8. In the **Virtual IP** address field, enter the virtual IP address
9. Click the **Next** button to view the **Downlink Port Configuration** screen.

Pre-deployment – Step 3: VLT Downlink Port Configuration

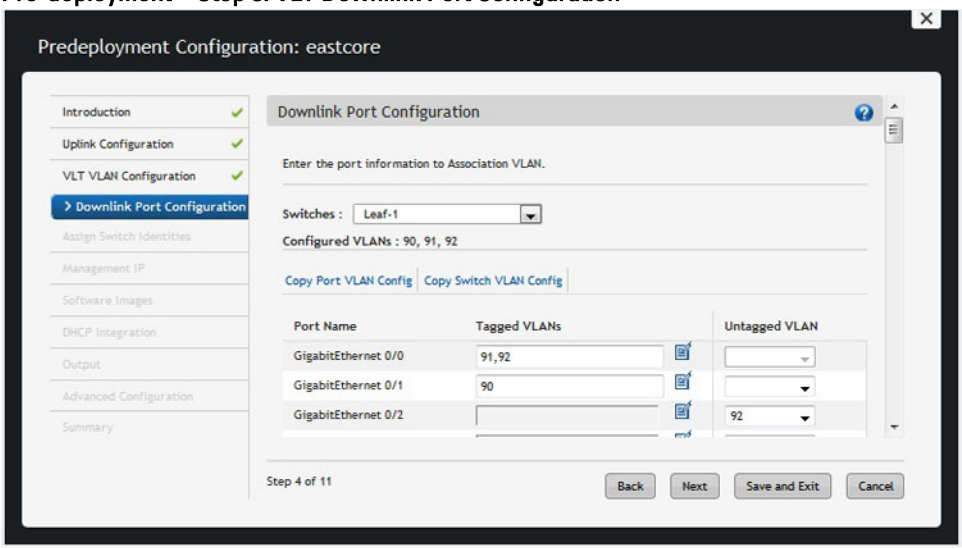


Figure 22. Layer 2 VLT Downlink Port Configuration

To add VLANs and associate ports on the different leaves to which VLAN, use the **Downlink Port Configuration** screen. Once that is done you can copy switch VLAN or port VLAN configurations. You can be associate one or more tagged VLANs with a port and for untagged VLAN only one is allowed. For information about Downlinks, see VLT Terminology.

Table 14. Layer 2 VLT Downlink Port Field Descriptions

Field Name	Description
Configured VLANs	Displays list of VLANs specified in the VLT VLAN Configuration screen.
Port Name	Displays the port name. This a *read only* field.
Tagged VLANs	**Manual Entry**: Enter one or more VLANs to associate with the port. Validation Criteria: The VLANs have to be from the Configured VLANs list and the Untagged VLAN field should be empty. Default: <Blank> 1. Select from the list (click on the icon next to the field entry) 2. Select one or more VLANs to be associated with the port.
Untagged VLANs	Select a VLAN to associate with the port from the drop down list. Validation Criteria: Tagged VLAN field should be empty. Default: <Blank>

Table 15. Layer 2 Downlink Port Options

Option	Description
Copy Switch VLAN Config	Copies the VLAN association from the current switch to other switch(es) in the fabric.
Copy Port VLAN Config	Copies the VLAN association from a selected port to other port(s) within a switch.

To configure downlink ports on the leaf switches:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **Deploy Fabric** pull-down menu, select the **Pre-deployment Configuration** option.
3. Navigate to the **Downlink Port Configuration** screen.
4. From the **Switches** pull-down menu, select a leaf switch.
5. In the **Tagged VLANs**, click on the icon next and enter one or more VLANs to be associated with the port.
6. When you are finished, click the **Next** button to go to the **Pre-deployment: Step 4**: — **Assign Network Identities** screen.

Pre-deployment – Step 4: Assign Switch Identities

To assign the system MAC addresses to the switches in the fabric, use the **Assign Switch Identities** page. Entering the serial numbers and service tags. Load the CSV file that contains the system MAC addresses, serial numbers, and service tags for the switches in the fabric.

The following is a sample CVS file.

Table 16. Sample CVS Format

serial_number	purchase_order	mfg_part_number	mac_address
00AS104600860	163	S4810-01-GE-44T-AC-R	00:01:E8:8B:15:86

NOTE: Before you begin, obtain the CSV file that contains the system MAC addresses, service tag, and serials numbers for each switch provided from Dell manufacturing or manually enter this information.

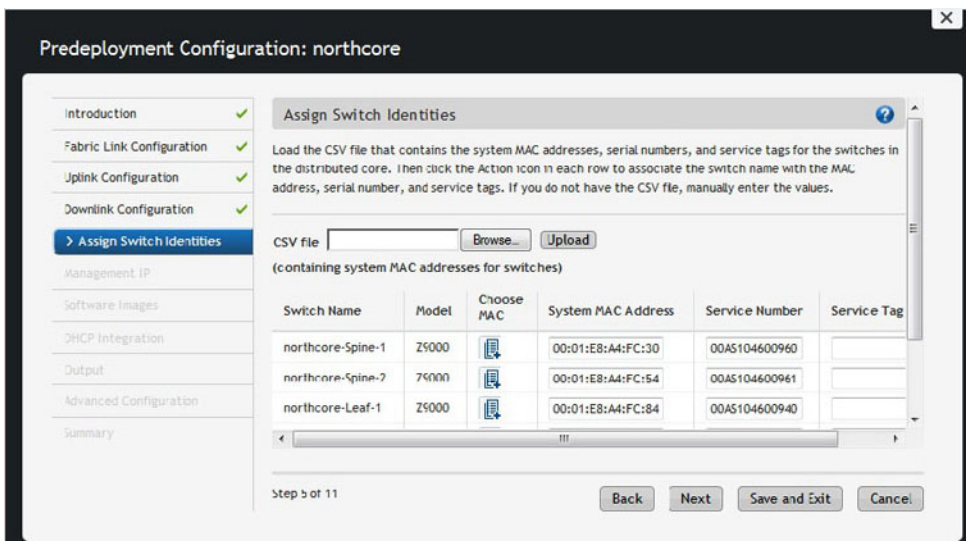


Figure 23. Assign Switch Identities

To assign switch identities:

1. Locate the CSV file that contains the system MAC addresses, serial numbers, and service tags for the switches in the fabric. Contact your Dell Networking sales representative for this file.
2. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
3. From the **Deploy Fabric** pull-down menu, select the **Pre-deployment Configuration** screen option.
4. Navigate to the **Assign Switch Identities** screen.
5. Click the **Browse** button and specify the path of the CSV file. If you do not have this file, manually enter this information in the **System MAC Address** fields.
6. Click the **Upload** button.
7. Click the **Action** icon in each row to associate the switch name with the MAC address, serial number, and service tags using the CVS file or manually enter this information.
8. Map the system MAC address, serial number, and service tag to each switch.
9. Click **Next** to the go to the **Assign Management IP** screen.

Pre-Deployment – Step 5: Management IP

To assign a management IP address to each switch in the fabric, use the **Management IP** screen.

NOTE: Before you begin, gather the addresses for all the switches in the Layer 2 or Layer 3 fabric for the management port. All management switch IP addresses must be on the same subnet.

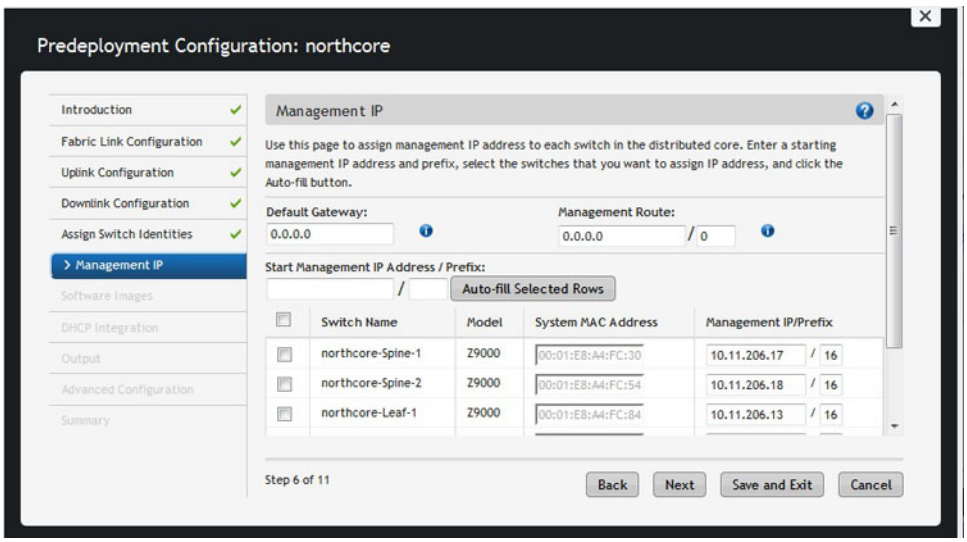


Figure 24. Assign Management IP to Each Switch in the Fabric

To assign a management IP address to the switches in the fabric:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **Deploy Fabric** pull-down menu, select the **Pre-deployment Configuration** option.
3. Navigate to the **Management IP** screen.
4. In the **Default Gateway** field, enter the address of the default gateway for the management interface.
5. In the **Management Route** field, enter the route and prefix of the management interface.
6. In the **Start Management IP Address/Prefix** fields, enter the starting management IP address and prefix.
7. Select the switches to assign a management IP address.

8. Click the **Auto-fill Selected Rows** button.
   The system automatically assigns a management IP address to all the selected switches in the fabric.
9. Click **Next** to go to the **Software Images** screen.

Pre-Deployment – Step 6: Software Images

To specify which software images to stage for each type of switch in the fabric from a TFTP or FTP site, use the **Software Images** screen. The software image must be the same for each type of platform. Place the software image(s) for the switches on the TFTP or FTP site so that the switches can install the appropriate FTOS software image and configuration file. To change the address of the TFTP or FTP site, navigate to the **Administration > Settings** screen.

NOTE: Before you begin, make sure that you have loaded the software image for each type of switch on to the TFTP or FTP site.

NOTE: To download the latest FTOS switch software version, see the Upload Switch Software" section in the *AFM Installation Guide*.

To specify which software images to load onto each switch in the fabric from the TFTP or FTP site:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **Deploy Fabric** pull-down menu, select the **Pre-deployment Configuration** option.
3. Navigate to the **Software Images** screen.
4. Select the **TFTP** or **FTP** site option that contains the software image.
5. Enter the path of the software image(s) to the TFTP or FTP site.
6. Click **Next** to go to the **DHCP Integration** screen.

Pre-Deployment – Step 7: DHCP Integration

The **DHCP Integration** screen uses the information configured at the **Assign Switch Identities**, **Management IP**, and **Software Images** screens to create a DHCP configuration file named **dhcpd.cfg**, which contains the following information:

- System MAC addresses and fixed management IP addresses for each switch in the fabric
- Location of the software images and configurations for the switches on the TFTP or FTP server

You can automatically integrate the file into the AFM local DHCP server by using the default setting **Local (AFM provisioned to be a DHCP server)** The AFM automatically generates a switch configuration file and transfers it to the local DHCP server on AFM. When you select the **Remote (External DHCP server)** option, manually integrate the DHCP configuration into the external DHCP server.

After you power cycle the switches, the switches use BMP.

BMP provides the following features:

- Automatic network switch configuration
- Automated configuration updates
- Enforced standard configurations
- Reduced installation time
- Simplified operating system upgrades

Automated BMP reduces operational expenses, accelerates switch installation, simplifies upgrades, and increases network availability by automatically configuring Dell Networking switches. BMP eliminates the need for a network

administrator to manually configure a switch, resulting in faster installation, elimination of configuration errors, and enforcing standard configurations.

With BMP, after a you install a switch, the switch searches the network for a DHCP server. The DHCP server provides the switch with a management IP address and the location of a TFTP or FTP file server. The file server maintains a configuration file and an approved version of FTOS for the Dell Networking S55, S60, S4810, S4820T, Z9000, and MXL Blade switches. The switch automatically configures itself by loading and installing an embedded FTOS image with the startup configuration file.

For more information about BMP, refer to the *Open Automation Guide* at https://www.force10networks.com/CSPortal20/KnowledgeBase/Documentation.aspx . Select the **Open Automation** heading.

Important: When you enter the system MAC address into the **Assign Switch Identities** screen, the AFM generates a port MAC address from the pre-deploy configuration, not a chassis MAC address.

1. **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **Deploy Fabric** pull-down menu, select the **Pre-deployment Configuration** option.
3. Navigate to the **DHCP Integration** screen.
4. Click **Save to ...** and then specify the location to save the generated DHCP configuration file. You can also copy and paste the configuration into the DHCP server.
5. Install the DHCP file onto the DHCP server before your deploy the fabric.

   Important: Install the DHCP configuration file onto your DHCP server before you deploy the fabric.
6. Click **Next** to go to the **Advance Configuration** screen.

Pre-Deployment – Step 8: Advance Configuration

Use the **Advance Configuration** screen to do the following:

- View the Auto-Generated Configuration
- Associate Templates to Fabrics

  NOTE: You must first create a template for a fabric before you can associate it. For more information, see Adding Templates
- Add Switch Specific Custom Configuration
- Preview Combined Configuration

View the Auto-generated Configuration

To view the AFM auto-generated configuration:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **CLI Configuration** pull-down menu, select the **Custom Configuration** option.

   The **Switch Specific Custom Configuration** screen is displayed.

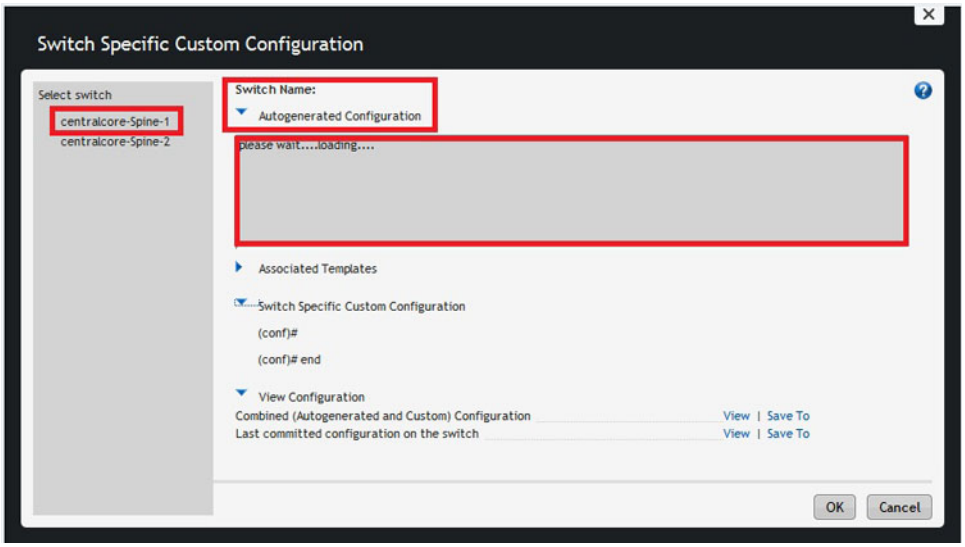


Figure 25. View Autogenerated Configuration

3. Click on the arrow next to the **Autogenerated Configuration** option to view its contents.

Associating Templates

You can associate one or more existing configuration templates to the fabric (entire fabric), all spines, all leaves or a set of switches. When a template is associated to an entire fabric or all spines or all leaves, the template gets automatically applied to the newly added switches (instead of the you having to create new associations manually).

Important: Each template can have only one association per fabric. The AFM does not support the ordering of templates for sequencing the commands. If you want to do this, we recommend that you manually combine the templates into a single template.

To associate a template:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **CLI Configuration** pull-down menu, select the **Associate Templates** option.
   The **Associate Templates** screen displays:
3. Click the **Add Association** link.
4. In the **Template Name** pull-down menu, select the template that you want to use.
5. (Optionally) In the **Comments** field, enter your comments.
6. In the **Select Association** area, select one the following options:
   a) **Fabric** — Associates template to all the switches in the fabric.
   b) **Spines** — Associates template to all the spine switches.
   c) **Leafs** — Associates template to all the leaf switches.
   d) **Custom** — Associates template with specific switches. In the **Available Switches**, select the switches that you want to associate the template with.
7. Click the **Apply** button.

Adding a Switch-Specific Custom Configuration

Before editing the existing configuration, backup the existing running configuration in the flash with a unique name consisting of the date and time.

To create and apply a customized switch-specific configuration and deploy it:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **CLI Configuration** pull-down, select the **Custom Configuration** option.
3. In the left navigation pane, select the switch to apply the switch specific-custom configuration to.

   The Switch Specific Custom Configuration screen displays.

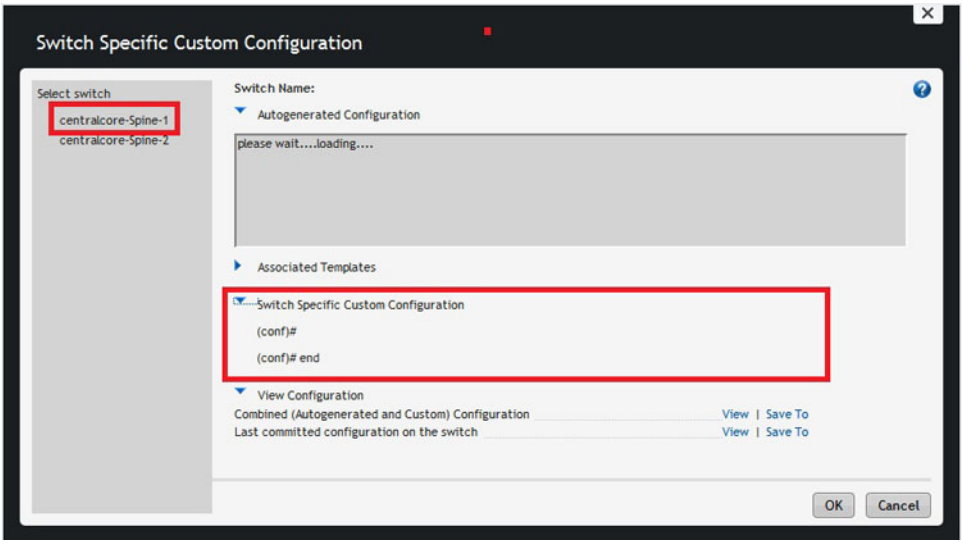


Figure 26. Switch Specific Custom Configuration

   The **Switch Specific Custom Configuration** screen provides support to view the auto-generated configuration and switch-specific custom configuration that is applied to the individual switches in the fabric. Only the switches that are deployed are listed.

4. Enter the switch specific-custom configuration (FTOS CLI commands) in the **Switch Specific Custom Configuration** area.
5. Under the **View Configuration** heading, click the **View** button next to the **Preview the combined auto-generated and custom configuration**. This option allows you to view the auto-generated configuration, global custom configuration, and switch specific configuration.

   The **View Combined Configuration** screen displays.
6. To view the last applied configuration or save it, click the **View** button or **Save To…** button next to the **Last committed configuration on the switch** area. The AFM displays the timestamp for the last committed configuration on the switch.
7. Review the combined configuration and make any necessary changes.
8. Click the **Save To ...** button to save the combined auto-generated and custom configuration.
9. Click the **Close** button.

Preview Combined Configuration

1. Navigate to the **Network** > *Fabric Name* > *Switch Name* screen.
2. From the **CLI Configuration** pull-down menu, select the **Custom Configuration** option.

   The **Switch Specific Custom** displays.
3. In the **Combined (Autogenerated and Custom) Configuration** area, click the **View** link. You can also save the combined configuration using the **Save To ..** option.

Pre-Deployment – Step 9: Output

To review the uplinks or downlinks for each switch in the fabric, use the **Pre-deployment Output** screen.

To view the uplinks and downlinks for each switch in the fabric:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **Deploy Fabric** pull-down-menu, select the **Pre-deployment Configuration** option.
3. Navigate to the **Output** screen.
4. From the **View** pull-down menu, select one of the following options:
   a. **Downlink Output**
   b. **Uplink Output**
5. Click **Export** to export this information.
6. Click **Next** to go to the **Summary** screen.

   NOTE: Only hardware inventory for the fabric interlinks (the connections between the spines and leaves) display in the pre-deployment summary screen.

Pre-Deployment – Step 10: Summary

To review the pre-deployment configuration, use the **Summary** screen . This screen displays the following information:

- Specified IP and protocol settings for the fabric, uplink, and downlink configuration
- Software image information for each type of switch
- Configuration file transfer status to the remote or local TFTP or FTP server

To view the pre-deployment configuration:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **Deploy Fabric** pull-down menu, select the **Pre-deployment Configuration** option.
3. Navigate to the **Summary** screen.
4. Carefully review the pre-deployment configuration before you commit it.
5. Click **Finished** button to commit the your changes.

Next Steps:

1. Verify that the DHCP configuration file that you created for the fabric is integrated into the DHCP server so that the switches are assigned a management IP address before you deploy the fabric.
2. Power on the switches in the fabric when you have completed the pre-deployment process. After you power cycle the switches, the switches use bare metal provisioning (BMP).

   Important: If you are using a switch that has already been deployed, you must reset its factory settings to use it in the fabric. The switch must be in BMP mode. For more information about BMP, see Pre-Deployment – Step 7: DHCP Integration and refer to the *Open Automation Guide* at https://www.force10networks.com/CSPortal20/KnowledgeBase/Documentation.aspx . Select the Open Automation heading.
3. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
4. From the **Deploy Fabric** pull-down menu, to deploy and validate the fabric, select the **Deploy** and **Validate** option.

Viewing the DHCP Configuration File

NOTE: If you are using an IE browser with the Windows 7 OS, change your indexing options:

1. Navigate to the **Control Panel->Indexing Options** screen.
2. Click the **Advanced** button and then click on the **File Types** Tab.
3. In the **Add new extension to list**: field, enter "conf" as the extension file type and then click the **Add** button.
4. Click the **OK** button.

To view the DHCP configuration file created for the fabric:

1. Navigate to the **Network >** *Fabric Name*> **Configure and Deploy** screen.
2. From the **Deploy Fabric** pull-down menu, select the **View DHCP Configuration** option.
3. From the **Deploy** pull-down menu, select **View DHCP Configuration**. For more information on DHCP, see Pre-Deployment – Step 5: DHCP Integration.

Deploying and Validating the Fabric

This section contains the following topics:

- Deploying the Fabric
- Validating the Fabric
- Viewing Deployment and Validation Status

Deploying the Fabric

To deploy the fabric, use the **Deploy** screen. Make sure that the fabric matches the deployed fabric. AFM prompts you to fix any errors when you deploy the fabric. To view the DHCP configuration file for the selected fabric, navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen. From the **Deploy Fabric** pull-down menu, select the **View DHCP Configuration** option.

To view a custom configuration file, navigate to the **Network >** *Fabric Name*> **Configure and Deploy** screen. From the **CLI Configuration** pull-down menu, select the **Custom Configuration** option.

Use the following Deployment Status table to troubleshoot deployment issues.

Table 17. Deployment Status

Deploy			
Sl.No	Status	Status Details	Recommended Action
1	Required	Deployment Required	NA
2	Complete	Deployment successfully completed.	NA
3	Error	Protocol transfer failed	Verify TFTP/FTP connectivity; verify FTP credentials.
5	Error	Device cleanup task failed	1. From the AFM, verify the switch connectivity using Telnet or SSH.

			2. Restart the deployment of the switch from the **Network** > *Fabric Name* > **Configure and Deploy** screen by selecting the switch from the list and then click on the **Deploy Selected** link.
6	Error	Complete config upload failed	1. Verify TFTP/FTP or Telnet/SSH connectivity. For FTP, verify credentials. 2. Restart the deployment of the switch from the **Network** > *Fabric Name* > **Configure and Deploy** screen by selecting the switch from the list and then click on the **Deploy Selected** link.
7	Error	Smart script transfer failed	NA
8	Error	Custom config upload failed	Verify the login and configuration commands on the switch.
9	Error	Backup config failed	1. Verify Telnet or SSH connectivity from the AFM. 2. Restart the deployment of the switch from the **Network** > *Fabric Name* > **Configure and Deploy** screen by selecting the switch from the list and then click on the **Deploy Selected** link.
10	InProgress	Verifying that the switch is eligible for the deploy process	NA
11	InProgress	Protocol transfer in progress...	NA
12	InProgress	Device cleanup task done, reload in progress...	NA
13	InProgress	Complete config upload in progress...	NA
14	InProgress	Smart script transfer Inprogress...	NA
15	InProgress	Custom config upload in progress...	NA
16	InProgress	Backup config in progress...	NA
17	InProgress	Merged config upload in progress...	NA

To deploy a fabric:

1. Verify that the software images for the switches are installed on to the TFTP or FTP server.
2. Verify that you have configured the correct TFTP or FTP address at the **Administration > Settings** screen. Changing the TFTP server now does not correct the address unless you redo the pre-deployment.
3. For a remote DHCP server only, verify that the DHCP configuration file generated by the AFM for the switches in the fabric is integrated into the DHCP server. This file enables the switch to connect to the DHCP server and download the correct configuration and boot.

4. Restart the DHCP server that contains the generated DHCP file that you created in the **DHCP Integration** screen. For information about DHCP integration, see Pre-Deployment Wizard – Step 7: DHCP Integration
5. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
6. From the **Deploy Fabric** pull-down menu, select the **Deploy and Validate** option.

   The **Deploy and Validate** screen displays.
7. On the **Deploy** tab, select the spines and leaves that you want to deploy in the **Switch** column.
8. Power up the selected switches. The switches must be IP ready.
9. Click the **Deploy Selected** link and wait for the fabric to deploy.
10. Check the progress and status of the deployment in the **Status**, **Status Details**, **Response Actions**, and **Last Deployed** columns.

    For information about how to view validation errors, see Validation Status and Errors. See also Troubleshooting. For information about the progress and status of selected switches and operations allowed during a fabric state, see Operations Allowed During Each Fabric State and Understanding Fabric Phases.

Validation

To verify that the discovered fabric matches the planned fabric and correct any errors, use the **Validate** screen . Mismatches are reported as errors and the corresponding alarms generate. If you fix the errors found during validation, to verify that all the issues were fixed according to the planned fabric, validate the fabric again.

Validation Status

Validation			
Sl. No	**Status**	**Status Details**	**Response Action**
1	Required	Validation Required	NA
2	Complete	Validation completed.	NA
3	Error	HOSTNAME/MAC Address/MODEL Mismatch	Check for switch mismatch errors: 1. Navigate to the **Network** > *Fabric Name* > **Configure and Deployment** screen. 2. Click the **Errors** link. 3. Click on the **Discovered Errors** tab to view error details. 4. Fix any errors.
4	Error	HOSTNAME/MAC Address/MODEL Mismatch and STANDBY UNIT down	Check for switch mismatch errors: 1. Navigate to the **Network** > *Fabric Name* > **Configure and Deployment** screen. 2. Click the **Errors** link. 3. Click on the **Discovered Errors** tab to view error details. 4. Fix any errors.
5	Error	STANDBY UNIT down	1. Navigate to the **Network** > *Fabric Name* > **Configure and Deployment** screen.

			2. Click the **Errors** link. 3. Click on the **Discovered Errors** tab to view error details. 4. Fix any errors.
6	Error	Switch is not reachable	Verify the switch connectivity from the AFM. 1. Navigate to the **Network** > *Fabric Name* > **Configure and Deployment** screen. 2. Click the **Errors** link. 3. Click on the **Discovered Errors** tab to view error details. 4. Fix any errors.
7	Error	Switch is not Discovered	Verify the switch connectivity from the AFM. 1. Navigate to the **Network** > *Fabric Name* > *Switch Name* > Troubleshoot screen. 2. Click the **Errors** link. 3. Click on the **Undiscovered Errors** tab to view error details. 4. Fix any errors.
8	Error	Configuration mismatch errors exists	Check for switch configuration mismatch errors: 1. Navigate to the **Network** > *Fabric Name* > **Configure and Deployment** screen. 2. Click the **Errors** link. 3. Click on the **Config Mismatch Errors** tab to view error details. 4. Fix any errors.
9	Error	Custom Configuration errors exists	Check for switch custom configuration errors: 1. Navigate to the **Network** > *Fabric Name* > **Configure and Deployment** screen. 2. Click the **Errors** link. 3. Click on the **Custom Config Errors** tab to view error details. 4. Fix any errors.
10	Error	Wiring Errors Exists	Verify the Errors in the **Wiring Error** tab.

			1. Navigate to the **Network** > *Fabric Name* > **Configure and Deployment** screen. 2. Click the **Errors** link. 3. Click on the **Wiring Errors** tab to view error details. 4. Fix any errors.
11	InProgress	Node validation in progress...	NA
12	InProgress	Configuration Validation in progress...	NA
13	InProgress	Wiring Validation in progress...	NA

Validating the Fabric

To verify that the discovered fabric matches the planned fabric and correct any errors:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
   The **Configure and Deploy** screen displays.
2. In the **Switch** column, select the switches to validate.
3. Click the **Validate Selected** link.
4. Review the progress in the **Status**, **Status Details**, **Response Actions**, and **Last Validated** columns.
5. Correct any errors.
6. If you fix the errors found during validation, to verify that all the issues were fixed according to the planned fabric, validate the fabric again.

Viewing Deployment and Validation Status

To view the deployment and validation status of the fabric.

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. Select the fabric that you want to view.
3. From the **Deploy Fabric** pull-down menu, select the **Deploy and Validate** option.
   You can also view the status of the fabric deployment at the **Network** > *Fabric Name* > **Configure and Deploy** > **Errors** screen.

Custom CLI Configuration

This section contains the following topics.

- Managing Templates
- Associating Templates
- Viewing Custom Configuration History
- Switch Specific Custom Configuration

Managing Templates

This section contains the following topics:

- Adding Templates
- Editing Templates
- Deleting Templates
- Copying Templates

Adding Templates

You can add (create) a CLI configuration template. This is useful for applying a custom configuration to the following:

- Specific switches in a fabric
- All the switches in the fabric
- All the leafs in the fabric
- All the spines in the fabric

1. Navigate to the **Network** > *Fabric* > **Configure and Deploy** screen.
2. From the **CLI Configuration** pull-down, select the **Associate Template** option.
   The **Templates** screen displays.
3. Click the **Add Template** link.
4. In the **Template Name** field, specify a unique name for the template.
5. (Optional) In the **Description** field, enter a description of the template.
6. In the **Configuration Commands:** area, enter the CLI (FTOS) configuration commands that you want to include in the template.
7. Click the **OK** button.

For information about how to associate a template to a switch or fabric, see Associating Templates.

Editing Templates

1. Navigate to the **Network** > *Fabric* > **Configure and Deploy** screen.
2. From the **CLI Configuration** pull-down menu, select the **Manage Templates** option.
   The **Templates** screen displays.
3. Select the template that you want to edit.
4. Click the **Edit Template** link.
   The **Edit Template** window displays.
5. (Optional) In the **Template Name** field, enter a description of the template.
6. In the **Configuration Commands** area, edit the CLI (FTOS configuration).
7. Click the **OK** button.

Deleting Templates

Before you delete a template, make sure that template is not being used. You cannot delete a template when it is associated with one or more switches. You can only delete templates that are not being used. You can only delete one

template at a time. If you attempt to delete a template that is being used, AFM displays an error message indicating which fabric(s) the template is associated with.

NOTE: To delete a template, you must have superuser or administrator privileges.

1. Navigate to the **Network** > > **Configure and Deploy** screen.
2. From the **CLI Configuration** pull-down menu, select the **Delete Template** option.
3. Click **OK**.

Copying Templates

You can copy an existing template, modify it, and then apply it to fabric or switch. For information on how to edit a template, see Editing Templates. When you copy a template, AFM does not copy over any associations to the switches. For information about how to associate templates, see Associating Templates.

1. Navigate to the **Network** > *Fabric* > **Configure and Deploy** screen.
2. From the **CLI Configuration** pull-down, select the **Manage Templates** option.

   The **Templates** screen displays.
3. Click on the **Copy Template** link.

   The **Copy Template** displays.
4. Select the template to copy.
5. In the **Template Name** field, enter a unique name for the new template.
6. Click the **OK** button.

Associating Templates

You can associate one or more existing configuration templates to the entire fabric, all spines, all leaves, or a set of switches. When a template is associated to an entire fabric or all spines or all leaves, the template is automatically applied to the newly added switches (instead of having to create new associations manually). You can also edit and delete templates.

Important: Each template can have only one association per fabric. AFM does not support ordering of templates for sequencing the commands. If you want to do this, Dell Networking recommends manually combining the templates into a single template.

This section contains the following topics:

- Associating Templates
- Editing Template Associations
- Deleting Template Associations

Associating Templates

To associate templates:

1. Navigate to the **Network** > *Fabric* > **Configure and Deploy** screen.
2. From the **CLI Configuration** pull-down menu, select the **Associate Templates** option.
3. Click the **Add Association** link.
4. In the **Template Name** pull-down menu, select the template to use.
5. (Optionally) In the **Comments** field, enter your comments about this association.

6. In the **Select Association** area, select one the following options:
   - **Fabric** — Associates the template to all the switches in the fabric.
   - **Spines** — Associates the template to all the spine switches.
   - **Leafs** — Associates the template to all the leaf switches.
   - **Custom** — Associates the template with specific switches. In the **Available Switches**, select the switches to associate to the template.
7. Click the **Apply** button.

Editing Template Associations

To edit a template association:

1. Navigate to the **Network** > *Fabric* > **Configure and Deploy** screen.
2. From the **CLI Configuration** pull-down menu, select the **Associate Templates** option.
3. Select the template to edit the association.
4. Click the **Edit Association** link.
5. Edit the association.
6. Click the **OK** button.

Deleting Template Associations

To delete a template association:

1. Navigate to the **Network** > *Fabric* > **Configure and Deploy** screen.
2. From the **CLI Configuration** pull-down menu, select the **Associate Templates** option.
3. Select the template to delete the association.
4. Click the **Delete** link.
5. Click the **OK** button.

Adding a Switch-Specific Custom Configuration

Before editing the existing configuration, backup the existing running configuration in the flash with a unique name consisting of the date and time.

To create and apply a customized switch-specific configuration and deploy it:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **CLI Configuration** pull-down, select the **Custom Configuration** option.
3. In the left navigation pane, select the switch to apply the switch specific-custom configuration to.

   The Switch Specific Custom Configuration screen displays.

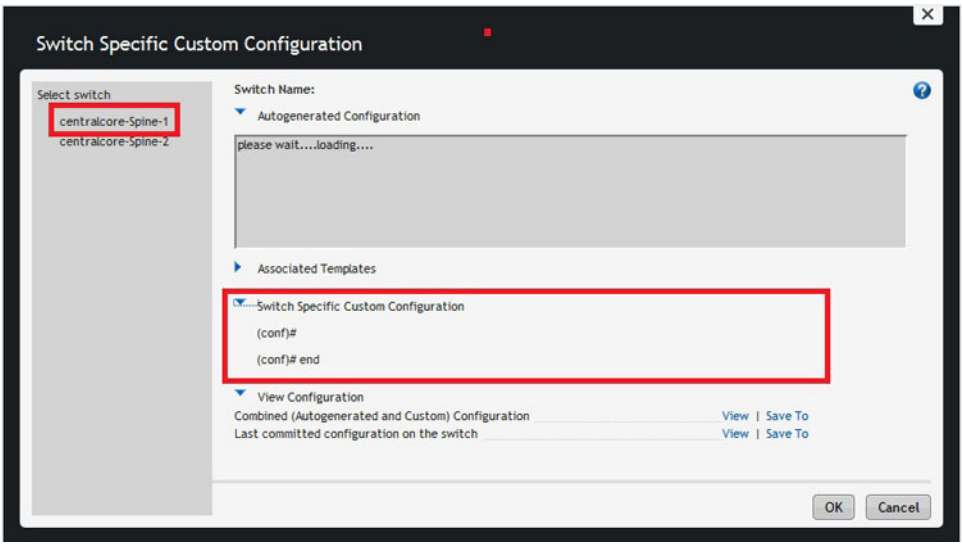


Figure 27. Switch Specific Custom Configuration

The **Switch Specific Custom Configuration** screen provides support to view the auto-generated configuration and switch-specific custom configuration that is applied to the individual switches in the fabric. Only the switches that are deployed are listed.

4. Enter the switch specific-custom configuration (FTOS CLI commands) in the **Switch Specific Custom Configuration** area.
5. Under the **View Configuration** heading, click the **View** button next to the **Preview the combined auto-generated and custom configuration**. This option allows you to view the auto-generated configuration, global custom configuration, and switch specific configuration.

   The **View Combined Configuration** screen displays.
6. To view the last applied configuration or save it, click the **View** button or **Save To…** button next to the **Last committed configuration on the switch** area. The AFM displays the timestamp for the last committed configuration on the switch.
7. Review the combined configuration and make any necessary changes.
8. Click the **Save To ...** button to save the combined auto-generated and custom configuration.
9. Click the **Close** button.

Viewing Custom Configuration History

To view a complete history of all custom configuration applied to each of the switches, use the **Custom Configuration History** screen.

- **Custom Configuration History** – Displays a list of custom configuration applied to the switch at different times; selecting a row in the table displays the corresponding details.
- **Applied Custom Configuration Commands** – Captures all template-based custom configuration commands and switch-specific custom configuration commands that were applied during deployment or redeployment. This includes errors reported by the switch during command execution.

To view custom configuration history:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **CLI Configuration** pull-down menu, select the **View Custom Configuration History** option.
   The **Custom Configuration History** displays.

8

Viewing the Fabric

This section contains the following topics:

- Dashboard
- View Network Summary
- View Fabric Summary
- Switch Summary

Related Links: Fabric Performance Management.

Dashboard

To view the fabric and system health, use **Home > Dashboard** screen as shown.

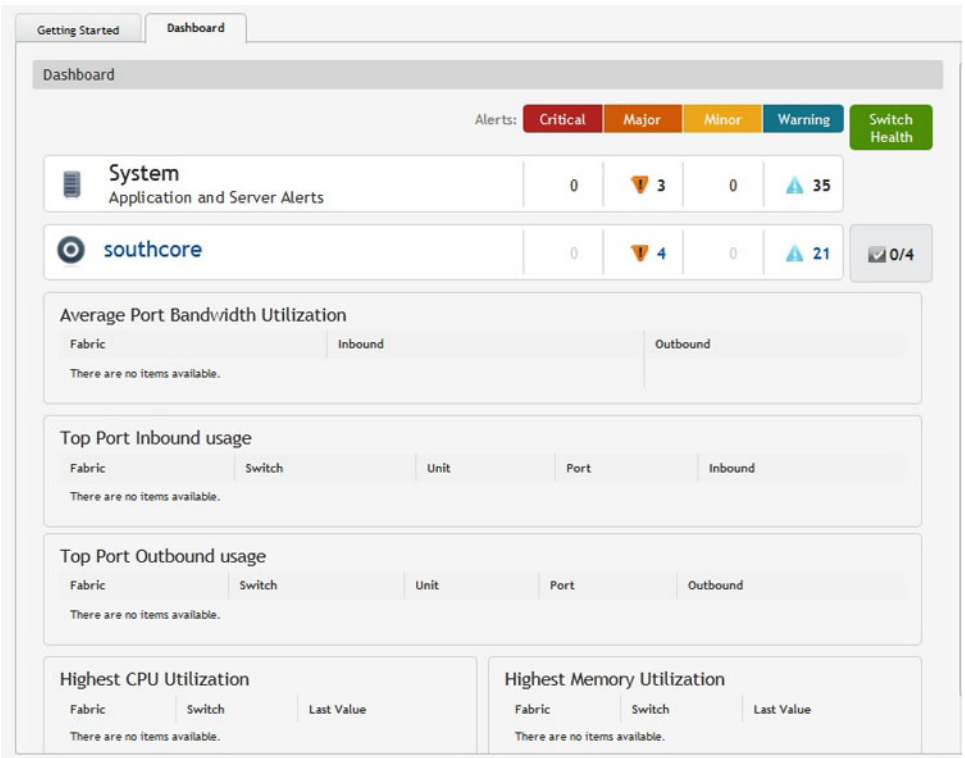


Figure 28. Dashboard

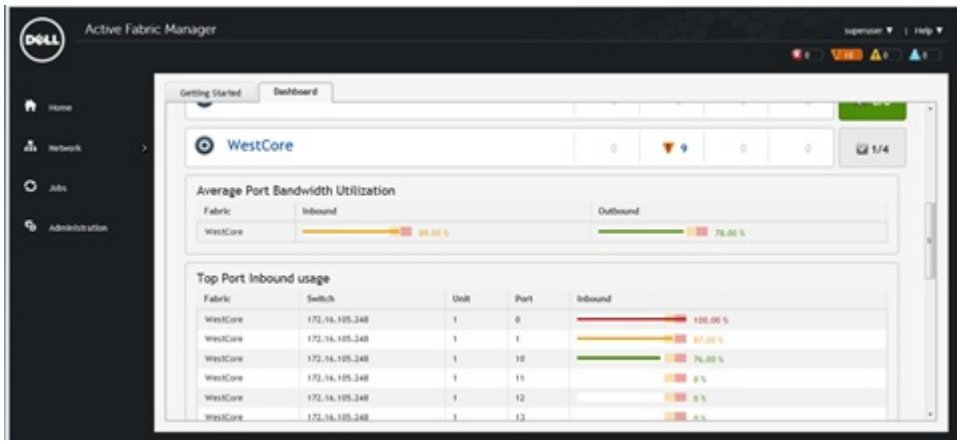


Figure 29. Dashboard with Color Codes

The Dashboard provides the following key performance information:

- **System** — Provides a tabular listing of system health and fabrics being managed by the AFM and lists the corresponding alert count by severity. The **Switch Health** column displays the number of switches that are alert free and the total switches that are part of the fabric.
- **Average Port Bandwidth Utilization** — Displays the average port bandwidth utilization for all fabrics managed by the AFM.
- **Top Port Usage** — Displays the top 10 ports usage for all fabrics with following columns:
  - Fabric
  - Switch
  - Port number
  - Inbound (%): number with color code bar
  - Outbound (%): number with color code bar

Table 18. Inbound and Outbound Link Utilization Color Codes

Color	Range	Description
Green (Good)	x < 80 %	Represents normal inbound or outbound link utilization.
Yellow (Minor)	x > = 80 % and x < 90 %	Represents low link utilization.
Red (Critical)	x > = 90 %	Represents high link utilization.

NOTE: When the color code is yellow or red, the AFM displays an alarm at the **Network** > *Fabric Name* > *Switch Name* > **Alerts and Events > Current** screen.

- **Highest CPU Utilization** — Displays the highest 5 CPU utilization in 5 minute intervals for all fabrics with the following information:
  - Fabric
  - Switch
  - Last Values (%): number with color code bar

Table 19. CPU Utilization Color Codes

Color	Range	Description
Green (Good)	x < 70 %	Represents normal CPU utilization.
Yellow (Minor)	x > = 70 % and x < 80%	Represents low CPU utilization.
Red (Critical)	x > = 80 %	Represents high CPU utilization.

NOTE: When the color code is yellow or red, the AFM displays an alarm at the **Network** > *Fabric Name* > *Switch Name* > **Alerts and Events > Current** screen.

- **Highest Memory Utilization** — Displays the highest 5 memory utilization for all fabric with following information:
  - Fabric
  - Switch
  - Last value (%): number with color code

Table 20. Memory Utilization Color Codes

Color	Range	Description
Green (Good)	x < 82 %	Represents normal memory utilization.
Yellow (Minor)	> = 82 % and < 92%	Represents low memory utilization.
Red (Critical)	> = 92 %	Represents high memory utilization.

NOTE: When the color code is yellow or red, the AFM displays an alarm at the **Network** > *Fabric Name* > *Switch Name* > **Alerts and Events** > **Current** screen.

Related links:

- Alerts
- Monitor

Network Topology

To display all the fabrics in the network topology in graphical or tabular view, use the **Network > Summary** screen. The network topology view contains a collection of fabric icons with status color coded and fabric names. There are no links between fabrics.

Network Topology Tabular View

Navigate to the **Network > Summary** screen and then click the **Tabular** tab.

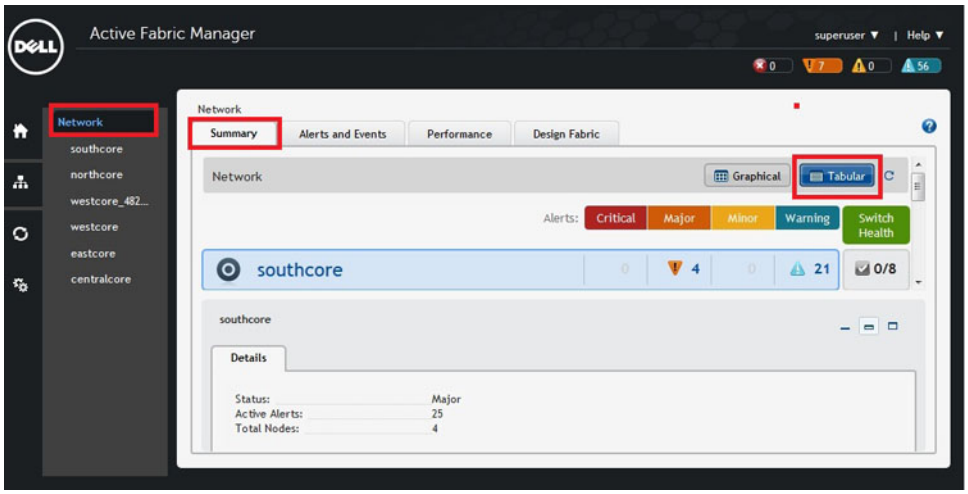
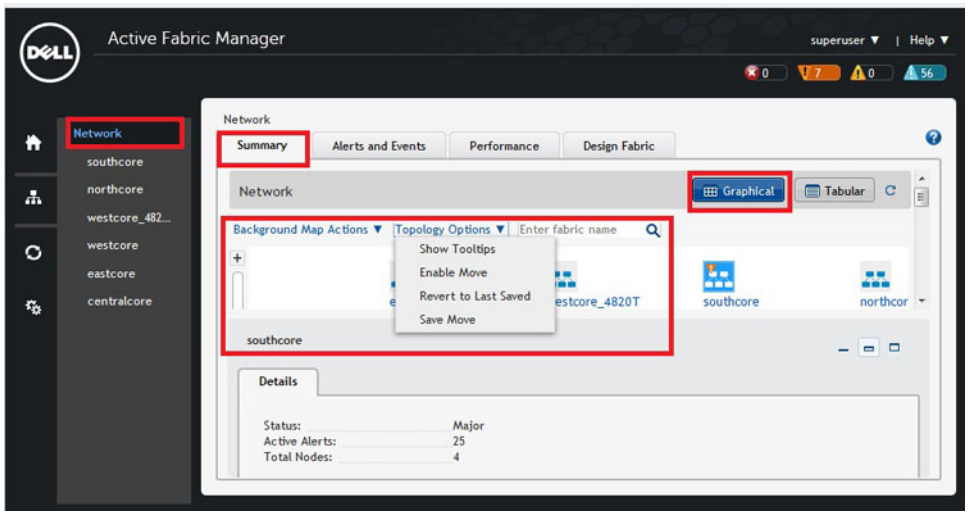


Figure 30. Network Summary Tabular View

Network Topology Graphical View

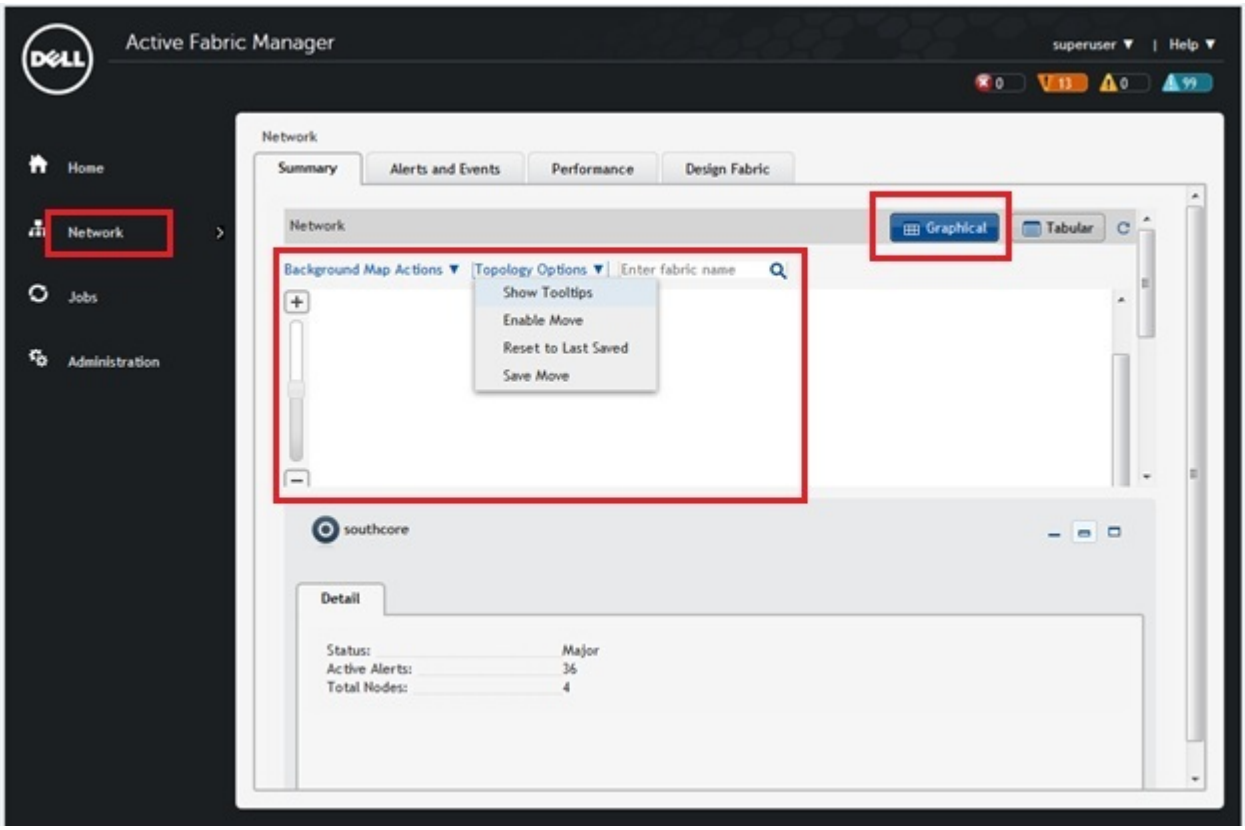


The network topology contains fabric icons. Each fabric icon has the following functions:

- **Status:** Displays the status of the fabric using the following colors:
  - Red: Critical alerts
  - Orange: Major alerts
  - Yellow: Minor alerts
  - Blue: Warning alerts
  - Green: Information alerts or no alerts
  - Gray: For unmanaged or un-deployed fabric
- **Selection:** Clicking a fabric icon highlights the icon and displays the fabric data in the **Detail** tab.
- **Show Tooltips:** Displays tooltip information about a fabric (fabric name, status, active alerts, and the total number of switches in the fabric) when you place your mouse over a fabric icon.

- **Enable Move:** After enabling this option, you can move each fabric icon to a new location in the map.
- **Revert to Last Saved:** Revert to fabric locations to last saved version.
- **Save Move:** Save the location of the fabrics that were moved.
- **Popup menu:** Right-click a fabric to display a menu that contains actions that can be applied to the fabric. The menu contains the fabric name and "Open" menu item, which opens the fabric view.
- **Enter fabric name**: To locate a fabric, enter the name and then click the search icon.
- **Background Map Actions**: Load or delete a geographical background map for the network.
- **Enter fabric name**: Enter the fabric name and then click the search icon to locate a fabric in the network.

Navigate to the **Network > Summary** screen and then click the **Graphica**l tab.



Fabric Summary

To display the status of the fabric in a graphical view (**Graphical** button), which is the default view, and the tabular view (**Tabular** button) for all the switches in the fabric, use the **Network** > *Fabric Name* > **Summary** screen

Displaying the Fabric in a Tabular View

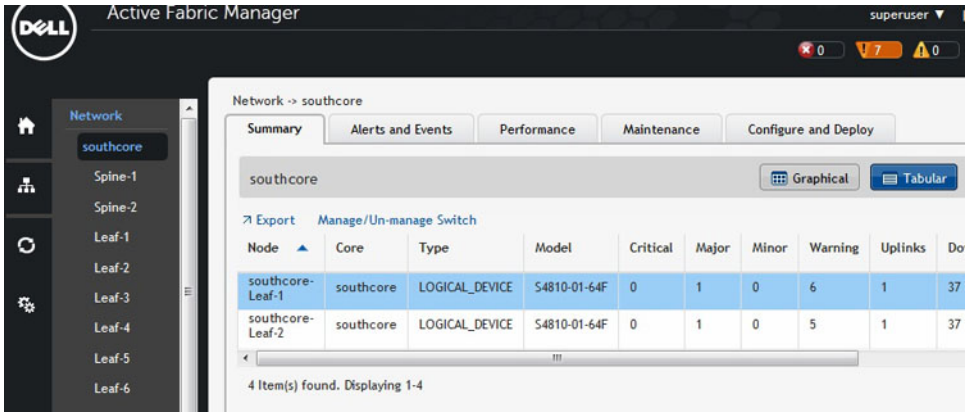


Figure 31. Fabric Tabular View

With the fabric tabular view, you view the switches in the fabric and check the alarms. Export your results using the **Export** link. You can also manage or unmanage a switch using the **Manage/Unmanage Switch** link. For additional information about the fabric, select the following tabs:

- **Detail**
- **Links**
- **Hardware**
- **VLT Domain**

Displaying the Fabric in Graphical View

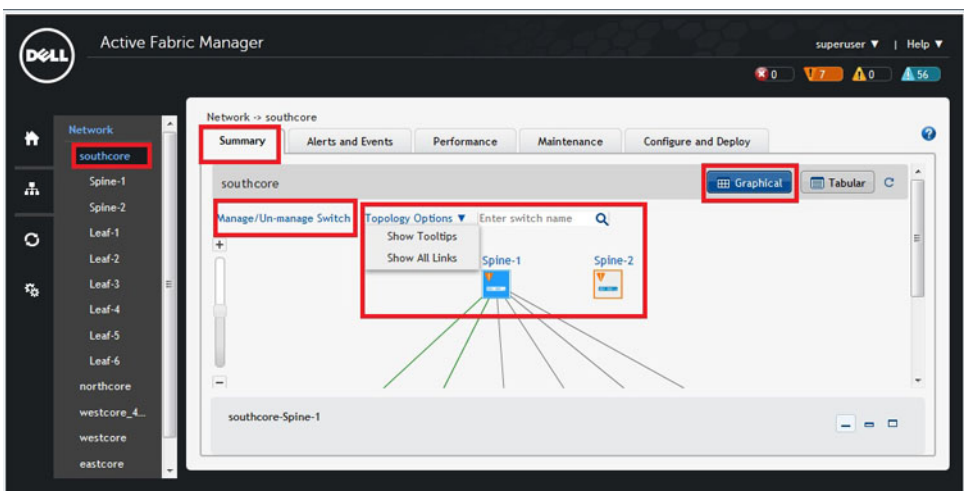


Figure 32. Fabric Graphical View (Topology View)

A fabric graphical view provides the topology view of the fabric. The fabric type and name display at the top of the fabric view. View the leafs associated with a spine by clicking on the spine. The following options are also available:

- **Manage/Unmanage** — Unmanaged switches appear in the fabric but are not actively managed. A switch must be in a managed state to monitor and manage it.
- **Show Tooltips** — Displays information (fabric, switch name, model name, IP address, alarm status, and manage state) about a switch when you place the cursor over the switch.
- **Show All Links** — Displays all the links between the spines and the leaves.
- **Enter switch name** — Enter the switch name and click the search icon to locate a switch in the fabric. The switch name is case sensitive.

For additional information about the fabric, select the following tabs:

- **Detail**
- **Links**
- **Hardware**
- **VLT Domain**

Switch Summary

To view the following switch summary information, navigate to the **Network** > *Fabric Name* > *Switch Name* screen and then click the **Summary** tab. Make sure that the Graphical button is selected in the upper right of the screen. Click on a port to display information about the state of the port. Click on the **Port Legends** arrow to display the port legends.

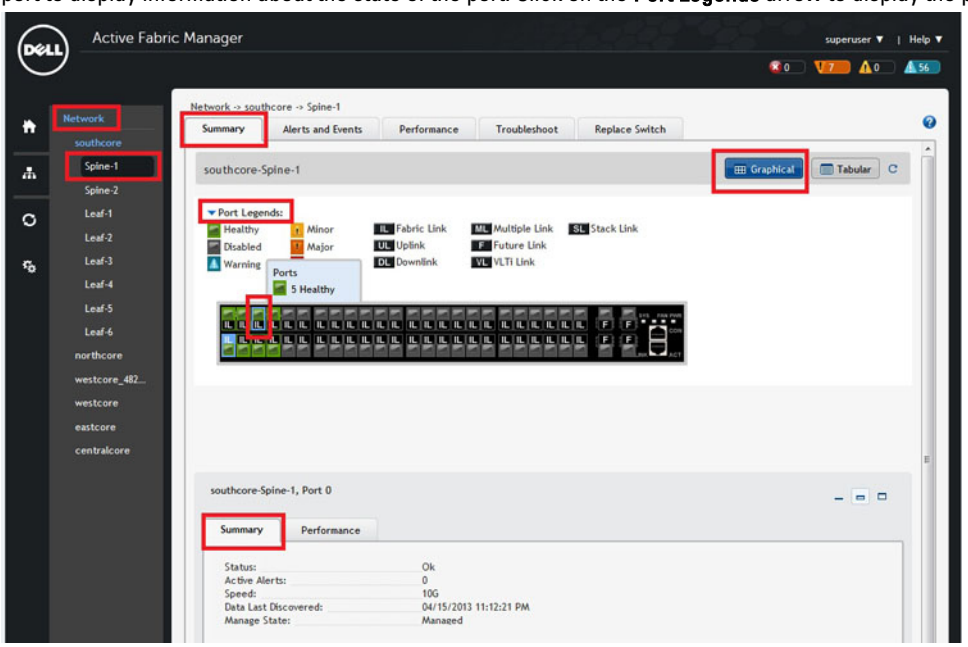


Figure 33. Switch Summary Screen — Graphical View

- Status
- Active Alerts
- Speed
- Manage State

9

Troubleshooting

This section contains the following topics:

- Ping, Traceroute, SSH, and Telnet
- Validation Alarms
- Deployment and Validation Errors
- TFTP/FTP Error
- Switch Deployment Status
- Validating Connectivity to the ToR

For more information about troubleshooting, see Ping, Traceroute, SSH, and Telnet.

Ping, Traceroute, SSH, and Telnet

To troubleshoot a switch in the fabric, use ping, traceroute, SSH, and Telnet:

- Ping
- Traceroute
- SSH
- Telnet

NOTE: SSH or Telnet will work depending upon what you have configured in the switch protocols.

Ping

To ping a switch in a fabric:

1. Navigate to the **Network** > *Fabric Name* > *Switch Name* > **Troubleshoot** screen.
2. Click the **Ping** button to display the ping results.

Traceroute

To traceroute a switch in the fabric:

1. Navigate to the **Network** > *Fabric Name* > *Switch Name* > **Troubleshoot** screen. .
2. Click the **Traceroute** button to display the traceroute results.

SSH

To issue an SSH command on a switch:

1. Navigate to the **Network** > *Fabric Name* > *Switch Name* > **Troubleshoot** screen. .
2. Click the **SSH** tab.
3. In the **SSH Command** field, enter the SSH command.
4. Click the **Send Command** button to display the SSH results.

Telnet

To issue a Telnet command on a switch:

1. Navigate to the **Network** > *Fabric Name* > *Switch Name* > **Troubleshoot** screen.
2. Click the **Telnet** tab.
3. In the **Telnet Command** field, enter the Telnet command.
4. Click the **Send Command** button to display the Telnet results.

Validation Alarms

To troubleshoot alarms that are generated by theAFM, use the following section.

Table 21. Validation Alarms

Alarm	Recommended Action
Validation failed because the switch cannot be discovered.	If you have undiscovered switch errors, log on to the switch console to isolate the fault. **NOTE:** Make sure that the switch has been power cycled on and check the physical connection.
Validation failed because the switch has a mismatch MAC address.	1. Verify that you have correctly mapped the system MAC address to the associated switches: a. Navigate to the **Network**> *Fabric Name* > **Configure and Deploy** screen. b. From the **Deploy Fabric** pull-down menu, select the Pre-deployment Configuration option. c. Navigate to the **Assign Switch Identities** screen and check the system MAC address mapping for the associated switches. 2. Verify your change by validating the switch. a. Navigate to the **Network**> *Fabric Name* > **Configure and Deploy** screen. b. From the **Deploy Fabric** pull-down menu, select the **Deploy and Validate** option. c. Click on the **Validation** tab and the check the switch to validate. d. Click the **Validate Selected** link.
Validation failed because the switch has a name mismatch.	1. Verify that you have correctly mapped the system MAC address to the associated switches:

	a. Navigate to the **Network**> *Fabric Name* > **Configure and Deploy** screen. b. From the **Deploy Fabric** pull-down menu, select the Pre-deployment Configuration option. c. Navigate to the **Assign Switch Identities** screen and check the system MAC address mapping for the associated switches. 2. Verify your change by validating the switch. a. Navigate to the **Network**> *Fabric Name* > **Configure and Deploy** screen. b. From the **Deploy Fabric** pull-down menu, select the **Deploy and Validate** option. c. Click on the **Validation** tab and the check the switch to validate. d. Click the **Validate Selected** link.
Validation failed because the switch has a model mismatch.	1. Verify that you have correctly mapped the system MAC address to the associated switches: a. Navigate to the **Network**> *Fabric Name* > **Configure and Deploy** screen. b. From the **Deploy Fabric** pull-down menu, select the Pre-deployment Configuration option c. Navigate to the **Assign Switch Identities** screen and check the system MAC address mapping for the associated switches. 2. Verify your change by validating the switch: a. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen. b. From the **Deploy Fabric** pull-down menu, select the **Deploy and Validate** option. c. Click on the **Validation** tab and the check the switch to validate. d. Click the **Validate Selected** link.
Validation failed because the switch is in a disconnected state.	The switch is not reachable. Verify the reachability of the switch.
Validation failed because Te 0/1 has a wiring mismatch.	1. Reviewing the wiring plan. 2. Wire according to the wiring plan to fix the wiring mismatch. 3. Make sure that the ports on the switches have accurately mapped.
Validation failed because Te 0/1 has a missing link.	No connectivity is detected to the switch. Check the cables.
Validation failed because only a partial link can be verified for Te 0/1.	Check the connectivity of the link and the connectivity of the switch.

Validation failed because the switch has a configuration mismatch.	1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen. 2. Click the **Errors** link. 3. Select the **Configuration Mismatch** tab. 4. Review the configuration mismatch and correct the configuration errors.

Deployment and Validation Errors

This section contains the following topics:

- Pre-deployment Errors
- Deployment Errors
- Validation Errors

Pre-deployment Errors

Error Details	Recommended Action
Failed to transfer minimum configuration file via TFTP/FTP.	Verify the TFTP or FTP connectivity from the AFM. For FTP, verify the credentials and restart the **DHCP Integration** step using the **Pre-deployment Configuration** wizard. **To restart the DHCP Integration**: 1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen. 2. From the **Deploy Fabric** pull-down menu, select the **Pre-deployment Configuration** option. 3. Restart the **DHCP Integration** step.
Overwrite DHCP contents to local DHCP server failed.	Verify the permission of the directory and disk space availability on the AFM server; verify the local DHCP server configuration and then restart the **DHCP Integration** step using **Pre-deployment Configuration** wizard. **To restart the DHCP Integration**: 1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen. 2. From the **Deploy Fabric** pull-down menu, select the Pre-deployment Configuration option. 3. Restart the **DHCP Integration** step.

Deployment Errors

Error Details	Recommended Action
Protocol transfer failed	1. Verify the TFTP or FTP connectivity from the AFM. For FTP, verify the credentials.

	2. Restart the deployment of the switch from the **Network** > *Fabric Name* > **Configure and Deploy** by selecting the switch from the list and then click on the **Deploy Selected** link.
Device cleanup task failed	1. Verify the Telnet or SSH connectivity from the AFM. 2. Restart the deployment of the switch from the **Network** > *Fabric Name* > **Configure and Deploy** by selecting the switch from the list and then click on the **Deploy Selected** link.
Complete configuration upload failed	1. Verify TFTP/FTP or Telnet/SSH connectivity from the AFM. 2. Restart the deployment of the switch from the **Network** > Fabric Name > Configure and Deploy by selecting the switch from the list and then click on the Deploy Selected link
Smart script transfer failed	1. Verify connectivity to the switch from the AFM. 2. Restart the deployment of the switch from the **Network** > *Fabric Name* > **Configure and Deploy** by selecting the switch from the list and then click on the **Deploy Selected** link.
Custom configuration upload failed	1. Verify the switch login credentials and commands. 2. Restart the deployment of the switch from the **Network** > *Fabric Name* > **Configure and Deploy** by selecting the switch from the list and then click on the **Deploy Selected** link.
Backup config failed	1. Verify the Telnet SSH connectivity. 2. Restart the deployment of the switch from the **Network** > *Fabric Name* > **Configure and Deploy** by selecting the switch from the list and then click on the **Deploy Selected** link.

Validation Errors

Use the following tables to troubleshoot the following validation errors when you deploy a fabric.

To view validation errors, navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen and then click on the **Errors** link to view the following type of errors:

- Configuration
- Custom Configuration
- Custom Configuration Deployment
- Discovered Switch Errors
- Pre-deployment
- Undiscovered Switch Errors
- Wiring

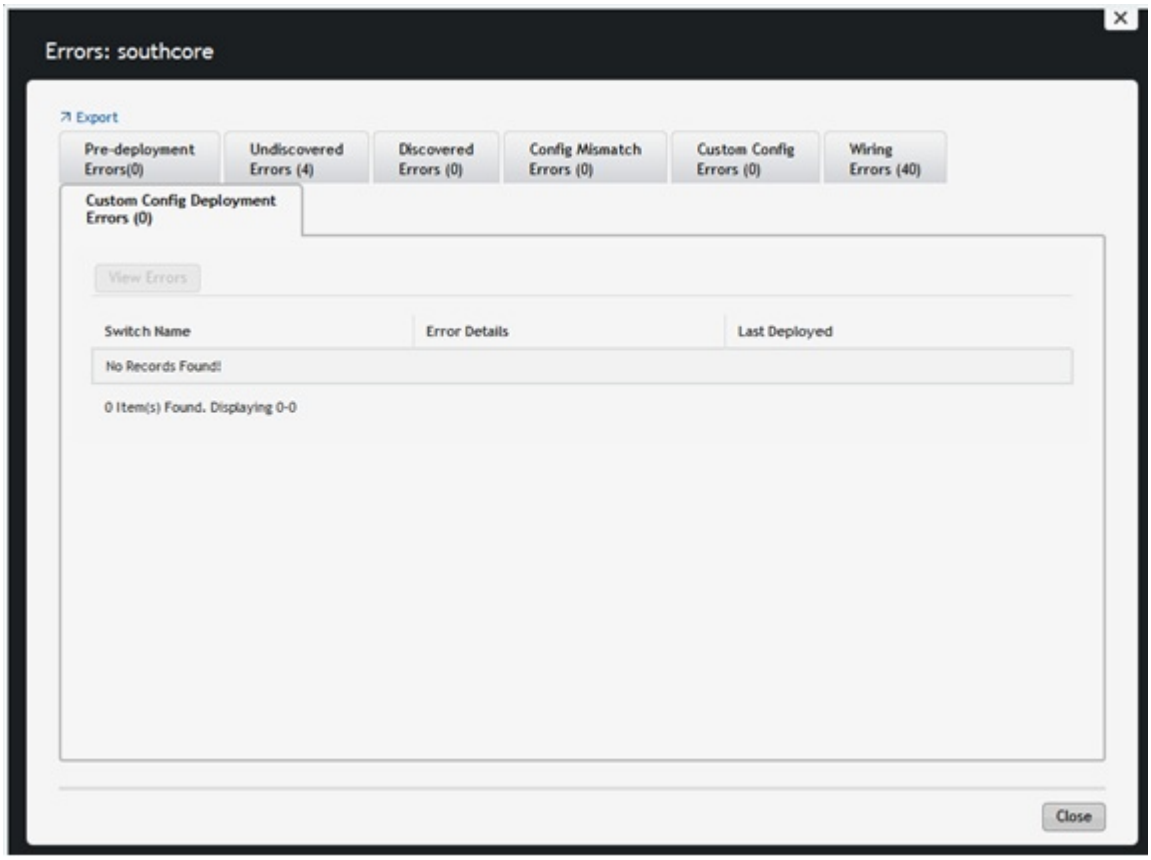


Table 22. Configuration Errors

Configuration Error	Recommended Action
Configuration Mismatch	1. On the **Deployment and Validation Status** screen, select the switch that you want to view. 2. Click the **View Mismatch** button. 3. Review the configuration mismatch and correct the configuration errors. 4. Restart validation of the switch from the **Deploy and Validate** screen by selecting the switch from the list and clicking the **Start Validation** button.

Table 23. Wiring Errors

Wiring Error	Recommended Action
Wiring Mismatch	1. Review the wiring plan. 2. Wire the switch according to the wiring plan to fix the wiring mismatch. 3. Validate the switch from the screen by selecting the switch from the list and clicking on the **Start Validation** button.
Missing Link	1. Review the wiring plan. 2. Wire the switch according to the wiring plan to fix the missing link. 3. Validate the switch.

	a. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy**. b. From the **Deploy Fabric** pull-down menu, select the **Deploy and Validate** option. c. Click the **Validation** tab and then select the switches to validate. d. Click the **Deploy Selected** link.
Partial Link	1. Verify that the switch is wired according to the wiring plan. 2. Verify the connectivity on the AFM from both of switches of the link. 3. Validate the switch. a. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy**. b. From the **Deploy Fabric** pull-down menu, select the **Deploy and Validate** option. c. Click the **Validation** tab and then select the switches to validate. d. Click the **Deploy Selected** link.

Table 24. Undiscovered Switch Error

Undiscovered Switch Error	Recommended Action:
	1. Verify that the switch has a valid IP address. 2. If required, correct the pre-deployment configuration. 3. From the AFM server, verify that the connectivity to the switch exists. 4. Verify that the switch is running the minimum required software. 5. Validate the switch. a. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy**. b. From the **Deploy Fabric** pull-down menu, select the **Deploy and Validate** option. c. Click the **Validation** tab and then select the switches to validate. d. Click the **Deploy Selected** link.

Table 25. Discovered Switch Error

Discovered Switch Error	Recommended Action
Disconnected	1. Verify that the connectivity to the switch exists from the AFM server. 2. Verify that the switch is running the minimum required software. 3. Validate the switch. a. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen. b. From the **Deploy Fabric** pull-down menu, select the **Deploy and Validate** option. c. Click the **Validation** tab and then select the switches to validate. d. Click the **Deploy Selected** link.
Switch Name Mismatch	1. Verify that the IP address to switch name mapping is correct in the pre-deployment configuration.

	2. If the pre-deployment configuration is updated, you might need to redeploy the switch. 3. Validate the switch. a. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen. b. From the **Deploy Fabric** pull-down menu, select the **Deploy and Validate** option. c. Click the **Validation** tab and then select the switches to validate. d. Click the **Deploy Selected** link.
Switch Model Mismatch	1. Verify that the IP address to switch name mapping is correct in the pre-deployment configuration. 2. If the pre-deployment configuration is updated, you might need to redeploy the switch. 3. Validate the switch. a. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy**. b. From the **Deploy Fabric** pull-down menu, select the **Deploy and Validate** option. c. Click the **Validation** tab and then select the switches to validate. d. Click the **Deploy Selected** link.
System MAC Address Mismatch	1. Verify that the IP address to switch name mapping is correct in the pre-deployment configuration. 2. If the pre-deployment configuration is updated, you might need to redeploy the switch. 3. Validate the switch. a. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen. b. From the **Deploy Fabric** pull-down menu, select the **Deploy and Validate** option. c. Click the **Validation** tab and then select the switches to validate. d. Click the **Deploy Selected** link.

Switch Deployment Status Errors

Use the following table to troubleshoot switch deployment status errors.

Table 26. Switch Deployment Status Errors

Switch Deployment Status	Description	Requires Action	Recommended Actions
NOT STARTED	Not Started	No	Start the deployment of the switch from the **Network >** *Fabric Name* > **Configure and Deploy** screen by selecting the switch from the list and then click on the **Deploy Selected** link. **NOTE:** The switch is in BMP mode.

CONFIG GENERATION IN PROGRESS	Configuration File Generation In-progress	No	Information only.
CONFIG GENERATION FAILED	Configuration File Generation Failed	Yes	1. Check the write permission for the AFM installation directory in the AFM server machine. 2. Verify that the disk space is not full in the AFM server. 3. Restart the deployment of the switch from the **Network** > *Fabric Name* > **Configure and Deploy**screen by selecting the switch from the list and then click on the **Deploy Selected** link. **NOTE:** The switch is in BMP mode.
CONFIG GENERATION SUCCESS	Configuration File Generation Completed Successfully	No	Information only.
CONFIG FILE TRANSFER IN PROGRESS	Configuration File Transfer In-progress	No	Information only.
CONFIG FILE TRANSFER FAILED	Configuration File Transfer Failed	Yes	1. Verify the connectivity to the TFTP server from the AFM server. 2. Restart the deployment of the switch from the **Network** > *Fabric Name* > **Configure and Deploy** by selecting the switch from the list and then click on the **Deploy Selected** link. **NOTE:** The switch is in BMP mode.
CONFIG FILE TRANSFER SUCCESS	Configuration File Transferred Successfully	No	Information only.
REQUEST TO DISCOVER NODE	Request To Discover Switch	Yes	1. Power on the switch. 2. Restart the deployment of the switch from the **Network** > *Fabric Name* > **Configure and Deploy** screen by selecting the switch from the list and then click on the **Deploy Selected** link. **NOTE:** The switch is in BMP mode.
MIN CONFIG UPLOAD INPROGRESS	Minimum Configuration Upload In-Progress	No	Information only.
MIN CONFIG UPLOAD ERROR	Minimum Configuration Upload Error	Yes	1. Verify the connectivity to the TFTP/FTP server from the switch. 2. Check the **Validation Status** column for errors and fix them.

			3. Verify that the system MAC address in the **dhcpd.conf** file matches the **csv.** file that contains the MAC addresses of the switches. 4. Verify that the **min.cfg** file is in the correct directory on the TFTP/FTP server. 5. Redeploy the switch from the **Network >** *Fabric Name* > **Configure and Deploy** screen by selecting the switch from the list and then click on the **Deploy Selected** link. **NOTE:** The switch is in BMP mode.
MIN CONFIG UPLOAD COMPLETED	Minimum Configuration Upload Successful	No	Information only.
INIT SOFT RELOAD	Initiated Soft Re-load on Switch	No	Information only.
INIT SOFT RELOAD ERROR	Error During Soft Re-load on Switch	Yes	1. Check the switch syslogs for a reload command failure. 2. Make any necessary fixes. 3. Restart the deployment of the switch from the **Network >** *Fabric Name* > **Configure and Deploy** screen by selecting the switch from the list and then click on the **Deploy Selected** link. **NOTE:** The switch is in BMP mode.
PROTOCOL CONFIG UPLOAD INPROGRESS	Protocol Configuration Upload In-Progress	No	Information only.
PROTOCOL CONFIG UPLOAD ERROR	Protocol Configuration Upload Error	Yes	1. Verify the connectivity to the TFTP server from switch. 2. Check the **Validation Status** column for errors and fix them. 3. Verify that the DHCP server is running. 4. Verify that the CFG file correctly has been placed on the TFTP/FTP server and that you can ping it from the switch. 5. Redeploy the switch. **NOTE:** The switch is not in BMP mode.

			a. Navigate to the **Network >** *Fabric Name* > **Configure and Deploy** screen. b. From the **Deploy Fabric** pull-down menu, select the **Deploy and Validate** option. c. On the **Deploy** tab, check the switch to deploy and then click the **Deploy Selected** link.
PROTOCOL CONFIG UPLOAD COMPLETED	Protocol Configuration Upload Succesful	No	Information only.
DEVICE DEPLOYMENT SUCCESS	Switch Deployment Successful	No	Information only.
UPLINK CONFIG GENERATED	Uplink Configuration Generated	No	Information only.
UPLINK CONFIG UPLOAD IN PROGRESS	Uplink Configuration Upload In-Progress	No	Information only.
UPLINK CONFIG UPLOAD ERROR	Uplink Configuration Upload Error	Yes	1. Verify the connectivity between the AFM server and switch. 2. Check the **Validation Status** column for errors and fix them 3. Restart the deployment . **NOTE:** The switch is not in BMP mode. a. Navigate to the **Network >** *Fabric Name* > **Configure and Deploy** screen. b. From the Deploy Fabric pull-down menu, select the Deploy and Validate option. c. On the **Deploy** tab, check the switch to deploy and then click the **Deploy Selected** link.
UPLINK RECONFIGURED REDEPLOY REQUIRED	Uplink re-configured, Re-deployment of Switch is required	Yes	Restart the deployment of the switch. **NOTE:** The switch is not in BMP mode. 1. Navigate to the **Network >** *Fabric Name* > **Configure and Deploy** screen. 2. From the Deploy Fabric pull-down menu, select the Deploy and Validate option. 3. On the **Deploy** tab, check the switch to deploy and then click the **Deploy Selected** link.

REDEPLOYMENT REQUIRED	Re-deployment of the switch is required	Yes	Restart the deployment of the switch. **NOTE:** The switch is not in BMP mode. 1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen. 2. From the Deploy Fabric pull-down menu, select the Deploy and Validate option. 3. On the **Deploy** tab, check the switch to deploy and then click the **Deploy Selected** link.

TFTP/FTP Error

To troubleshoot TFTP/FTP when the deployment status is “TFTP /FTP Failed”, use the following table.

Table 27. Deployment Status Configuration Errors

Deployment Status	Error Category	Error Details	Recommended Action
TFTP/FTP Failed	Configuration Deployment Error	Error occurred during TFTP/FTP	1. Check the TFTP/FTP connectivity on the network. 2. Make sure that you have specified the correct TFTP/FTP address at the **Administration** > **Settings** screen.

Validating Connectivity to the ToR

To validate the leaves downlink connections to the ToR:

1. Ping the ToRs from the leaves.
2. Confirm the VLAN configured on the leaf is same on the port.

10

Alerts and Events

This section contains the following topics:

Current — Active Alerts

To view active alerts at the network, fabric and switch levels, use the **Current** tab. To acknowledge an active alert, select the active alert and then click the **Acknowledge** button. To display more information about the active alert, select the active alert. The system displays more information about the alert at the bottom of the screen. To unacknowledge an active alert, select the active alert and then click the **Unacknowledge** button. You can also clear active alerts.

- To filter active alerts at the network level, navigate to the **Network** > **Alerts and Events** screen.
- To filter active alerts at the fabric level, navigate to the **Network** > *Fabric Name* > **Alerts and Events** screen.
- To filter active alerts at the switch level, navigate to the **Network** > *Fabric Name* > *Switch Name* > **Alerts and Events** screen.

1. Click the **Current** button.
2. Click the filtering icon on the right of the screen. You can use the filter options, **from date** and **to date**.

   The filtering options display.
3. In the **Severity** pull-down menu, select one of the following filtering criteria:
   a) **All**
   b) **Critical**
   c) **Major**
   d) **Minor**
   e) **Cleared**
   f) **Warning**
   g) **Unknown**
   h) **Info**
   i) **Indeterminate**
4. In the **Source IP** field, enter the source IP address.
5. In the **Source Name** field, enter the source name.
6. In the **Description** field, enter a description.
7. In the **Ack** (acknowledgement) pull-down menu, select one of the following:
   a) **All**
   b) **Yes**
   c) **No**
8. Click the **Apply** button.

Historical — Alerts and Event History

To view historical events at the network, fabric or switch level, use **Alerts and Events** screen .

- To filter active alerts at the network level, navigate to the **Network** > **Alerts and Events** screen.
- To filter active alerts at the network level, navigate to the **Network** > *Fabric Name* > **Alerts and Events** screen.
- To filter active alerts at the switch level, navigate to the **Network** > *Fabric Name* > *Switch Name* > **Alerts and Events** screen.

To filter historical events:

1. Click the **Historical** button.
2. Click the filtering icon. You can use the filter options, **from date** and **to date**.
   The filtering options display.
3. In the **Severity** pull-down menu, select one of the following filtering criteria:
   a) **All**
   b) **Critical**
   c) **Major**
   d) **Minor**
   e) **Warning**
   f) **Cleared**
   g) **Unknown**
   h) **Info**
   i) **Indeterminate**
4. In the **Source IP** field, enter the source IP address.
5. In the **Source Name** field, enter the source name.
6. In the **Description** field, enter the description.
7. In the **Ack** (acknowledgement) pull-down menu, select one of the following:
   a) **All**
   b) **Yes**
   c) **No**
8. Click the **Apply** button.
9. If you want to export your results, click the **Export** link.

11

Performance Management

You can monitor performance at the network, fabric, switch, and port level.

This section contains the following topics:

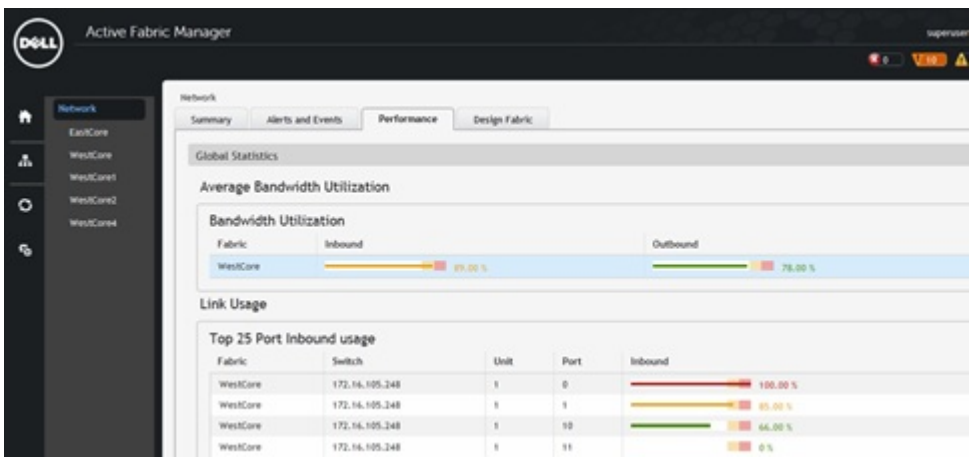
- Network Performance Management
- Fabric Performance Management
- Switch Performance Management
- Port Performance Management
- Detailed Port Performance
- TCA Threshold Setting
- Data Collection
- Reports

Network Performance Management

To monitor the following network historical data for all the fabrics, use the **Network** > **Performance** screen:

- Bandwidth utilization
- Top 25 port inbound usage
- Top 25 port outbound usage
- Highest CPU utilization
- Highest memory utilization

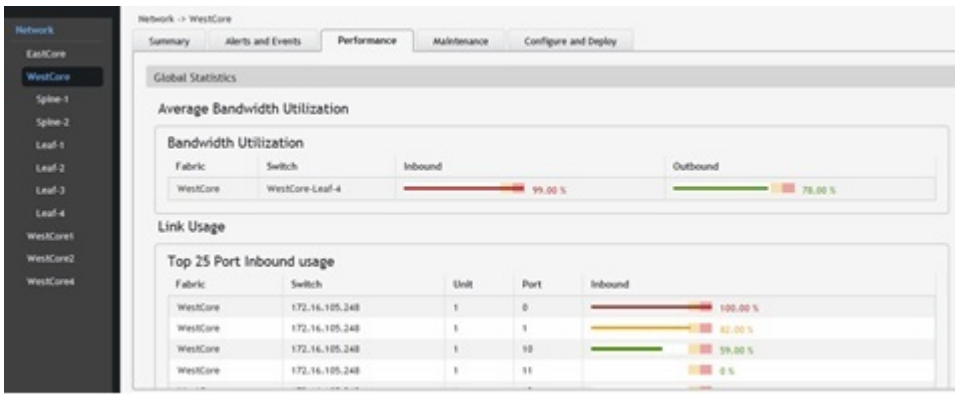
For information about the color codes for the historical data, see Dashboard.



Fabric Performance Management

To monitor the following for all the switches in the fabric, use the **Network** > *Fabric Name* > **Performance** screen:

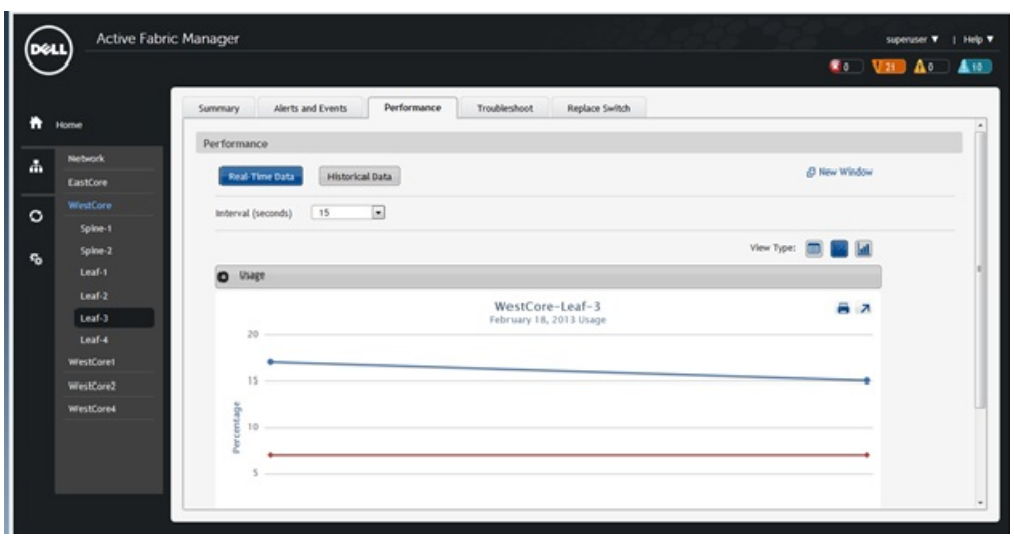
- Bandwidth utilization
- Top 25 port inbound usage
- Top 25 port outbound usage
- Top 10 highest CPU utilization
- Top 10 high memory utilization



Switch Performance Management

To view historical and real-time data switch level performance, use the **Network** > *Fabric Name* > *Switch Name* > **Performance** screen . By default, the historical view is shown in tabular format. You can also monitor performance in graphical (chart or bar) format in the **View Type** area or move to the real-time data monitoring from this screen.

NOTE: To view performance, enable data collection at the **Jobs > Data Collections** screen.



Port Performance Management

To view a summary of historical and real-time data port performance:

1. Navigate to the **Network** > *Fabric Name* > *Switch Name* > **Summary** screen.

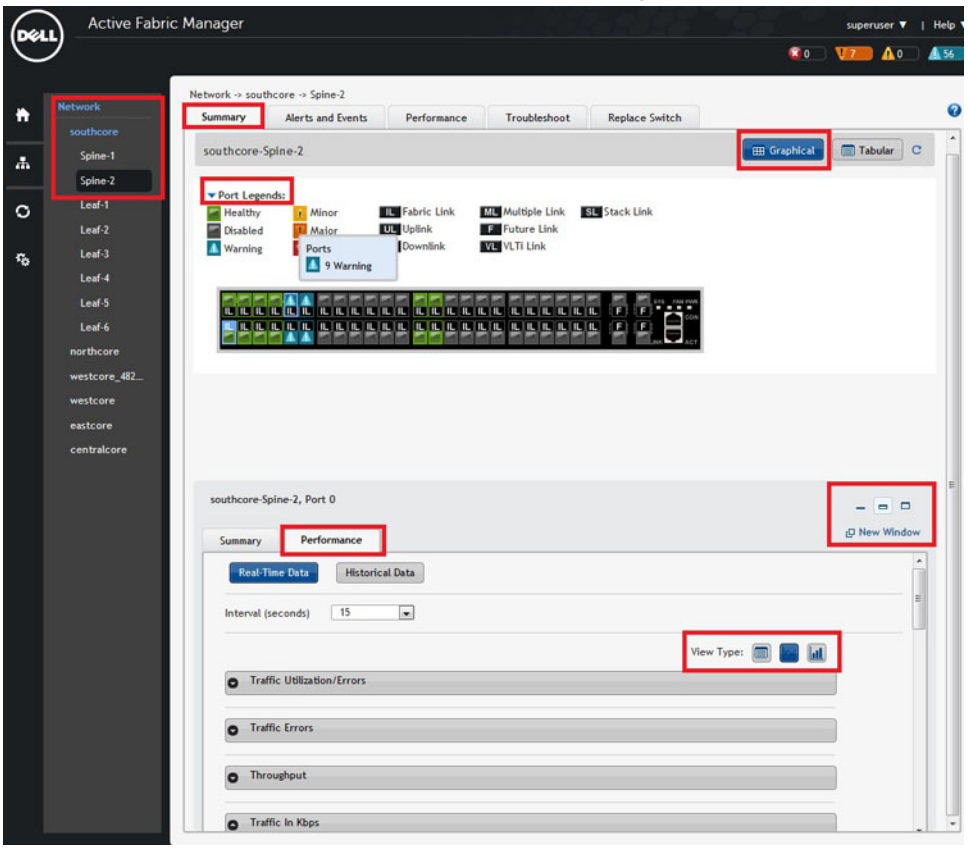


Figure 34. Displaying Summary of Port Performance

2. Select a port and then click on the **Performance** tab to view port performance.
3. Click the **Real-Time Data** or **Historical** button.
4. Select one of the following **View Type** options to display port performance: **Bar**, **Graphical**, or **Tabular**.
5. Review the performance information.

Detailed Port Performance Management

You can view detailed port level performance screen in a graphical (chart) or tabular format:

- Traffic utilization
- Traffic errors
- Throughput
- Traffic in Kbps

- Packets

To display detailed historical and real-time data port level performance:

1. Navigate to the **Network** > *Fabric Name* > *Switch Name* > **Summary** screen.
2. Click the **Performance** tab at the bottom of the screen.

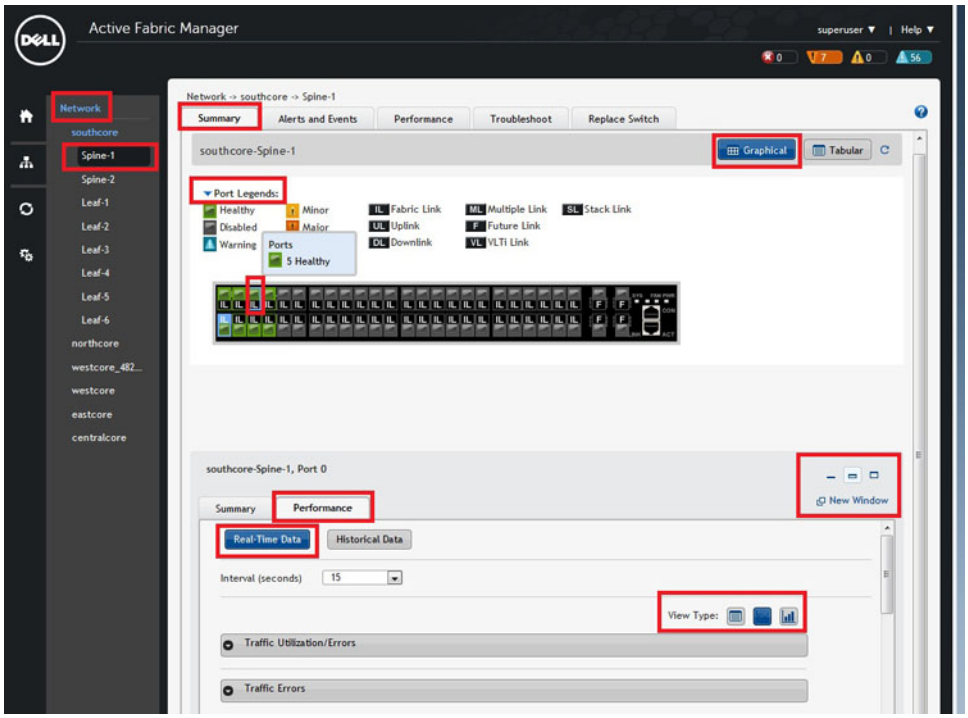


Figure 35. Display Detailed Port Performance

3. In the upper right of the screen, select the format to view the data using the **Graphical** or **Tabular** options.
4. In the lower left of the screen near the **Performance** tab, select the **Real-Time Data** or **Historical Data** option. The default is real-time data.
   - For real-time data, from the **Interval (seconds)** pull-down menu, select the interval to collect real-time data (**15**, **30**, **45**, **60**) seconds.
   - For historical data, from the **Date Range** pull-down menu, select one of the following options: **Last 12 hours**, **1 d**, **1 w**, or **1 m**.

Data Collection

To configure the data collection schedule:

1. Navigate to the **Jobs > Data Collection** screen.
2. Click the **Schedule Data Collection** link.
   The **Edit Data Collection** window displays.
3. Check the fabrics to enable data collection.
4. From the **Polling Rate** pull-down menu, select the polling rate.
   a) **15 Minutes (default)**

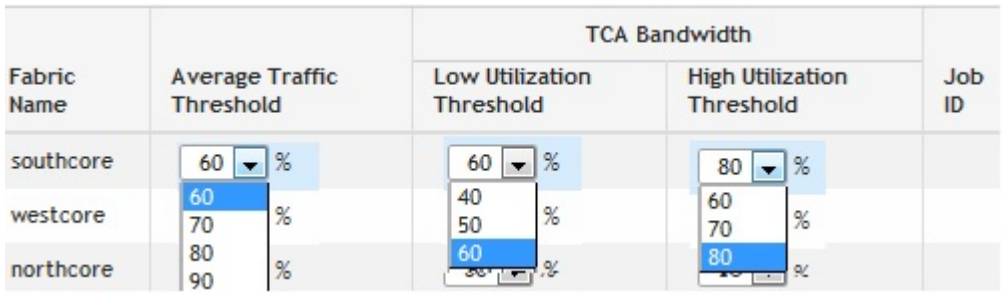
b) **30 Minutes**
c) **45 minutes**
d) **1 Hour**

5. Check the fabric to collect data from.
6. Click the **OK**.

TCA Threshold Settings

To configure the monitoring link bundle and Threshold Crossing Alert (TCA) between the spine switches and the leaf switches for a fabric, use the **Jobs > Data Collections > Edit Threshold Settings** screen. The **Average Traffic Threshold** option monitors the Layer 3 fabric link bundle. The **TCA bandwidth** option monitors Layer 2 and Layer 3 fabrics low bandwidth and high bandwidth "In Traffic Utilization" and "Out Traffic Utilization".

When the average traffic, low and high utilization thresholds are both exceeded AFM receives an alarm from the switch on the **Alerts > Active Alerts** screen.



Average Traffic Threshold	Average Traffic Threshold configures the threshold value for a Layer 3 fabric. The monitoring value is only configured on the fabric link between the spine and leaf switches. Range: 60--90%
Low Utilization	Low Utilization Threshold sets the value for TCA. When the statistics is set below the Low utilization, the TCA alarm clears. The graphical performance monitoring removes a RED solid line with label as "Traffic Utilization Alert Threshold" from the chart. Range: 40-60%
High Utilization	High Utilization Threshold sets the highest value for TCA. When the statistics is beyond the threshold, the TCA alarm raises. The behavior from graphical performance monitor is to draw a RED solid line with label as "Traffic Utilization Alert Threshold" on the chart. Range: 60-80%
Job ID	When the schedule is created, AFM creates a job ID.

With real-time performance management at the port level, a RED solid line appears on the threshold with the label "Traffic Utilization Alert Threshold". This indicates that TCA has exceeded the threshold. When the alarm is cleared, the RED solid line disappears.

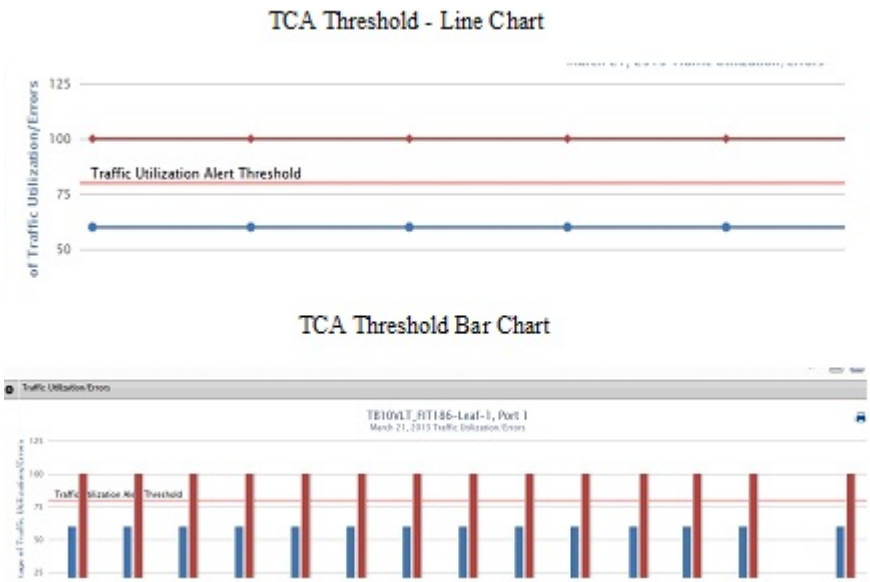


Figure 36. Example: TCA Exceeds the Threshold

For information about how to view port performance, see Port Performance. Make sure that you select the **Real-Time Data** option.

Reports

This section contains the following topics:

- Creating New Reports
- Editing Reports
- Running Reports
- Deleting Reports
- Duplicating Reports

NOTE: To run a report, schedule the data collection to start the task. See Data Collection.

Creating New Reports

To create a new report:

1. Navigate to the **Network** > *Fabric Name* > **Reports** screen.
2. Click the **New Report** button.
   The **Add/Modify Reports** screen displays.
3. In the **Report Name** field, enter the name of the report.
4. (Optional) In the **Description** field, enter a description of the report, then click **Next**.
5. In the **Type and Output** field:
   a) Select a report type: **Switch** or **Port**.
   b) Select a report output format: **Tabular** or **Chart**.

6. Click **Next**.
7. In the **Date/Time Range** pull-down menu, select a date or time range using one of the following options. If you select the custom range, specify a start and end date.
   a) **30 days**
   b) **7 days**
   c) **24 hours**
   d) **Custom Range**
8. Click **Next**.
9. In the **Monitors** field, select which monitors to use for the report: **CpuUtilization** (CPU utilizatizaton), **MemUtilization** (memory utilization), and then click the **>>** button.
10. In the **Query** field, to determine what nodes to include in the report for a fabric:
    a) Select the core to query from the first pull-down menu.
    b) Select the type of switches (spine and leaves) from the 2nd pull-down menu.
11. In the **Available Nodes/Ports** area, select the nodes to include in the report, and then click the **>>** button.
12. In **Summary** screen, review the report settings.
13. If you want to run the report now, check the **Run Report Now** option.
14. Click the **Finish** button.

Editing Reports

To edit a report:

1. Navigate to the **Network** > *Fabric Name* > **Reports** screen.
2. Select the report to edit.
3. Click the **Edit** button.

   The **Add/Modify Report** screen displays.
4. Edit the report. Click the **Next** button to navigate to different parts of the report.
5. In the **Summary** area, review your changes.
6. Click **Finish**.

Running Reports

Before you can run a report, schedule the data collection to start the task. For information on scheduling data collection, see Data Collection.

To run a report:

1. Navigate to the **Network** > *Fabric Name* > **Reports** screen.
2. Select the report to run.
3. Click the **Run** button.

Duplicating Reports

To duplicate a report:

1. Navigate to the **Network** > *Fabric Name* > **Reports** screen.
2. Select a report to duplicate.
3. Click the **Duplicate** button.

The **Duplicate** screen displays.

4. In the **Report Name** field, enter the name of the report.
5. (Optional) In the **Description** field, enter a description.
6. Modify the report as needed.
7. Click the **Next** button to navigate to different parts of the report that you want to duplicate.
8. Click **Finish**.

Deleting Reports

To delete a report:

1. Navigate to the **Network** > *Fabric Name* > **Reports** screen.
2. Select the report to delete.
3. Click the **Delete** button.
   The **Delete Confirmation** window displays.
4. Click **Yes**.

12

Maintenance

This section contains the following topics:

- Backing Up the Switch Configuration
- Scheduling Switch Software Updates
- Replacing a Switch
- Updating the AFM

Back Up Switch

To schedule the number of days to keep switch backup files on the AFM, use the **Back Up Switch** screen. Use this screen to view the fabric, switch name, software version that the switch is running, the startup configuration, running configuration, backup time, and description of the backup configuration.

This screen has the following options:

- **Switch Backup** — Schedule a back up for a switch running configuration and startup configuration files to run now or schedule it for a later time. For information about this option, see Scheduling a Back Up Switch Configuration.
- Edit Description — Edits the description of the backup. After you have created a back up, you can then edit the description of the backup configuration.
- Restore — Restores either the startup configuration (default) or running configuration that has been backed up earlier.
- Delete — Deletes a backup configuration.

Restoring a Switch Configuration

To either restore the startup configuration (default) or running configuration that has been backed up earlier:

1. Navigate to the **Network** > *Fabric Name* > **Maintenance** screen.
2. Click the **Switch Backup** button to display the switch backup options.
3. Select a backup switch configuration to restore.
4. Click the **Restore** link.
5. Select one of the following restore options:
   - **Restore Startup Config (default)**
   - **Restore Running Config**
6. Click the **OK** button.

Deleting a Backup Configuration

To delete a switch backup configuration:

1. Navigate to the **Network** > *Fabric Name* > **Maintenance** screen.
2. Click the **Switch Backup** button to display the switch backup options.
3. Select a backup switch configuration to delete.
4. Click the **Delete** link to delete the switch backup configuration.
5. Click the **Yes** button.

Editing Description

To edit a switch backup description:

1. Navigate to the **Network** > *Fabric Name* > **Maintenance** screen.
2. Click the **Switch Backup** button to display the switch backup options.
3. Select a backup switch configuration to edit.
4. Click the **Edit Description** link to edit the description for switch backup configuration.
5. Edit the description.
6. Click the **OK** button.

Updating the Switch Software

The **Network** > *Fabric Name* > **Maintenance** > **Update Software** screen displays the summary of software for each switch in the fabric. This screen has the following options:

- Schedule Switch Software Update — Creates new schedule job software image upgrade and software image activation.
- Schedule Activate Standby Partition— Activates the software available in the standby partition of the device as a schedule job to happen at later time or to run immediately.

Replacing a Switch

To replace a switch in the fabric:

1. Decommission Switch
2. Pre-deploy the Replacement Switch
3. Deploy Replacement Switch

Step 1: Decommissioning a Switch

When you decommission (replace) a switch, consider the following:

- The switch needs to be manually powered off.
- The switch is automatically placed in an “unmanaged state”.

- When there is a “dead device”, the AFM uses the latest periodic backup file or latest configuration file for validation.
- The new switch should have a factory default setting (to avoid skipping the DHCP configuration load).
- This configuration is deployed to the replaced new switch.
- Backup configuration is always the current running configuration.
- Before powering on the new switch, powered-off the old switch.
- Update the DHCP configuration on the DHCP server with the new system MAC address as generated by the AFM and FTOS images and device configuration files should be available in the FTP/TFTP server.

To decommission a switch:

1. Navigate to the **Network** > *Fabric Name* > *Switch Name*.
2. Click the Replace Switch tab and then click the **Decommission Switch** link.

   The **Decommission Switch** screen is displayed.
3. Review and follow the instructions on the **Decommission** screen.
4. Click the **Save** button to save the text file that contains information to submit a Return Material Authorization (RMA). Send this information to your Dell Networking software support to arrange replacement.

   For information about pre-deploying a replacement switch, see Pre-deploy Replacement.

Step 2: Pre-deploy Replacement Switch

To pre-deploy a replacement switch:

1. Navigate to the **Network** > *Fabric Name* > *Switch Name* screen.
2. Click the **Replace Switch** tab and then click the **Pre-deployment Replacement** link.
3. Review the instructions on the **Switch Cabling** screen. Confirm that the replacement switch is racked, cabled, and powered on. If this is not the case, use the following wiring diagram to cable the replacement switch.
4. Click the **Next** button.

   The **MAC Replacemen**t screen displays.
5. In the **New MAC address** field, enter the system MAC address for the replacement switch.
6. Click the **Next** button.

   The **DHCP** screen is displayed.
7. Save the replacement switch DHCP configuration file.
8. Review the **Summary** screen and then click the **Finish** button.
9. Before you deploy the switch, integrate the new DHCP file, which contains the system MAC address of the replacement switch, into the DHCP server.
10. Deploy the switch. See Deploy Replacement Switch.

Step 3: Deploy Replacement Switch

To deploy a replacement switch:

1. Navigate to the **Network** > *Fabric Name* > *Switch Name* screen.
2. Click the **Replacement Switch** tab.
3. Click the **Deploy Replacement** link.

   Note: If you make changes to switch outside of the AFM; for example, using Telnet, you might need to use the restore option, to restore the switch configuration.

Updating the AFM

To view and manage AFM server updates. use the **Administration** > **Update Server** screen.

Updating the AFM Software

1. Navigate to the **Administration** > **Update Server** screen and then click the **Update Server** link.
   The **Update Server** screen is displayed.
2. In the **Select RPM packing file location** area, choose one of the following options:
   - **Local Drive (DVD, USB)**
   - **Remote Server**
     1. From the **Protocol Typ**e pull-down menu, select the protocol type: **https**, **ftp**, or **sftp**
     2. Specify the path of the RPM packaging file.
     3. (Optional) Enter the user name.
     4. (Optional) Enter the password.
3. From the **Select the software method** area, choose one of the following options.
   - **Stage Software Update Only** — The update is copied to the standby partition on the server but will not be applied. This option does not cause a reboot. You must manually triggered the update from the AFM server software update page.
   - **Apply Software Update on the Next Reboot** — The update is copied to the standby partition on the AFM server and applied on the next reboot.
   - **Apply Software Update Now and Reboot** — The update is copied to the standby partition on the server. The update is applied and the reboot automatically occurs once the update completes.
4. Click the **Update** button.

Activating the AFM Standby Partition

Navigate to the **Administration** > **Update Server** screen and then click the **Activate Available Partition** link.

13

Jobs

This section contains the following topics:

- Displaying Job Results
- Scheduling Jobs

Displaying Job Results

To display the status of your jobs, use the **Job Results** screen.

1. Navigate to the **Jobs > Jobs Results** screen.
2. In the upper right of the screen, click the filter icon to filter your job results.
3. In the **Job Name** field, enter the job name.
4. In the **Status** pull-down menu, select one of the following filtering options:
   - **All**
   - **Success**
   - **Failure**
   - **In Progress**
5. In the **Start From** area, click the select date and time icon to specify the start from date.
6. In the **Start To** area, click the select date and time icon to specify the start to date.
7. In the **End Date From** area, click the select date and time icon to specify the end date from.
8. In the **End Date to** area, click the select date and time icon to specify the end date to.
9. Click the **Apply** button.

Scheduling Jobs

To schedule jobs, use the **Jobs** > **Scheduled Jobs** screen. You can also schedule jobs at the **Network** > **Fabric Name** > **Maintenance** screen.

- **Add Job** — Create a new schedule job to do the following:
  - Switch Backup — Backup a switch running configuration and startup configuration file.
  - Switch Software Update — Creates a job to upgrade the switch software image.
  - Switch Software Activation — Activate the software available in the standby partition of the switch as a schedule job to happen at later time or to run immediately.
- **Run Now** — Starts a job immediately. Select a job and then click the **Run** link.
- **Edit** — Edit or modify an existing job schedule.

NOTE: You can only change the scheduled time. You cannot change the job name, image location, or switch.

- **Delete** — Deletes a job. Select a job and then click the **Delete** link.
- **Enable** — Enable the job or activate the schedule.
- **Disable** — Disable the job or the schedule, without having to delete the job.

Switch Backup

To backup a switch running configuration and startup configuration files, use the **Switch Backup** screen.

1. Navigate to the **Jobs** > **Scheduled Jobs** screen.
2. From the **Add** pull-down menu, select the **Switch Backup** option.
   The **Switch Backup** screen displays.
3. In the **Name** field, enter the name of the job.
4. (Optional) In the **Description** field, enter a description of the job.
5. Click the **Next** button.
   The **Selected Switches** screen displays.
6. In the **Available** area, select the fabric and then switches to backup.
7. Click the **>>** button to move the switches to backup to the **Selected Switches** area and the click the **Next** button.
8. On the **Schedule** screen select one of the following options:
   - **Run Now** — Back ups the switch software immediately.
   - **Schedule job to start on** — Specify a date and time to schedule the job to backup the switch software.

   The **Summary** screen displays.
9. Review the settings in the **Summar**y screen and then click the **Finish** button.

Switch Software Updates

As part of ongoing data center operations, you must periodically update the software and configurations in the fabric. You can update one or more switches. Specify the location from which to get the software updates and then schedule the updates to be performed immediately or schedule it for a later date and time.

1. Navigate to the **Jobs** > **Scheduled Jobs** screen.
2. From the **Add** pull-down menu, select the **Switch Software Update** option.
   The **Switch Software Update** screen displays.
3. In the **Job Name** field, enter the name of the switch software job.
4. (Optional) In the **Description** field, enter a description of the job.
5. Click the **Next** button.
   The **Switch Select** screen is displayed.
6. In the **Available** area, select the fabric and then switches to update.
7. Click the **>>** button to move the switches to update to the **Selected** area and the click the **Next** button.
8. In the **Update Location** area, if required, select the TFTP or FTP site for the software updates using the **Edit TFTP or FTP settings** link.

9. In the **Path and Image file name to the software updates on selected TFTP or FTP site** field, specify the path and image file to the switch software update.
10. Click the **Next** button.
11. In **Update Option**, select one of the following options and then click the **Next** button:
    - **Manual** — Update is staged to the secondary partition but not applied.
    - **Automatic** — Apply software update and reboot.

    The **Schedule** screen displays.
12. On the **Schedule** screen select one of the following options:
    - **Run Now** — Updates the switch software immediately.
    - **Schedule job to start on** — Specify a date and time to schedule the job to update the switch software.

      The **Summary** screen is displayed.
13. Review the settings in the **Summary** screen and then click the **Finish** button.

Switch Software Activation

To activate the software available in the standby partition of the switch as a scheduled job to happen at later time or to run immediately, use the **Switch Software Activation** option.

To active the software in the standby partition of the switch:

1. Navigate to the **Jobs** > **Scheduled Jobs** screen.
2. From the **Add** pull-down menu, select the **Switch Software Activation** option.

   The **Activate Standby partition** screen displays.
3. In the **Job Name** field, enter the name of the job.
4. (Optional) In the **Description** field, enter a description of the job.
5. Click the **Next** button.

   The **Switch Select** screen displays.
6. In the **Available Switches** area, select the fabric and then the switches to update.
7. Click the **>>** button to move the selected switches into the **Selected** area and then click the **Next** button.

   The **Schedule** screen displays.
8. Select one of the following options and then click the **Next** button:
    - **Run Now** — Actives the standby partition immediately.
    - **Schedule job to start on** — Specify a date and time to schedule the job.

    The **Summary** screen displays.
9. Review the settings and then click the **Finish** button.

Scheduling Switch Software Updates

The **Update Software** screen displays the summary of software for each switch in the fabric. To create a new schedule job for backup, software image upgrade and software image activation, use the **Schedule Switch Software Update** option.

As part of ongoing data center operations, you must periodically update the software and configurations in the fabric. You can update one or more switches. Specify the location to get the software updates and then schedule the updates load immediately or schedule it for a later date and time.

To schedule switch software updates:

1. Navigate to the **Network** > *Fabric Name* > **Maintenance** screen.
2. Click the **Update Software** button.
3. Click the **Schedule Switch Software Update** link.
4. **Job Name**:
   - In the **Job Name** field, enter a unique name for the software job.
   - (Optionally) In the **Description** field, enter a description for the schedule software update.

     The **Select Switches** screen displays.
5. **Switch Select**:
   a. In the **Available** area, select the fabric and then the switches to update.
   b. Click the **>>** button to move the selected switches to the **Selected Switches** area.
   c. Click **Next**.
6. In the **Update Location**:
   - Select the TFTP or FTP site for the software updates using the **Edit TFTP or FTP settings** link.
   - Enter the path and image name of the software file on the TFTP or FTP site for each type of switch.
   - Click the **Next** button.
7. In **Update Option**
   - Select one of the following options:
     * **Manual** — Update is staged to the secondary partition but not applied.
     * **Automatic** — Apply software update and reboot.
   - Click the **Next** button.
8. In the **Schedule** screen, select one of the following options and then click the **Next** button:
   - **Run Now** — Run the switch software update immediately.
   - **Schedule job to start on** — Schedule the job at a later time. Specify the start date and time for the software update job.
9. In the **Summary** screen, review the software update software settings and then click the **Finish** button.

Activating Standby Partition Software

To activate the software available in the standby partition of the switch as a scheduled job to occur at a later time or to run immediately, use the **Schedule Activate Standby Partition** option.

To active the software in the standby partition of the switch:

1. Navigate to the **Network** > *Fabric Name* > **Maintenance** screen.
2. Click the **Update Software** button.

3. Click the **Schedule Activate Standby Partition** link.
4. In the **Job Name** field, specify the name of the job.
5. (Optional) In the **Description** field, enter a description of the job.
6. Click the **Next** button.
7. From the **Spines and Leaves** pull-down menu select one of the following options:
   - **Spines and Leaves**
   - **Leaves**
   - **Spines**
8. Select that switches to have their standby partition activated and then click the **>>** to move them to the **Selected** area and then click the **Next** button.
9. From the **Schedule** screen, select one of the following options and then click the **Nex**t button.
   - **Run Now** — Schedule the job to run immediately.
   - **Schedule job to start on** — Schedule the job to run at later time.
10. Review the **Summary** settings and click the **Finished** button.

Scheduling a Back Up Switch Configuration

To schedule the number of days to keep the switch backup files in the AFM:

1. Navigate to the **Network** > *Fabric Name* > **Maintenance** screen.
2. Click the **Switch Backup** button to display the switch backup options.
3. Click the **Switch Backup** link.

   The **Job Name** screen displays.
4. In the **Name** field, enter the name of the software job name.
5. In the **Description** field, optionally enter a description and then click the **Next** button.

   The **Select Switches** screen displays.
6. Navigate to the **Available** area:
   a. From the **Switch Type** pull-down menu, select the type of switches to update.
   b. In the **Available Switches** area, select the switches to update.
   c. Click the **>>** button to move the selected switches to the **Selected Switches** area and then click the **Next** button.

      The **Schedule** screen displays.
7. In **Start** area, select one of the following options:
   - **Run Now** — Run the job now.
   - **Schedule job to start** — Specify when to schedule job.
8. In the **Summary** screen, review your settings, and then click the **Finish** button.

14

Administration

This section contains the following topics:

Administrative Settings

To configure Administrative Settings, use the **Administration** > **Settings** screen:

NOTE: The AFM allows you to configure the SNMP configuration and CLI credentials before designing and deploying the fabric. You cannot edit SNMP and CLI credentials settings during the run phase.

CLI Credentials

To provision the fabric, enter the FTOS CLI user's credential and enable the configuration credential for all the switches in the fabric. This option allows you to remotely make configuration changes to the switches in the fabric.

To configure the CLI credentials and enable the configuration credential for all the switches in the fabric:

1. Navigate to the **Administration > Settings** screen.
2. In the **CLI Credentials** area, click the **Edit** button.
3. In the **Protocol** pull-down menu, select one of the following options:
   - **Telnet**
   - **SSHv2**
   - In the **User Name** field, enter the user name.

- In the **Password** field, enter the password.
- In the **Confirm Password** field, confirm the password. The privilege level is a read-only field and is set at 15.
- In the **Enable Password** field, enter a password for the privilege level.
- In the **Confirm Enable Password** field, confirm the enabled password for the privilege level.
- Click **OK**.

Client Settings

To configure the maximum number of browser windows for each user's session and the polling interval from the AFM to the switches in the fabric:

1. Navigate to the **Administration > Settings** screen.
2. In the **Client Settings** area, click **Edit**.
3. In the **GUI Polling Interval (in Seconds)** pull-down menu, select one of the following options. The default value is **60** seconds.
   - **15 Secs**
   - **30 Secs**
   - **60 Secs**
   - **120 Secs**
4. In the **Pop-out Client Session** pull-down menu, select the maximum number of browser windows (from 3 to 7) for each user's session. The default value is **3**.
5. Click **OK**.

Data Retention Settings

To configure the amount of time to retain performance history:

1. Navigate to the **Administration > Settings** screen.
2. In the **Data Retention** area, click the **Edit** button.
3. In the **Performance History** area, enter the number of days you want to retain your performance history. The range is from 1 and 180 days.
4. In the **Daily Purge Execution Time** pull-down menu, specify the time to begin purging the performance history data.
5. Click **OK**.

DHCP Server Settings

1. Navigate to the **Administration > Settings** screen.
2. Navigate to the DHCP Server Settings area and select one of the following settings:
   - **Local** — AFM provisioned as a DHCP server. When you select this option, the AFM automatically integrates the generated dhcp.config file into the DHCP server on the AFM during pre-deployment.
   - **Remote** — Use External DHCP server. When you select this option, manually install the dhcpd.conf file that is generated during pre-deployment into the DHCP server before you deploy the fabric.

3. Click the **OK** button.

NTP Server Settings

To configure NTP Server Settings:

1. Navigate to the **Administration** > **Settings** screen.
2. In the **NTP Server Settings** area, click the **Edit** link.
3. Enter the NTP server primary IP address.
4. Enter the IP status address.
5. Enter the NTP server secondary IP address.
6. Enter the Secondary IP status address.
7. Click the **OK** button.

SMTP Email

To configure SMTP email:

1. Navigate to the **Administration Settings** screen
2. In the **Secure SMTP Email Settings** area, click the **Edit** link.
3. In the **Outgoing Mail Server** field,
4. In the **Server Port** field, enter the port number of the email server.
5. In the **User Name** field, enter the user name.
6. In the **To Email Address(es)** , enter the mail addresses separated by comma " ; ".
7. In the **Minimum severity level to Email Notification** pull-down menu: select one of the following settings:
   - **Critical**
   - **Major**
   - **Minor**
   - **Warning**
8. Click the **OK** button.

SNMP Configuration

Configure SNMP so that theAFM can perform SNMP queries on the switches in the fabric. The values you enter in the SNMP configuration are also used for configuring the switches during the build phase and for monitoring during the run phase.

1. Navigate to the **Administration > Settings** screen.
2. In the **SNMP Configuration** area, click **Edit**
3. In the **Read Community String** field, enter the read community string. For example, “public”.
4. In the **Write Community String** field, enter the write community string. For example, “private”.
5. In the **Port** field, enter the SNMP port number of the switches. The port number is typically 161.

6. In the **Trap Host** field, specify the IP address of the AFMso that the traps are sent to the AFM.
7. Click **OK**.

Syslog Server IP Addresses

1. Navigate to the **Administration > Settings** screen.
2. In the **System IP Addresses** area, you can configure up to 8 syslog server IP addresses to log events on the switches in the fabric. By default, the first syslog IP address entry is the AFM system IP address.

System Information

1. Navigate to the **Administration > Settings** screen.
2. From the **System IP Address** pull-down menu, select the IP address to manage the AFM.

   NOTE: If there are multiple Network Interface Card (NIC) adapter cards on the AFM, select the IP address to manage the AFM.

TFTP/FTP Settings

1. Navigate to the **Administration > Settings** screen.
2. From the **File Transfer Protocol** pull-down menu, select one of the following options:
   - **TFTP** (default)
   - **FTP**
3. In the **TFTP/FTP Settings** area, select one of the following options:
   - **Local** — AFM provisioned as a TFTP/FTP server.

     NOTE: When you use the **Local** option, the TFTP or FTP server must be in the same subnet.

     * If you select the local TFTP server option, the TFTP server uses the AFM management IP address.
     * If you select the local FTP server option, the FTP server uses the AFM management IP address. Enter the AFM user name and password.
   - **Remote** — External TFTP/FTP server
     * If you select the FTP protocol and remote options, enter the FTP server IPv4 address, user name and password.
     * If you select the TFTP protocol and remote options, enter the TFTP IPv4 address.

Managing User Accounts

To view and manage user accounts, use the **Administration > User Accounts** screen.

- User Accounts Summary View — Displays a summary view of user accounts when the user's role is **Superuser**. When the role is a **user** or **administrator**, only the current logged in user's account information displays.
- Add User — Adds new user accounts. You can have up to 50 user accounts but only one **Superuser**.

- Edit User — Edits user accounts.
- Change Password — Allows a user to change his or her password.
- Delete User — Deletes one or more user accounts. The system default user, **Superuser**, cannot be deleted.
- Unlock — Unlocks a user who was locked out because he or she exceeded the maximum login attempts. To unlock a user, select the user and click the **Unlock** option.
- Default User — During the installation process, AFMprompts you to create a **Superuser**.
- Reset Default User (**Superuser**) Password — Contact technical support if you need to reset the **Superuser** password.
- Password Rules — Enforces special password rules for enhanced security. The password must be a minimum of 6 characters and contain one capital letter and one number. The password is masked when you enter it.
- Unsuccessful Login Limit — Specifies the unsuccessful login limit for a user's account. When the unsuccessful login limit is exceeded, the lockout duration is applied.
- Lockout Duration — Specifies the amount of time a user is locked out when he or she exceeds the unsuccessful login limit.
- Sessions Allowed — Specifies the number of sessions a user is allowed.
- Session Timeout — Specifies the session timeout values.

NOTE: The AFM root user name is "superuser" and password is "Superuser1".

The system comes with three pre-defined roles with the following permissions:

Superuser

- Views a summary of user accounts.
- Adds, deletes, and edits users.
- Locks and unlocks users.
- Resets passwords.
- Performs configuration changes.
- Sets session timeout values.
- Terminates AFM users' sessions at the **Administration > User Session** screen.

Administrator

- Performs configuration changes.
- Views performance monitoring.
- Changes his or her own password.

User

- Views configuration and performance monitoring information.
- Changes his or her own password.

Adding a User

To add a user account, you must be a **Superuser**. For more information about user accounts, see Managing User Accounts.

To add a user:

1. Navigate to the **Administration > User Accounts** screen.
2. Click **Add User**.
   The **Add User** screen displays.
3. In the **User Name** field, enter the user's name.
   Enter a unique name that is alphanumeric.
   Length: from 1 to 25 characters.
4. In the **Password** field, enter the user's password.
   The password length must be from 8 to 32 characters and include 3 of the following categories:
   - At least 1 upper-case letter
   - Lower-case letters
   - At least 1 numeric digit
   - At least 1 special character
5. In the **Confirm Password** field, enter the user's password.
6. In the **First Name** field, enter the user's first name.
   The first name can contain any characters.
   Length: 1 to 50 characters.
7. (Optional) In the **Last Name** field, enter the user's last name.
   The last name can contain any characters.
   Length: 1 to 50 characters.
8. From the **Role** pull-down menu, select one of the following roles: **Admin** or **User**.
   For information about roles, see Managing User Accounts.
9. In the **Sessions Allowed** pull-down menu, specify the number sessions allowed for the user.
   You can specify from **1** to **5** sessions. The default value is **5**.
10. In the **Session Timeout** pull-down menu, specify one of the following timeout values. The default value is **15 minutes**.
    a) **15 minutes**
    b) **30 minutes**
    c) **45 minutes**
    d) **60 minutes**
11. In the **Unsuccessful Login Limit** pull-down menu, select value from **3** to **10**. The default value is **5**.
12. In the **Lockout Duration** pull-down menu, select one of the following options. The default value is **30 minutes**.
    a) **15 minutes**
    b) **30 minutes**
    c) **45 minutes**
    d) **60 minutes**
    e) **Permanent**
13. Click **OK**.

Deleting a User

To add or delete users, you must be a **Superuser** . For more information about user accounts, see Managing User Accounts.

To delete a user:

1. Navigate to the **Administration > User Accounts** screen.
2. Select the user that you want to delete.
3. Click the **Delete** button.
4. Click **Yes**.

Editing a User

To edit a user, you must be a **Superuser** . For more information about user accounts, see Managing User Accounts.

To edit a user:

1. Navigate to the **Administration > Settings > User Accounts** screen.
2. Click on the user to edit.
3. Click **Edit**.
   The **Edit User Settings** screen displays.
4. In the **First Name** field, enter the user's first name.
5. In the **Last Name**, enter the user's last name.
6. In the **Password** field, enter the user's password.
7. In the **Confirm Password** field, enter the user's password.
8. In the **Sessions Allowed** pull-down menu, specify the number sessions allowed for the user.
9. In the **Session Timeout** pull-down menu, specify one of the following timeout values:
   a) **15 minutes**
   b) **30 minutes**
   c) **45 minutes**
   d) **60 minutes**
10. In the **Unsuccessful Login Limit** pull-down menu, select the number of allowed unsuccessful logins (3 to 10)
11. From the **Lockout Duration** pull-down menu, select one the following options:
    a) 15 minutes
    b) 30 minutes
    c) 45 minutes
    d) 60 minutes
    e) Permanent
12. Click **OK**.

Unlocking a User

To unlock a user, you must be a **Superuser** . For information about user accounts, see Managing User Accounts.

To unlock a user:

1. Navigate to the **Administration > Users Accounts** screen.
2. Select the user you want to unlock.
3. Click the **Unlock** button.
4. Click **OK**.

Changing Your Password

To change your password:

1. Go to the upper right of the screen next to your login name.
   A pull-down menu displays.
2. Select **Change Password**.
   The **Change Current Account Password** screen displays.
3. In the **Current Password** field, enter your current password.
4. In the **New Password** field, enter your new password.
   The password length must be from 8 to 32 characters and include 3 of the following categories:
   - At least 1 upper-case letter
   - Lower-case letters
   - At least 1 numeric digit
   - At least 1 special character
5. In the **Confirm Password** field, confirm your new password.
6. Click **OK**.
   For more information about user accounts, see Managing User Accounts.

Managing User Sessions

To display activeAFM users and terminate users' sessions, use the **User Sessions** screen. Only the **Superuser** can terminate a AFM user's session. For more information about user accounts, see Managing User Accounts.

This screen displays the following information:

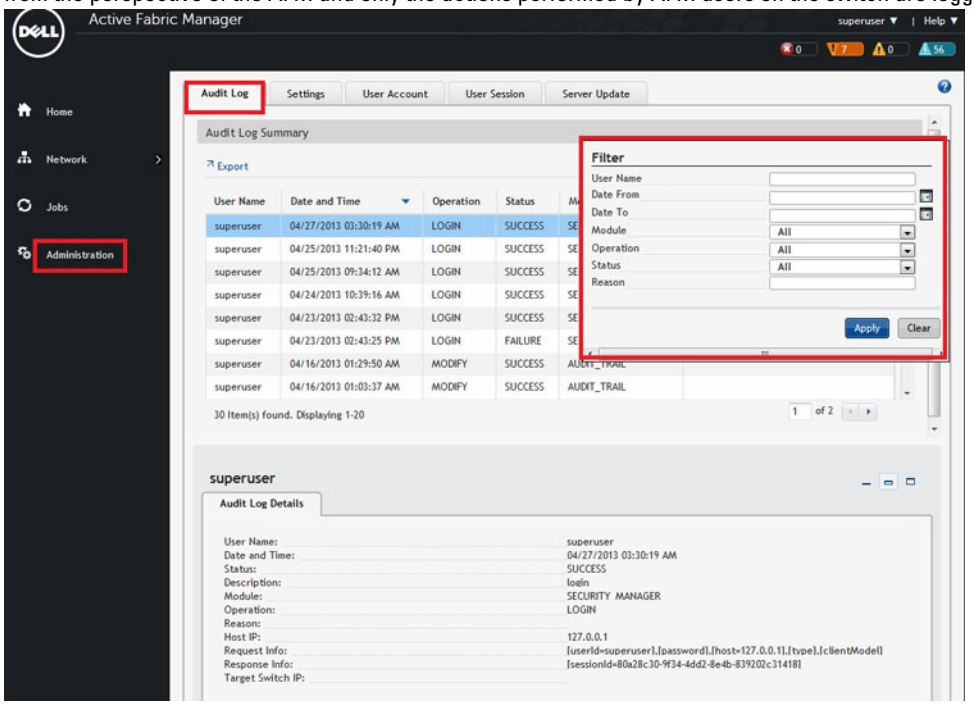
- **Username**
- **Session Login Time**
- **Client IP Address**
- **Current Session**

To terminate AFM **users' sessions**:

1. Navigate to the **Administration > User Sessions** screen.
2. Select the users that you want to log off.
3. Click the **Force Logoff** button.
4. Click **OK**.

Audit Log

To log a chronological sequence of audit records, each of which contains information on who has accessed the switch and what operations the user has performed during a given period of time, use the **Audit Log** screen. The audit log is from the perspective of the AFM and only the actions performed by AFM users on the switch are logged.



1. Navigate to the **Administration** > **Audit Log** screen.
2. Click the filter icon on the upper right of the screen to display the audit trail options.
3. Enter and select your filter criteria for the **User Name** field. For example, "superuser".
4. From the **Date From** pull-down menu, select the beginning date and time of the operation.
5. From the **Date To** pull-down menu, select the end date and time of the operation.
6. From the **Module** pull-down menu, select one of the following AFM modules:
   a) **Security Activation**
   b) **Security Manager**
   c) **Audit Trail**
   d) **UI Manager**
7. From the **Status** pull-down menu, select the one of the following status of audit trail operations:
   a) **Queued**
   b) **In Progress**
   c) **Success**
   d) **Failure**
   e) **Timeout**
   f) **Response Delivered**
   g) **Invalid Request**
8. Click the **Apply** button. You also export your results using the **Export** link.