Active Fabric Manager (AFM) Deployment Guide 2.5

2014 - 4

Rev. A0X

Contents

1

Introduction

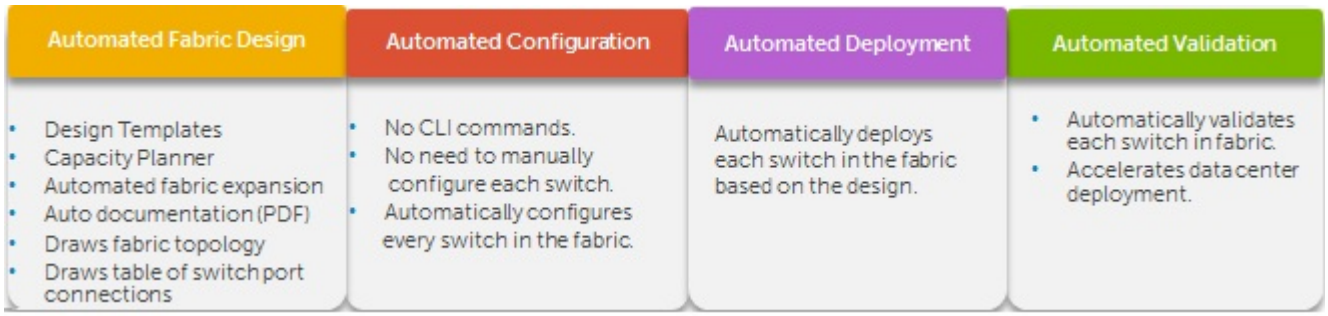
Active Fabric Manager (AFM) is a graphical user interface (GUI) based network automation and orchestration tool that enables you to design, build, deploy, and optimize a Layer 2 Virtual Link Trunking (VLT), Layer 3 distributed core, and Layer 3 with Resiliency (Routed VLT) fabric for your current and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

You can monitor performance at the network, fabric, switch, and port level. You can also display additional performance statistics through AFM using a Dell OpenManage Network Manager (OMNM) server. It automates common network management operations and provides advanced network element discovery, remote configuration management, and system health monitoring to proactively alert network administrators to potential network problems. OMNM provides SOAP-based web services to provide integration with non-Dell products. AFM supports Dell Networking S4810, S4820T, S55, S60, S5000, S6000, IOA blade, 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, that is, manually document 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 that the switches are physically connected to the right switches.

Solution: Active Fabric Manager



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, Layer 3 with Resiliency (Routed VLT), 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

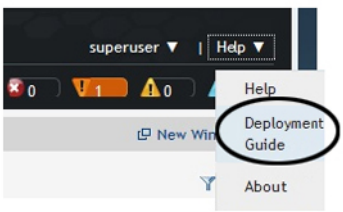
This section contains the following topics:

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

Related links:

- Designing the Fabric
- AFM Site Map
- Supported Fabric Types

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.

NOTE: If you are using the **OpenStack Neutron Managed** option, refer to the *AFM Plug-in for OpenStack Guide*.

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 on the **Home** > **Getting Started** screen. After you complete the installation process, 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 , import an existing design, and discover an existing fabric.

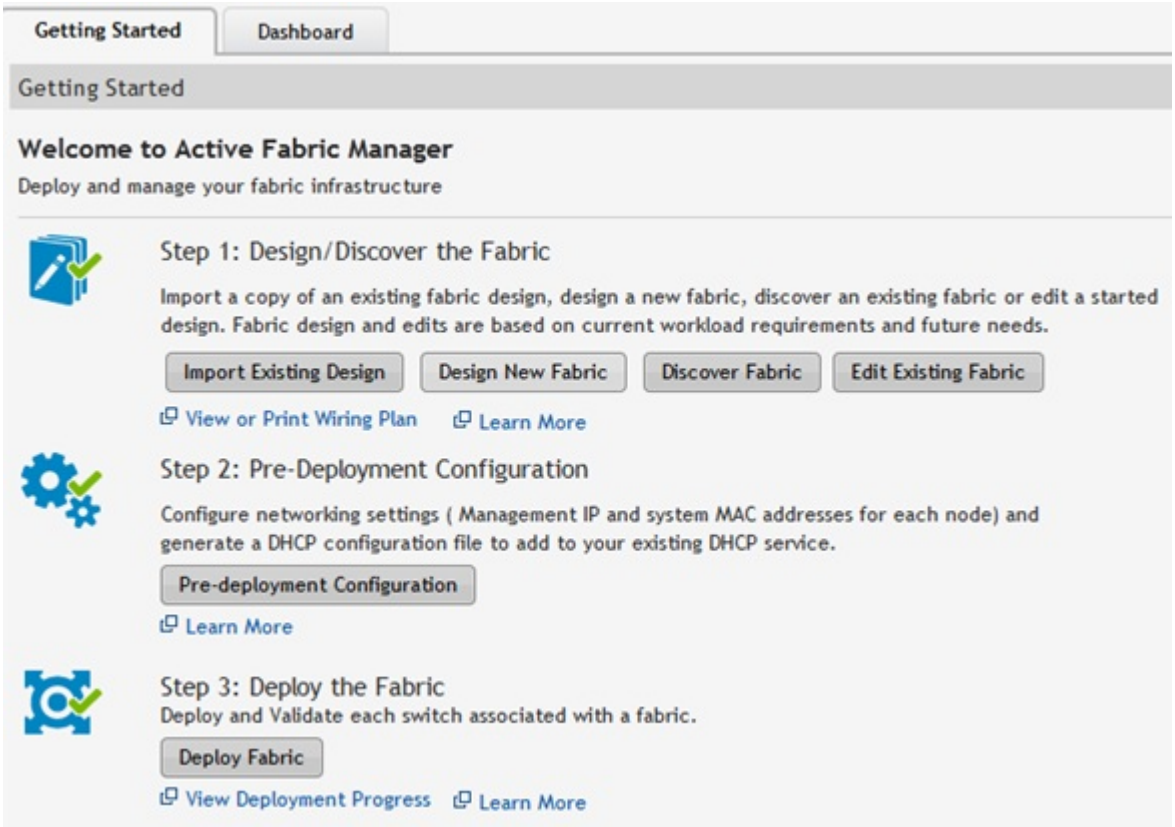


Figure 1. Getting Started Wizard

To design and deploy a Layer 2 VLT, Layer 3 distributed core fabric, or Layer 3 with Resiliency (Routed VLT)

1. Gather useful information.

   Related links.

   - Gather Useful Information for Layer 2 VLT Fabric
   - Gathering Useful Information for a Layer 3 Distributed Core Fabric.
   - Gathering Useful Information for a Layer 3 with Resiliency (Routed VLT) 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 Layer 2 VLT and Layer 3 with Resiliency (Routed VLT) Fabric Design

   Related links for designing a Layer 3 distributed core fabric:

   - Overview of a Distributed Core
   - Terminology

- Selecting a Distributed Core Design

Related links for designing a Layer 3 with Resiliency (Routed VLT):

- Key Considerations for Designing Layer 3 with Resiliency (Routed VLT)
- Selecting a Layer 2 VLT and Layer 3 with Resiliency (Routed VLT) Fabric 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.

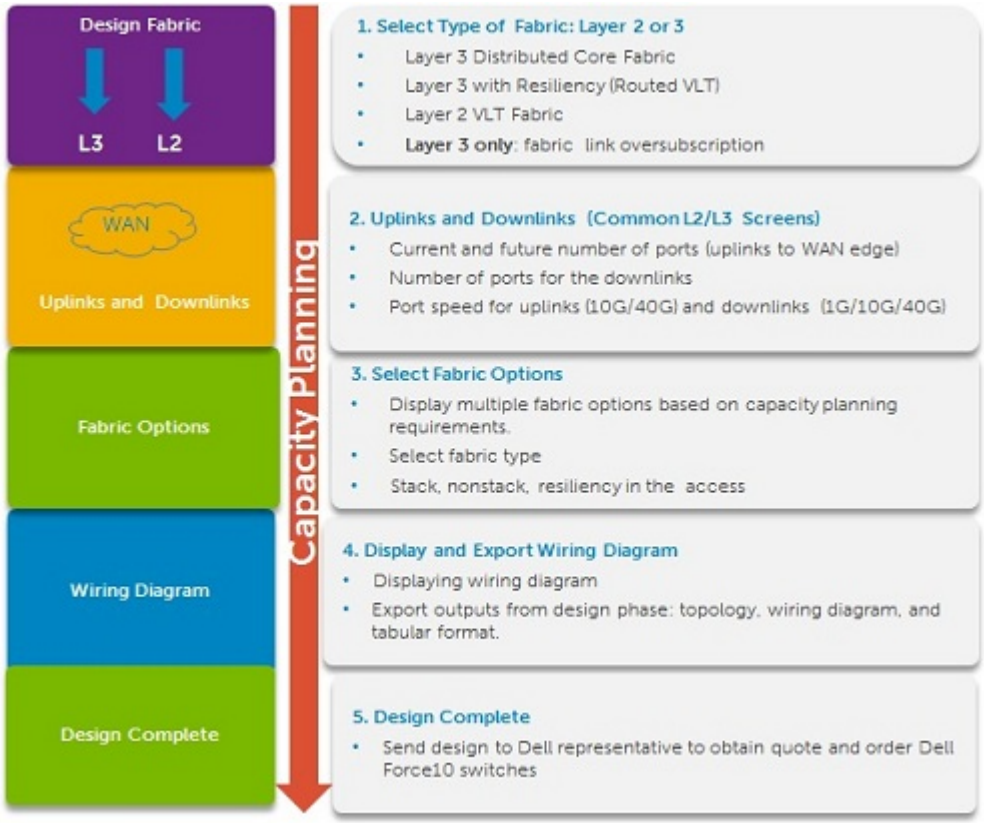


Figure 2. Capacity Planning

Figure 3. Provisioning

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 Discover Fabric Discovery Status	
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 Replace Switch Deploy Switch
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** Active Link Settings CLI Credentials Client Settings Data Retention 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

		DHCP Server Settings NTP Server Settings Email Settings Syslog IP Addresses SNMP Configuration System Information TFTP/FTP Settings			

5

Supported Fabric Types

The fabric design wizard defines the basic configuration for a Layer 2 VLT, Layer 3 distributed core, and Layer 3 with Resiliency (Routed 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 Layer 2 VLT and Layer 3 with Resiliency (Routed VLT) Fabric Design.
- Use the Layer 3 with Resiliency (Routed VLT) fabric to extend equal cost multi-pathing capabilities. For information about supported tiers, see Selecting a Layer 2 VLT and Layer 3 with Resiliency (Routed VLT) Fabric Design.
- Use the IOA fabric design wizard to design a Layer 2 fabric that has an I/O Aggregator (IOA) blade switch in a M1000e chassis. For more information about the IOA Fabric Design Wizard, seeIOA Fabric Design Wizard.

See also Deployment Topology Use Cases. For information about tiers, see Deployment Topology.

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 AFM, it starts the **Getting Started** configuration wizard in the **Welcome to Active Fabric Manager** screen.

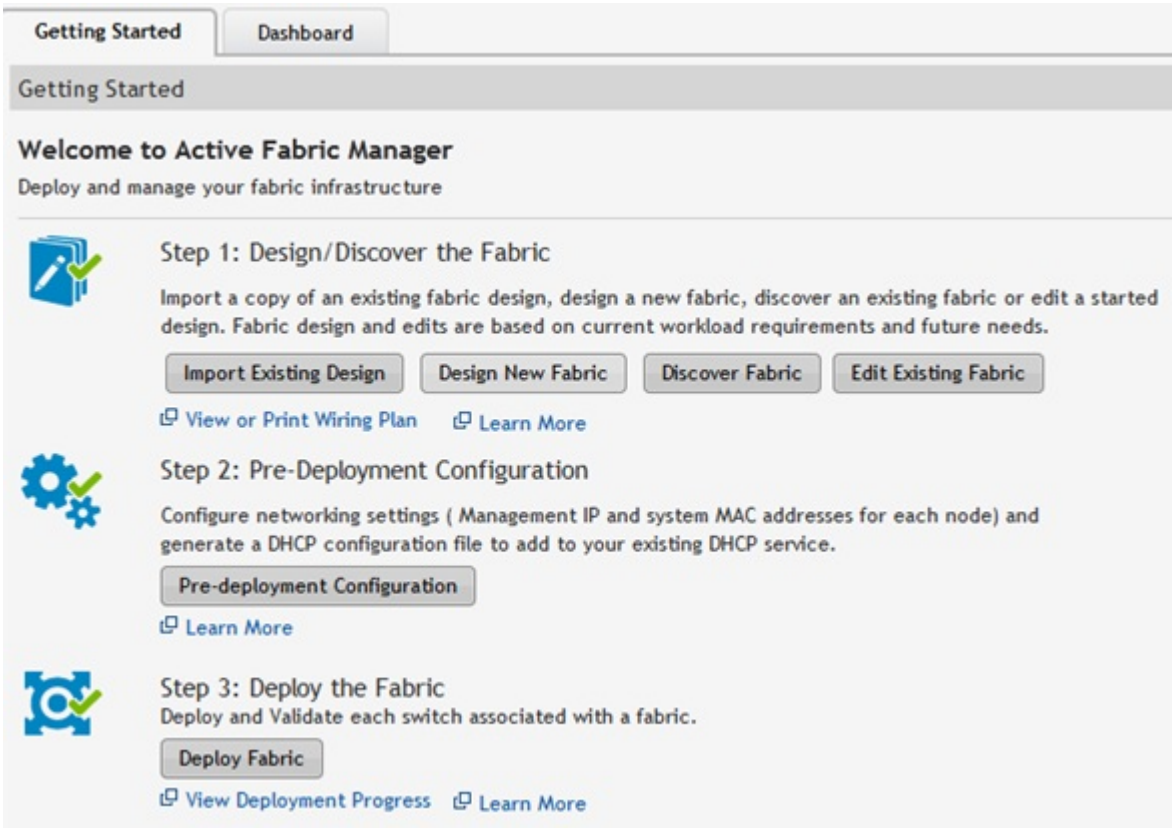


Figure 4. Getting Started Wizard

Key Considerations for Designing a Layer 3 with Resiliency (Routed VLT) Fabric

Use the Layer 3 with Resiliency (Routed VLT) fabric to extend equal cost multi-pathing capabilities. When designing a Layer 3 with Resiliency (Routed VLT) fabric, consider the following:

- You can deploy up to 10 fabrics. However, the fabrics do not communicate with each other.
- AFM manages Dell Networking S4810, S4820T, S6000, and Z9000 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 DHCP Integration and the *FTOS Configuration Guide* for the Dell Networking S4810, S4820T, S6000, and Z9000 switches at https://www.force10networks.com/CSPortal20/KnowledgeBase/Documentation.aspx.

The number and type of switches in a Layer 3 with Resiliency (Routed VLT) fabric are based on the following:

- The number of current uplinks (minimum of 2) and downlinks for the access switches.
- The number of planned edge ports (future uplinks and downlinks) for the access switches.
- Whether the access switches need to act as a ToR or access.

- Fabric interlink bandwidth (the links between the aggregation and access switches).
- Downlinks which can be 1Gb, 10Gb, or 40 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 Bandwidth and Port Count screen, you can only expand the downlinks on the existing fabric.

For information on how to expand a fabric, refer to Editing and Expanding an Existing Fabric Design. For information about tiers, refer to Deployment Topology and Deployment Topology Use Cases.

Gathering Useful Information for a Layer 3 with Resiliency (Routed VLT) Fabric

To gather useful information for a Layer 3 with Resiliency (Routed 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. To specify a TFTP/FTP site, go to the **Administration** > **Settings >TFTP/FTP** screen. For information about which software packages to use, refer to the Release Notes.
- Download the software image for each type of switch in the fabric. 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.
- 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, refer to DHCP Integration.
- Obtain the pool of IP addresses for the management port for each switch in the fabric.
- Obtain IP addresses (must be an even number) for the uplink configuration from the ISP service. The uplink port number range is based on whether a 10 Gb or 40 Gb bandwidth is selected.
  - For 10 Gb uplink bandwidth, AFM supports 2 to 32 uplinks.
  - For 40 Gb uplink bandwidth, AFM supports 2 to 8 uplinks.
- Obtain IP addresses or VLAN ID for the downlink configuration for connecting to the server or ToR.
- Gather protocol configuration for uplinks and downlinks.

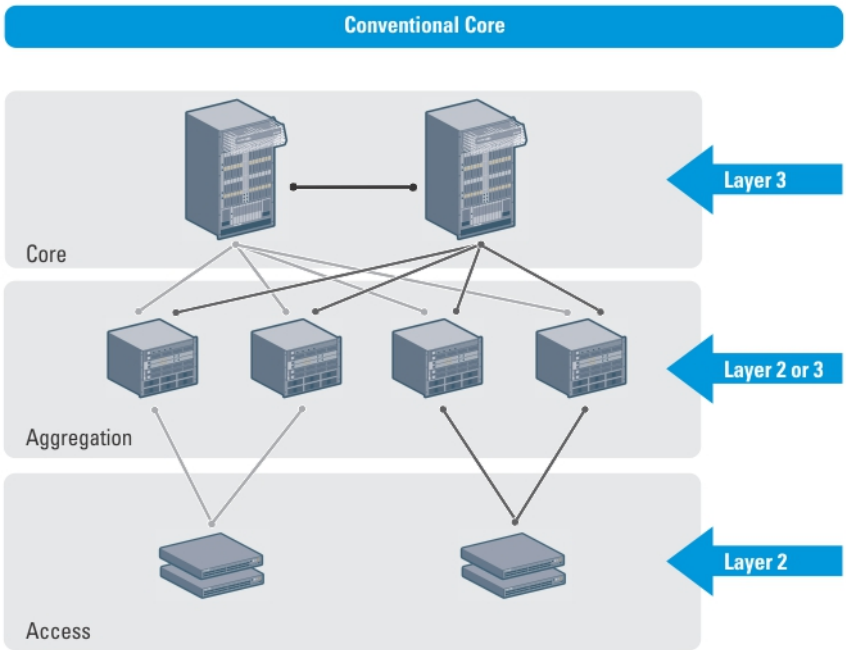
Conventional Core Versus Distributed Core

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:

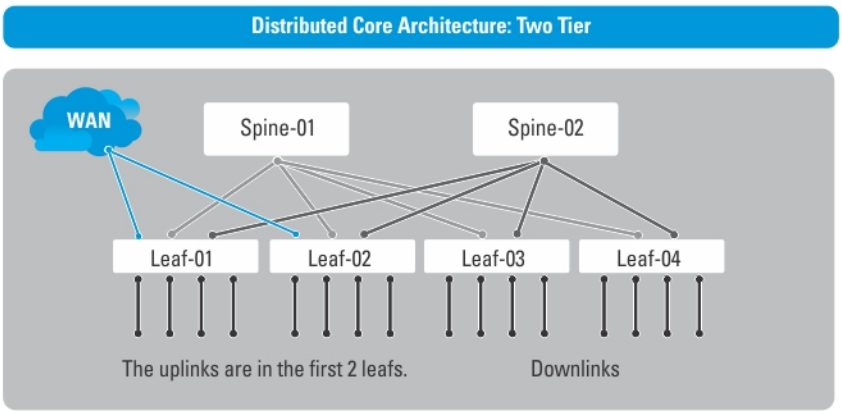
- Core — The core layer routes traffic to and from the internet and the extranet. Redundancy and resiliency are the main factors for high availability, which requires chassis-based core routers.
- Aggregation layer — The aggregation layer connects with top of rack (ToR) switches and aggregates the traffic 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 fabric 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 switches, servers, storage devices, or top-of-rack (TOR) elements. The role of the leaves switches 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 the leaves switches. The role of the spine is to provide an interconnect to all the leaves 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). The uplink can also connect to a router gateway or an external switch.
- Downlinks — An edge port link that connects the leaves to the data access layer; for example, servers or ToR elements.

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

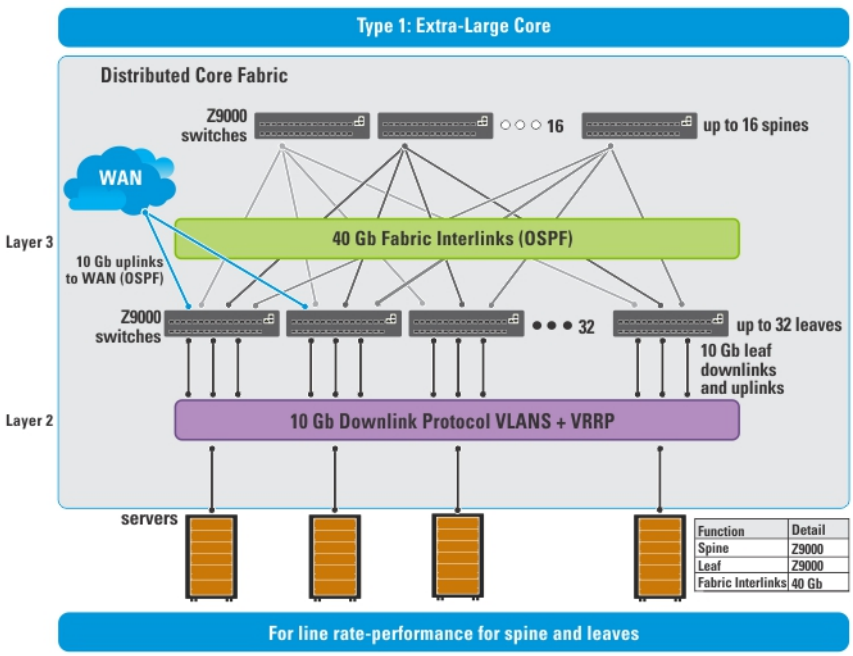
- Fabric Interlinks — Links that connect the spines to the leaves. The fabric interlink bandwidth is fixed: 10 Gb or 40 Gb.
- Fabric over-subscription ratio — Varies the maximum number of available interconnect links. This ratio determines the number of fabric interlinks (the number of communication 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, select the 1:1 fabric over-subscription ratio. This ratio is useful when you require a lot of bandwidth and not a lot of ports.

  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 leaves can act as a 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, S4820T, S6000, 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 DHCP Integration and the *FTOS Configuration Guide* for either the S4810, S4820T, S6000, or Z9000 switches at https://www.force10networks.com/CSPortal20/KnowledgeBase/Documentation.aspx. See also Deployment Topology Use Cases.

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 which are 10 Gb.
- Downlinks which are 1 Gb, 10 Gb, or 40 Gb.
- 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 Gb or 40 Gb.

Important: If you do not specify additional links in the fabric design for future expansion in the **Bandwidth and Port Count** screen, you can only expand the downlinks on the existing 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 comma-separated values (CSV) file that contains the system media access control (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) or File Transfer Protocol (FTP) address from your network administrator or network operator. To specify a TFTP/FTP site, go to **Administration** > **Settings** > **TFTP/FTP** screen. For information about which software packages to use, see the Release Notes.
- Download the software image for each type of switch in the fabric. Each type of switch must use the same version of the software image within the fabric. Place the software images on the TFTP or FTP site so that the switches can install the appropriate FTOS software image and configuration file.
- 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 server. 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 DHCP Integration.
- Obtain pool of IP addresses for the management port for each switch in the fabric.
- Obtain IP addresses (must be an even number) for the uplink configuration from the ISP service. The uplink port number range is based on whether a 10 Gb or 40 Gb bandwidth is selected.
  - For a 10 Gb bandwidth, AFM supports 2 to 32 uplinks.
  - For a 40 Gb bandwidth, AFM supports 2 to 8 uplinks.
- Obtain IP addresses for the downlink configuration for connecting to the server or ToR.
- Obtain IP addresses for the fabric link configuration for the spine and leaf switches.
- Gather protocol configuration for uplinks, downlinks and fabric link 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

- Key Considerations for Designing a Distributed Core Fabric
- Flowchart for Designing and Deploying a Fabric.

With a Layer 3 distributed core topology, you select the **Layer 3** option using the Design Wizard on the **Deployment Topology** screen. For information about distributed core, see Selecting a Distributed Core Design.

DL BW — Downlink Bandwidth

UL BW — Uplink Bandwidth

FLBSL — Fabric Link bandwidth between the spine and leaf

MND — Maximum number of downlinks

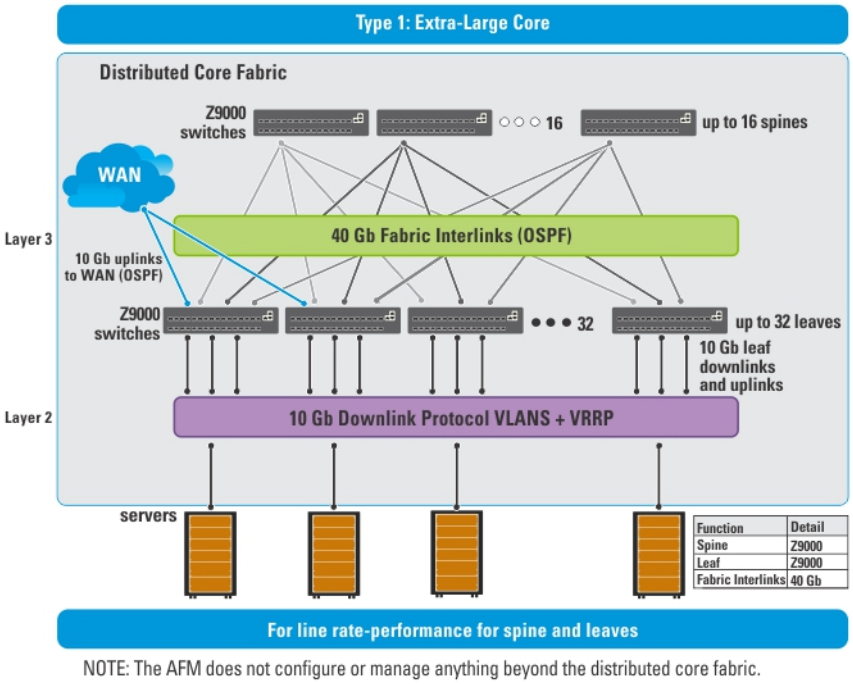
Attention: The maximum number of downlinks is based on using 2 uplinks.

Table 1. 2 Tier Layer 3 Distributed Core Topologies

Type	OS Ratio	DL BW	MND	Maximum # of Spines	Maximum # of Leafs	UL BW	FLBSL	Possible Topologies (Spine and Leaf)
Type 1- Extra Large Core	1:1	10G	2046	16	32	10G	40G	Z9000/Z9000 or S6000/S6000
Type 2- Large Core	1:1	10G	2046	32	64	10G	10G	S4810/S4810
Type 3- Medium Core	3:1	10G	766	4	32	10G	10G	S4810/S4810
Type 3- Medium Core	4:1	10G	1662	3	32	10G	40G	Z9000/S4810 or S6000/S4810
Type 4- Small Core	5:1	10G	894	2	8	10G	10G	S4810/S4810
Type 4- Small Core	3:1	10G	1534	4	16	10G	40G	Z9000/S4810 or S6000/S4810

Type 1: Extra Large Distributed Core Fabric

With a Type 1: Extra Large Distributed Core fabric design, the Z9000 spines (or S6000 spines) connect to the Z9000 leaves (S6000 leaves) at a fixed 40 Gb 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 5. 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 1:1 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 or S6000 leaf for the Type 1: Extra Large Distributed Core design has the following:

- Six hundred forty Gigabit of fabric interlink (fabric links) maximum capacity to the Spine (16 x 40 Gb)
- Forty-eight 10 Gb 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 (fabric links) bandwidth between the spines and leaves of 10 Gb 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 Gb. The maximum number of spines is 32 and the maximum number of leaves is 64, as shown in the following figure.

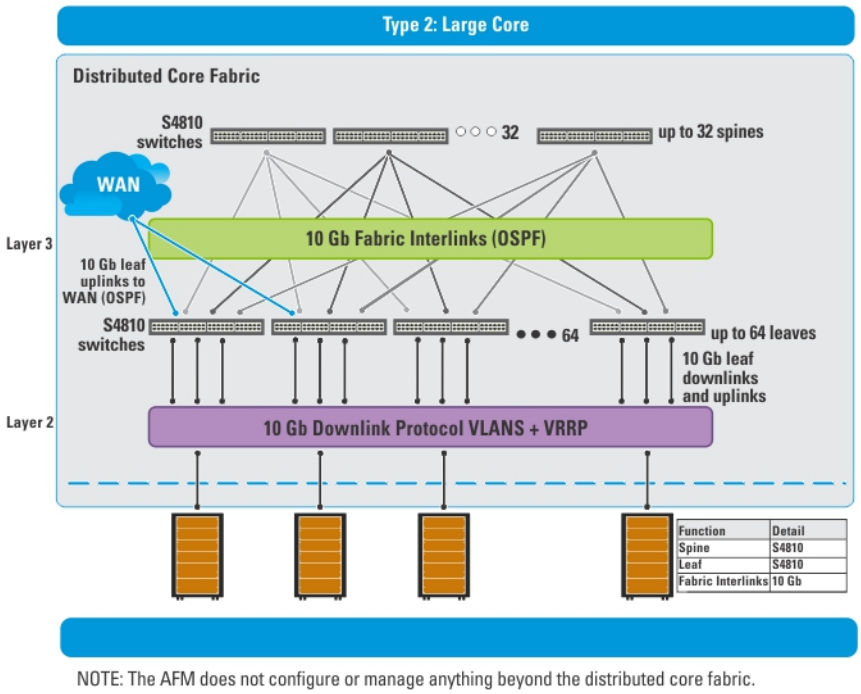


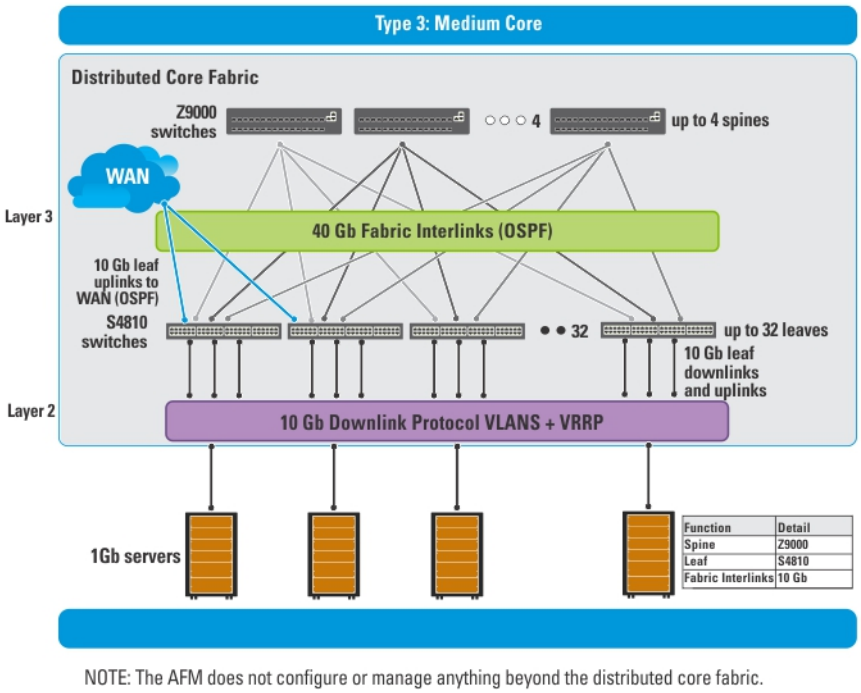
Figure 6. Type 2: Large Distributed Core Fabric Design

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

- Forty gigabit of fabric interlink (fabric links) maximum capacity to the spine (4x 10 Gb)
- Thirty-two 10 Gigabit ports will be used for fabric interlink (fabric links) 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 (S6000 spines) connect to the S4810 leaves at a fixed 40 Gb 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 7. Type 3: Medium Distributed Core Fabric Design

Use the Type 3: Medium Distributed Core design when:

- You require a fabric interlink (fabric links) bandwidth between the spines and leaves at a 40 Gb 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 (S6000 spine) for the Type 3: Medium Distributed Core design has the following:

- Six hundred and forty Gigabit of interlink (fabric links) 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 (fabric links) 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 (fabric links) bandwidth between the spines and leaves of 10 Gb.
- 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 Gb. The maximum number of spines is 4 and the maximum number of leaves is 16, as show in the following figure.

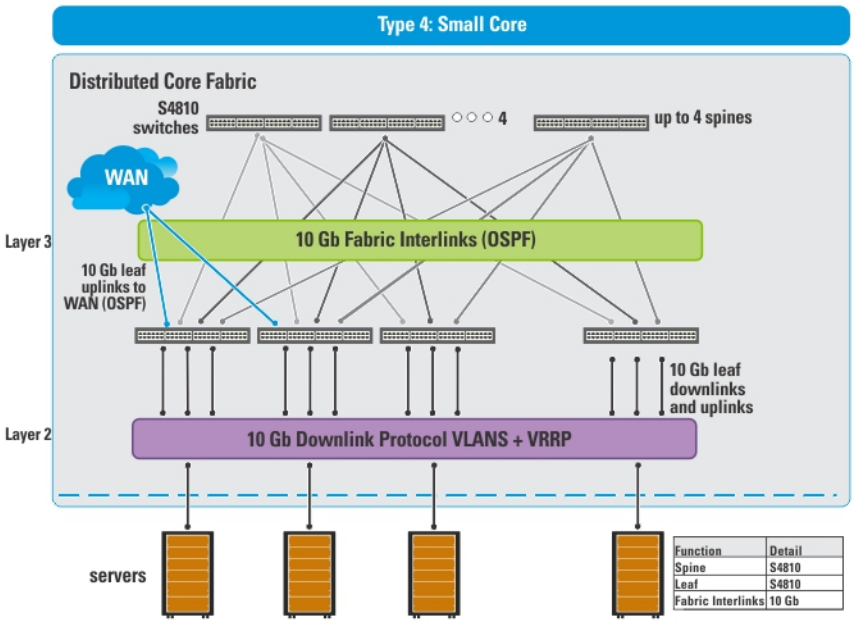


Figure 8. Type 4: Small Distributed Core Fabric Design

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

- Sixteen 10 Gigabit of fabric interlink (fabric links) 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 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, S6000, or the Z9000 at https://www.force10networks.com/CSPortal20/KnowledgeBase/Documentation.aspx. For more information about VLT, see Selecting a Layer 2 and Layer 3 with Resiliency (Routed 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 and Layer 3 with Resiliency (Routed 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 10 Gb or 40 Gb 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 and Layer 3 control planes across the two VLT peer switches. The VLT interconnect uses either 10 Gb or 40 Gb 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

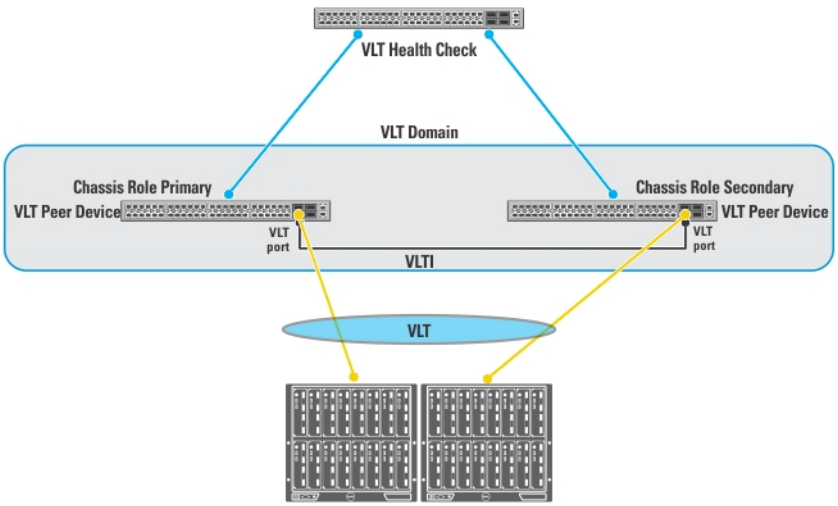
confused with failures of the VLT interconnect. VLT ensures that local traffic on a chassis does not traverse the VLTi and takes the shortest path to the destination via directly attached links.

VLT Fabric Terminology

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

- **Core** — A switch that connects to aggregation switches. The role of the core is to provide an interconnect to all the aggregation switches. All the ports on the core switch are used to connect the aggregation, various rack together.
- **Access** — A switch that connects switch, servers, storage devices, or top-of-rack (TOR) elements. The role of the access switch is to provide connectivity to the fabric. The access switch connects to all of aggregation switches above it in the fabric.
- **Aggregation** — A switch that connects to access switches. The role of the aggregation layer is to provide an interconnect to all the access switches. All the ports on the aggregation switches are used to connect the access, various racks together. The aggregation switch provides redundancy.
- **Edge ports** — The uplinks on the aggregation and downlinks on the access.
- **Uplinks** — An edge port link on the first two aggregation switches in the VLT fabric that connects to outside the fabric.
- **Downlinks** — An edge port link that connects the access switches to the access layer. For example, servers or ToR elements.
- **Fabric Interlinks (**Fabric Links**)** — The fabric interlink bandwidth is fixed: 10 Gb or 40 Gb.
  - For a 1-Tier, links that connect a pair of aggregation switches.
  - For a 2-Tier, links that connect the aggregation switches to the access switches.
  - For a 3-Tier, links that connect the core, aggregation, and access switches together.

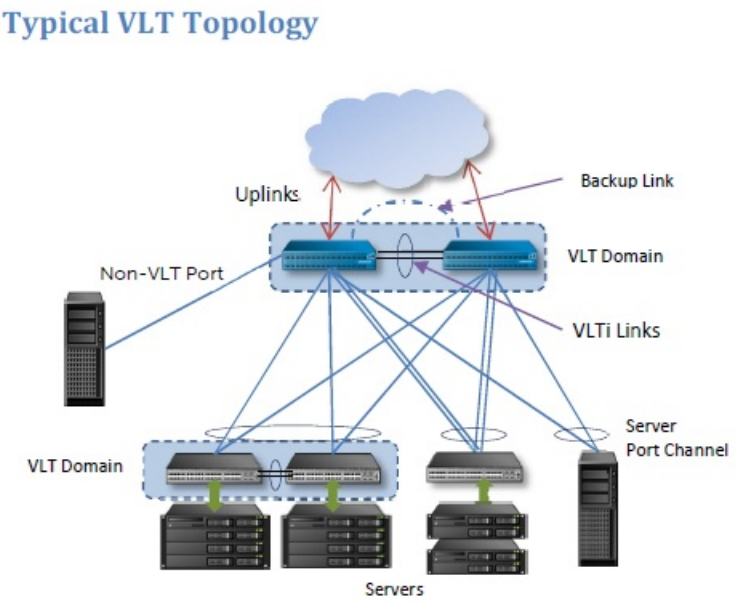
VLT Components



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 fabrics do not communicate with each other.
- For a VLT fabric, the AFM manages Dell Networking S4810, S4820T, S55, S60, S5000, S6000, Z9000, IOA blade 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 DHCP Integration and the *FTOS Configuration Guide* for the Dell Networking S4810, S4820T, S55, S60, S6000, Z9000, IOA blade and MXL blade switches at https://www.force10networks.com/CSPortal20/KnowledgeBase/Documentation.aspx.

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

- The number of current uplinks (minimum of 2) and downlinks for the access switches.
- The number of planned edge ports (future uplinks and downlinks) for the access switches.
- Whether the access switch needs to act as a switch or ToR.
- Fabric interlink bandwidth (the links between the aggregation and access switches).
- Downlinks which can be 1Gb, 10Gb, or 40 Gb.
- The fabric interlink bandwidth, 10 Gb or 40 Gb, is fixed and based on the fabric type.

NOTE: If you do not specify additional ports in the fabric design for future expansion in the **Bandwidth and Port Count** screen, you can only expand the downlinks on the existing 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. To specify a TFTP/FTP site, go to **Administration** > **Settings >TFTP/FTP** screen. For information about which software packages to use, see the Release Notes.
- Download the software image for each type of switch in the fabric. 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.
- 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 DHCP Integration.
- Obtain the pool of IP addresses for the management port for each switch in the fabric.
- Obtain IP addresses (must be an even number) for the uplink configuration from the ISP service. The uplink port number range is based on the whether a 10 Gb or 40 Gb bandwidth is selected.
  - For a 10 Gb bandwidth, AFM supports 2 to 32 uplinks.
  - For a 40 Gb bandwidth, AFM supports 2 to 8 uplinks.
- Obtain IP addresses or VLAN ID for the downlink configuration for connecting to the server or ToR.
- Gather protocol configuration for uplinks and downlinks.

Selecting a Layer 2 and Layer 3 with Resiliency (Routed VLT) Fabric Design

For workload migration over virtualized environments, use a Layer 2 VLT fabric design. To extend equal cost multi-pathing capabilities, use the Layer 3 with Resiliency (Routed VLT) fabric .

AFM supports the following Layer 2 VLT and Layer with 3 with Resiliency (Routed VLT) fabric designs:

- 1 and 2 Tier 10 Gb for Layer 2 LAN/SAN for iSCSI
- 1 and 2 Tier for 10 Gb Layer 2 LAN/SAN for Fibre Channel
- 1 Tier for 10 Gb and 40 Gb ToR for Layer 2 and Layer 3 Resiliency (Routed VLT)
- 2 Tier and 3 Tier Topologies for 1 Gb ToR VLT Deployment for Layer 2 and Layer 3 with Resiliency (Routed VLT)
- 10 Gb or 40 Gb Top of Rack Deployment (mVLT)
- 2 and 3 Tier 10 Gb ToR (mVLT) Deployment Topologies for Layer 2 or Layer 3 with Resiliency

- 10 Gb Blade Switch (MXL) for Layer 2 and Layer 3 with Resiliency (Routed VLT)

  For information about tiers, refer to Deployment Topology and Deployment Topology Use Cases.

For more information about VLT, refer to the following sections:

- Overview of VLT
- Key Core Design Considerations for VLT
- Getting Started.

1 and 2 Tier ToR 10 Gb for Layer 2 LAN/SAN for iSCSI Topologies

Table 2. 1 Tier ToR Layer LAN/SAN for iSCSI Topologies

						Possible Topologies	
DL BW	**UL BW**	**UL Port Range**	**iSCSI Port Range**	**DL Port Range**	**AVC**	**Aggregation**	**Access**
10G	10G	2 - 32	2 - 8	1 - 108	2 * 40G	S4810	NA
10G	40G	2 - 4	2 - 8	1 - 102	2 * 40G	S4810	NA

DL = Downlink

DL BW = Down Link Bandwidth

UL BW = Uplink Bandwidth

UL

AVC = Aggregation VLTi Capacity

Table 3. 2 Tier ToR Layer 2 LAN/SAN for iSCSI Topologies

						Possible Topologies	
Uplink Port Range	**iSCSI Port Range**	**Downlink Port Range**	**Aggregation VLTi Capacity**	**Access VLTi Capacity**	**FL BW AA**	**Aggregation**	**Access**
2 - 32	2 - 8	71 - 3410	2 * 40G	NA	20G	S4810	S4810
2 - 4	2 - 8	101 - 3224	2 * 40G	NA	20G	S4810	S4810
2 - 32	2 - 8	71 - 2916	2 * 40G	2 * 40G	20G	S4810	S4810
2 - 4	2 - 8	101 - 2808	2 * 40G	2 * 40G	20G	S4810	S4810
2 - 32	2 - 8	71 - 2970	2 * 40G	2 * 40G	20G	S4810	S4810

2 - 4	2 - 8	101 - 2808	2 * 40G	2 * 40G	20G	S4810	S4810

FL BW AA = Fabric Link Bandwidth between Aggregation & Access

Table 4. 2 Tier MXL for Layer 2 LAN/SAN for iSCSI Topologies

						Possible Topologies	
Uplink Port Range	**Uplink Bandwidth**	**Deployment Type**	**iSCSI Port Range**	**MXL Blade Pairs Range**	**FL BW AA**	**Aggregation**	**Access**
2 - 32	10G	Basic	2 - 8	2 - 27	20G	S4810	MXL
2 - 4	40G	Basic	2 - 8	2 - 26	20G	S4810	MXL
2 - 32	10G	Stacking	2 - 8	2- 27	40G	S4810	MXL
2 - 4	40G	Stacking	2 - 8	2 - 26	40G	S4810	MXL
2 - 32	10G	MXL - intraChassis resiliency	2 - 8	2 -27	20G	S4810	MXL
2 - 4	40G	MXL - intraChassis resiliency	2 - 8	2 - 26	20G	S4810	MXL

FL BW AA = Fabric Link Bandwidth between Aggregation & Access

1 and 2 Tier ToR 10 Gb for Layer 2 LAN/SAN for Fibre Channel Topologies

Table 5. One Tier LAN/SAN Layer 2 for Fibre Channel — 10 Gb Downlinks

Downlink Bandwidth	Uplink Bandwidth	Downlink Port Range	Aggregation VLTi Capacity	Possible Aggregation Topologies
10 Gb	10 Gb	1 - 86	2 * 40G	S5000
10 Gb	40 Gb	1 - 80	2 * 40G	S5000

Table 6. 2 Tier LAN/SAN Layer 2 for Fibre Channel — 10 Gb Downlinks

DL BW	UL BW	Deployment Type	Downlink Port Range	AVC	Access VLTi Capacity	FL BW AA	Possible Aggregation Topologies	
							Aggregation	Access
10 Gb	10G	Basic	87 - 2268	2 * 40G	NA	20G	S4810	S5000
10 Gb	40G	Basic	81 - 2184	2 * 40G	NA	20G	S4810	S5000

DL BW	UL BW	Deployment Type	Downlink Port Range	AVC	Access VLTi Capacity	FL BW AA	Possible Aggregation Topologies	
							Aggregation	Access
10 Gb	10G	Resiliency	87 - 2750	2 * 40G	2 * 40G	20G	S4810	S5000
10 Gb	40G	Resiliency	81 - 2600	2 * 40G	2 * 40G	20G	S4810	S5000

DL BW = Downlink Bandwidth

UL BW = Uplink Bandwidth

FL BW AA = Fabric Link Bandwidth between Aggregation & Access

1 Tier for 10 Gb and 40 Gb ToR for Layer 2 and Layer 3 Resiliency (Routed VLT)

Table 7. One Tier for 10 Gb and 40 Gb ToR for Layer 2 and Layer 3 Resiliency (Routed VLT)

DL BW	UL BW	Downlink Port Range	Aggregation VLTi Capacity	Possible Aggregation Topologies
10 Gb	10 Gb	1 - 110	2 * 40 Gb	S4810 or S4820T
10 Gb	40 Gb	1 - 104	2 * 40 Gb	S4810 or S4820T
40 Gb	10 Gb	1 - 59	2 * 40 Gb	Z9000 or S6000
40 Gb	40 Gb	1 - 58	2 * 40 Gb	Z9000 or S6000

DL = Downlink

DL BW = Downlink Bandwidth

UL BW = Uplink Bandwidth

Two Tier and Three Tier Topologies for 1 Gb ToR VLT Deployment for Layer 2 and Layer 3 with Resiliency (Routed VLT)

In a 1 Gb ToR VLT Deployment fabric design, the S4810 aggregation switches connect to access switches at 10 Gb. The maximum number of VLT aggregation is two switches and the maximum number of VLT access switches is based on the number of uplinks and downlinks in the fabric. With this topology, the downlinks connect to access S55 or S60 switches using a 1 Gb bandwidth.

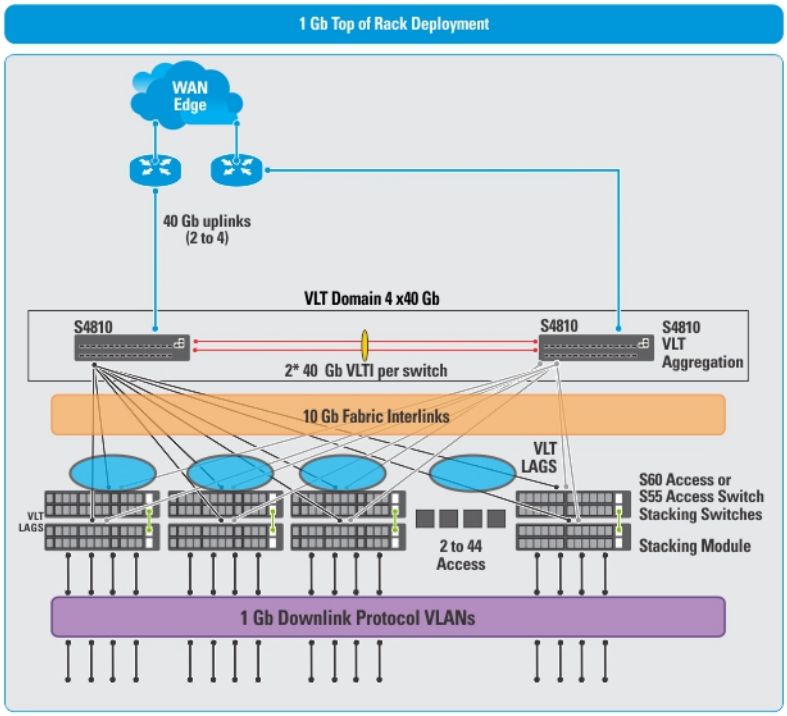


Figure 9. 1 Gb ToR VLT Deployment

Important: All the VLT aggregation switches must be same mode type for aggregation; for example, S4810. On the VLT access, you must configure the same model type.

AVG = Aggregation VLTi Capacity

DL = Downlink

DL BW = Down Link Bandwidth

FL BW AA = Fabric Link Bandwidth between Aggregation & Access

UL BW = Uplink Bandwidth

BW = Bandwidth

Use the following table as guideline to select the appropriate two tier Layer 2 VLT or Layer 3 with Resiliency (Routed VLT) fabric design for a 1 Gb ToR VLT deployment.

NOTE: With a Layer 2 VLT fabric, the uplinks come from the first two switches on the aggregation side. For information about tiers, see Deployment Topology.

Table 8. Two Tier (1 Gb Downlinks)

DL BW	ULBW	Type	DL Port Range	AVG	Access VLTi Capacity	FL BW A & A	Possible Topologies	
							Aggregation	Access
1 Gb	10 Gb	Stacking	1 - 2640	2 * 40 Gb	NA	40 Gb	S4810	S60 (12G or 24G)
1 Gb	10 Gb	Stacking	1 - 2640	2 * 40 Gb	NA	40 Gb	S4810	S55 (12G)
1 Gb	40 Gb	Stacking	1 - 2496	2 * 40 Gb	NA	40 Gb	S4810	S60 (12G or 24G)
1 Gb	40 Gb	Stacking	1 - 2496	2 * 40 Gb	NA	40 Gb	S4810	S55 (12G)
1 Gb	10 Gb	Basic	1 - 2640	2 * 40 Gb	NA	20 Gb	S4810	S60
1 Gb	10 Gb	Basic	1 - 2640	2 * 40 Gb	NA	20 Gb	S4810	S55
1 Gb	40 Gb	Basic	1 - 2496	2 * 40 Gb	NA	20 Gb	S4810	S60
1 Gb	40 Gb	Basic	1 - 2496	2 * 40 Gb	NA	20 Gb	S4810	S55

Use the following table as guideline to select the appropriate three tier Layer 2 VLT or Layer 3 with Additional Resiliency (Routed VLT) fabric design for a 1 Gb ToR VLT deployment.

AVG = Aggregation VLTi Capacity

AVC = Access VLTi Capacity

CVG = Core VLTi Capacity

DL = Downlink

DL BW = Downlink Bandwidth

FL BW C A = Fabric Link Bandwidth between Core & Aggregation

FL BW AA = Fabric Link Bandwidth between Aggregation & Access

FL BW = Fabric Link Bandwidth

UL BW = Uplink Bandwidth

BW = Bandwidth

Table 9. Three Tier ToR (1 Gb Downlinks) for Layer 2 and Layer 3 with Resiliency (Routed VLT)

DL BW	UL BW	Type	DL Port Range	CVG	AVG	AVC	FL BW CA	FL BW AA	Possible Topologies		
									Core	Aggregation	Access
1 Gb	10 Gb	Stacking	2641 - 32256	2 * 40 Gb	2 * 40 Gb	NA	80G	40 Gb	Z9000 or S6000	S4810	S55 (12G)
1 Gb	10 Gb	Stacking	2641 - 32256	2 * 40 Gb	2 * 40 Gb	NA	80G	40 Gb	Z9000 or S6000	S4810	S60 (12G or 24G)
1 Gb	40 Gb	Stacking	2497 - 32256	2 * 40 Gb	2 * 40 Gb	NA	80G	40 Gb	Z9000 or S6000	S4810	S55 (12G)
1 Gb	40 Gb	Stacking	2497 - 32256	2 * 40 Gb	2 * 40 Gb	NA	80G	40 Gb	Z9000 or S6000	S4810	S60 (12G or 24G)
1 Gb	10 Gb	Basic	2641 - 32256	2 * 40 Gb	2 * 40 Gb	NA	80G	20 Gb	Z9000 or S6000	S4810	S60
1 Gb	10 Gb	Basic	2641 - 32256	2 * 40 Gb	2 * 40 Gb	NA	80G	20 Gb	Z9000 or S6000	S4810	S55
1 Gb	40 Gb	Basic	2497 - 32256	2 * 40 Gb	2 * 40 Gb	NA	80G	20 Gb	Z9000 or S6000	S4810	S60
1 Gb	40 Gb	Basic	2497 - 32256	2 * 40 Gb	2 * 40 Gb	NA	80G	20 Gb	Z9000 or S6000	S4810	S55

10 Gb or 40 Gb ToR (mVLT)

Use the 10 Gb or 40 Gb ToR Deployment (mVLT) fabric when you require 10 Gb or 40 Gb downlinks for a ToR. For information about mVLT, refer to Multi-domain VLT. Refer to the MXL Topologies for MXL Blade Deployment.

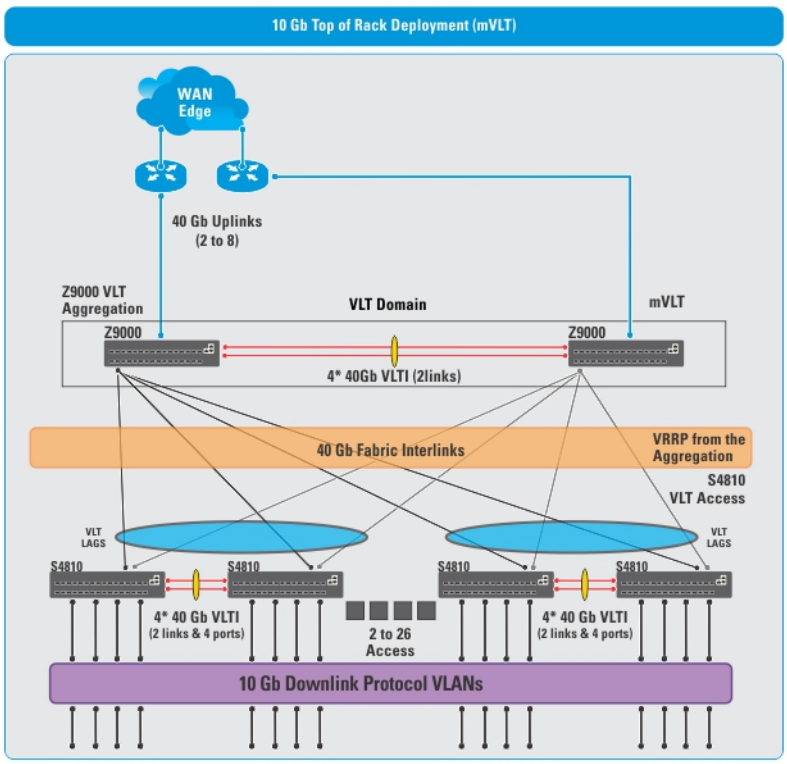


Figure 10. 10 Gb or 40 Gb ToR VLT Deployment (mVLT)

Important:

All the VLT aggregation switches must be same model for aggregation (for example, all Z9000 switches). On the VLT access, you can configure the same model or mixed the following models : S4810 and S4820T.

Two and Three Tier 10 Gb ToR (mVLT) Deployment Topologies for Layer 2 or Layer 3 with Resiliency

AVC = Aggregation VLTi Capacity

DL = Downlink

DL BW = Down Link Bandwidth

FL BWB A & A = Fabric Link Bandwidth between Aggregation & Access

UL BW = Uplink Bandwidth

Use the following tables as guideline to select the appropriate two tier Layer 2 VLT or Layer 3 with Resiliency (Routed VLT) fabric design.

NOTE: With a Layer 2 VLT fabric, the uplinks come from the first two switches on the aggregation side. For information about tiers, see Deployment Topology.

Table 10. 2 Tier ToR (mVLT) — 10 G Downlinks

DL BW	UL BW	Type	DL Port Range	AVC	Access VLTi Capacity	FL BWB A & A	Possible Topologies		
							Core	Aggregation	Access
10 Gb	10 Gb	Mixed node Stacking	111 - 2970	2 * 40 Gb	NA	40 Gb	NA	S4810	S4810 or S4820T
10 Gb	10 Gb	Mixed node Stacking	111 - 1392	2 * 40 Gb	NA	160 Gb	NA	Z9000 or S6000	S4810 or S4820T
10 Gb	10 Gb	Stacking	111 - 2970	2 * 40 Gb	NA	40 Gb	NA	S4810	S4810
10 Gb	10 Gb	Stacking	111 - 1392	2 * 40 Gb	NA	160 Gb	NA	Z9000 or S6000	S4810
10 Gb	10 Gb	Basic	111 - 3410	2 * 40 Gb	NA	20 Gb	NA	S4810	S4810
10 Gb	10 Gb	Basic	111 - 1624	2 * 40 Gb	NA	80 Gb	NA	Z9000 or S6000	S4810
10 Gb	10 Gb	Mixed node Basic	111 - 3410	2 * 40 Gb	NA	20 Gb	NA	S4810	S4810 or S4820T
10 Gb	10 Gb	Mixed node Basic	111 - 1624	2 * 40 Gb	NA	80 Gb	NA	Z9000 or S6000	S4810 or S4820T
10 Gb	10 Gb	Resiliency	111 - 2916	2 * 40 Gb	2 * 40 Gb	20 Gb	NA	S4810	S4810
10 Gb	10 Gb	Resiliency	111 - 1344	2 * 40 Gb	2 * 40 Gb	80 Gb	NA	Z9000 or S6000	S4810
10 Gb	10 Gb	Mixed node Resiliency	111 - 2916	2 * 40 Gb	2 * 40 Gb	20 Gb	NA	S4810	S4810 or S4820T
10 Gb	10 Gb	Mixed node Resiliency	111 - 1344	2 * 40 Gb	2 * 40 Gb	80 Gb	NA	Z9000 or S6000	S4810 or S4820T
10 Gb	40 Gb	Mixed node Stacking	105 - 2808	2 * 40 Gb	NA	40 Gb	NA	S4810	S4810 or S4820T
10 Gb	40 Gb	Mixed node Stacking	105 - 1392	2 * 40 Gb	NA	160 Gb	NA	Z9000 or S6000	S4810 or S4820T

DL BW	UL BW	Type	DL Port Range	AVC	Access VLTi Capacity	FL BWB A & A	Possible Topologies		
							Core	Aggregation	Access
10 Gb	40 Gb	Stacking	105 - 2808	2 * 40 Gb	NA	40 Gb	NA	S4810	S4810
10 Gb	40 Gb	Stacking	105 - 1392	2 * 40 Gb	NA	160 Gb	NA	Z9000 or S6000	S4810
10 Gb	40 Gb	Basic	105 - 3224	2 * 40 Gb	NA	20 Gb	NA	S4810	S4810
10 Gb	40 Gb	Basic	105 - 1624	2 * 40 Gb	NA	80G	NA	Z9000 or S6000	S4810
10 Gb	40 Gb	Mixed node Basic	105 - 3224	2 * 40 Gb	NA	20 Gb	NA	S4810	S4810 or S4820T
10 Gb	40 Gb	Mixed node Basic	105 - 1624	2 * 40 Gb	NA	80G	NA	Z9000 or S6000	S4810 or S4820T
10 Gb	40 Gb	Resiliency	105 - 2808	2 * 40 Gb	2 * 40 Gb	20 Gb	NA	S4810	S4810
10 Gb	40 Gb	Resiliency	105 - 1344	2 * 40 Gb	2 * 40 Gb	80G	NA	Z9000 or S6000	S4810
10 Gb	40 Gb	Mixed node Resiliency	105 - 2808	2 * 40 Gb	2 * 40 Gb	20 Gb	NA	S4810	S4810 or S4820T
10 Gb	40 Gb	Mixed node Resiliency	105 - 1344	2 * 40 Gb	2 * 40 Gb	80G	NA	Z9000 or S6000	S4810 or S4820T

AVC = Aggregation VLTi Capacity

BW = Bandwidth

DL = Downlink

DL BW = Downlink Bandwidth

FL BW AA = Fabric Link Bandwidth between Aggregation & Access

UL BW = Uplink Bandwidth

Use the following tables as guideline to select the appropriate two tier Layer 2 VLT or Layer 3 with Resiliency (Routed VLT) fabric design for a 40 Gb ToR (mVLT deployment).

NOTE: With a Layer 2 VLT fabric, the uplinks come from the switches on the aggregation side. For information about tiers, refer to Deployment Topology.

Table 11. Two Tier ToR (mVLT) — 40 G Downlinks for Layer 2 or Layer 3 with Resiliency (Routed VLT)

DL BW	UL BW	Type	DL Port Range	AVC	Access VLTi Capacity	FL BW AA	Possible Topologies	
							Aggregation	Access
40 Gb	10 Gb	Basic	60 - 870	2 * 40 Gb	NA	80 Gb	Z9000	Z9000
40 Gb	10 Gb	Basic	60 - 870	2 * 40 Gb	NA	80 Gb	S6000	S6000
40 Gb	10 Gb	Resiliency	60 - 784	2 *40 Gb	2 * 40 Gb	80 Gb	Z9000	Z9000
40 Gb	10 Gb	Resiliency	60 - 784	2 * 40 Gb	2 * 40 Gb	80 Gb	S6000	S6000
40 Gb	40 Gb	Basic	59 - 870	2 * 40 Gb	NA	80 Gb	Z9000	Z9000
40 Gb	40 Gb	Basic	59 - 870	2 * 40 Gb	NA	80 Gb	S6000	S6000
40 Gb	40 Gb	Resiliency	59 - 784	2 *40 Gb	2 * 40 Gb	80 Gb	Z9000	Z9000
40 Gb	40 Gb	Resiliency	59 - 784	2 *40 Gb	2 * 40 Gb	80 Gb	S6000	S6000

Three Tier Topologies for a 10 Gb or 40 Gb ToR (mVLT) Deployment Layer 2 or Layer 3 with Resiliency (Routed VLT)

Use the following tables as guideline to select the appropriate three tier Layer 2 VLT or Layer 3 with Resiliency (Routed VLT) fabric design for a 40 Gb Tor (mVLT) Deployment.

NOTE: With a Layer 2 VLT fabric, the uplinks come from the switches on the aggregation side. For information about tiers, refer to Deployment Topology.

AVC = Aggregation VLTi Capacity

CVC = Core VLTi Capacity

BW = Bandwidth

DL = Downlink

DL BW = Downlink Bandwidth

FL BW CA = Fabric Link Bandwidth between Core & Aggregation

FL BW AA = Fabric Link Bandwidth between Aggregation & Access

UL BW = Uplink Bandwidth

Table 12. 3 Tier ToR (mVLT) — 10 Gb Downlinks

DL BW	UL BW	Type	DL Port Range	CVC	AVC	AVC	FL BW CA	FL BW AA	Possible Topologies		
									Core	Aggregation	Access
10 Gb	10 Gb	Stacking	2971 - 36288	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	40 Gb	Z9000 or S6000	S4810	S4810
10 Gb	10 Gb	Stacking	2971 - 36288	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	40 Gb	Z9000 or S6000	S4810	S4820
10 Gb	10 Gb	Stacking	2971 - 18816	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	160 Gb	Z9000 or S6000	Z9000 or S6000	S4810
10 Gb	10 Gb	Stacking	2971 - 18816	2 *40 Gb	2 *40 Gb	NA	80 Gb	160 Gb	Z9000 or S6000	Z9000 or S6000	S4820
10 Gb	10 Gb	Basic	3411 - 41664	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	20 Gb	Z9000 or S6000	S4810	S4810
10 Gb	10 Gb	Basic	3411 - 41664	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	20 Gb	Z9000 or S6000	S4810	S4820
10 Gb	10 Gb	Basic	1625 - 21952	2 *40 Gb	2 *40 Gb	NA	80 Gb	80 Gb	Z9000 or S6000	Z9000 or S6000	S4810
10 Gb	10 Gb	Basic	1625 - 21952	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	80 Gb	Z9000 or S6000	Z9000 or S6000	S4820
10 Gb	10 Gb	Resiliency	2917 - 36288	2 * 40 Gb	2 * 40 Gb	2 * 40 Gb	80 Gb	20 Gb	Z9000 or S6000	S4810	S4810
10 Gb	10 Gb	Resiliency	2917 - 36288	2 * 40 Gb	2 * 40 Gb	2 * 40 Gb	80 Gb	20 Gb	Z9000 or S6000	S4810	S4820
10 Gb	10 Gb	Resiliency	1355 - 18816	2 *40 Gb	2 *40 Gb	2 * 40 Gb	80 Gb	80 Gb	Z9000 or S6000	Z9000 or S6000	S4810
10 Gb	10 Gb	Resiliency	1355 - 18816	2 * 40 Gb	2 * 40 Gb	2 * 40 Gb	80 Gb	80 Gb	Z9000 or S6000	Z9000 or S6000	S4820

DL BW	UL BW	Type	DL Port Range	CVC	AVC	AVC	FL BW CA	FL BW AA	Possible Topologies		
									Core	Aggregation	Access
10 Gb	40 Gb	Stacking	2809 - 36288	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	40 Gb	Z9000 or S6000	S4810	S4810
10 Gb	40 Gb	Stacking	2809 - 36288	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	40 Gb	Z9000 or S6000	S4810	S4820
10 Gb	40 Gb	Stacking	1393 - 18816	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	160 Gb	Z9000 or S6000	Z9000 or S6000	S4810
10 Gb	40 Gb	Stacking	1393 - 18816	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	160 Gb	Z9000 or S6000	Z9000 or S6000	S4820
10 Gb	40 Gb	Basic	3225 - 41664	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	20 Gb	Z9000 or S6000	S4810	S4810
10 Gb	40 Gb	Basic	3225 - 41664	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	20 Gb	Z9000 or S6000	S4810	S4820
10 Gb	40 Gb	Basic	1225 - 21952	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	80 Gb	Z9000 or S6000	Z9000 or S6000	S4810
10 Gb	40 Gb	Basic	1225 - 21952	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	80 Gb	Z9000 or S6000	Z9000 or S6000	S4820
10 Gb	40 Gb	Resiliency	2809 - 36288	2 * 40 Gb	2 * 40 Gb	2 * 40 Gb	80 Gb	20 Gb	Z9000 or S6000	S4810	S4810
10 Gb	40 Gb	Resiliency	2809 - 36288	2 * 40 Gb	2 * 40 Gb	2 * 40 Gb	80 Gb	20 Gb	Z9000 or S6000	S4810	S4820
10 Gb	40 Gb	Resiliency	1345 - 18816	2 * 40 Gb	2 * 40 Gb	2 * 40 Gb	80 Gb	80 Gb	Z9000 or S6000	Z9000 or S6000	S4810
10 Gb	40 Gb	Resiliency	1345 - 18816	2 * 40 Gb	2 * 40 Gb	2 * 40 Gb	80 Gb	80 Gb	Z9000 or S6000	Z9000 or S6000	S4820

AVC = Aggregation VLTi Capacity

CVC = Core VLTi Capacity

BW = Bandwidth

DL = Downlink

DL BW = Downlink Bandwidth

FL BWB C & A = Fabric Link Bandwidth between Core and Aggregation Switches

FL BWB A & A = Fabric Link Bandwidth between Aggregation and Access Switches

UL BW = Uplink Bandwidth

Table 13. Three Tier ToR (mVLT) — 40 Gb Downlinks

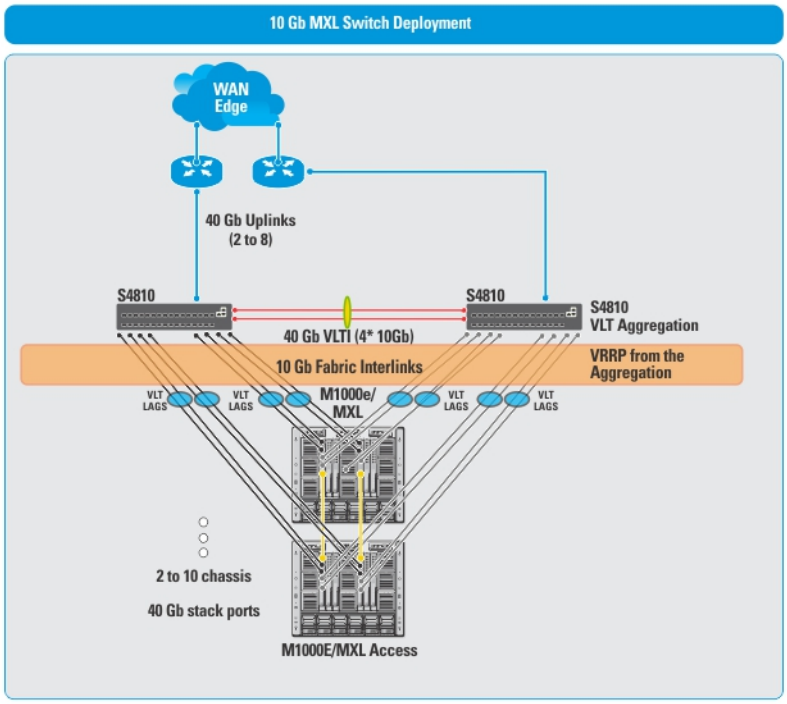
DL BW	UL BW	Type	DL Port Range	CVC	AVC	Access VLTi Capacity	FL BWB C & A	FL BWB A & A	Possible Topologies		
									Core	Aggregation	Access
40 Gb	10 Gb	Basic	871 - 11760	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	80 Gb	Z9000	Z9000	Z9000
40 Gb	10 Gb	Basic	871 - 11760	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	80 Gb	S6000	S6000	S6000
40 Gb	10 Gb	Resiliency	785 - 10976	2 * 40 Gb	2 * 40 Gb	2 * 40 Gb	80 Gb	80 Gb	Z9000	Z9000	Z9000
40 Gb	10 Gb	Resiliency	785 - 10976	2 * 40 Gb	2 * 40 Gb	2 * 40 Gb	80 Gb	80 Gb	S6000	S6000	S6000
40 Gb	40 Gb	Basic	871 - 11760	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	80 Gb	Z9000	Z9000	Z9000
40 Gb	40 Gb	Basic	871 - 11760	2 * 40 Gb	2 * 40 Gb	NA	80 Gb	80 Gb	S6000	S6000	S6000

Two and Three Tier MXL Blade Topologies for Layer 2 and Layer 3 with Resiliency (Routed VLT)

You can create a fabric using MXL blades by selecting the **MXL blade** option and **10 Gb** downlinks. For information about MXL fabric deployments, refer MXL Topologies for MXL Blade Deployment..

NOTE: All the VLT aggregation switches must be same model (for example, all S4810 switches). On the VLT access, all the switches must be MXL blades. Refer to the previous tables in this section for more information.

10 Gb Blade Switch (MXL) VLT Deployment



BW = Bandwidth

DL = Downlink

FL BWB A & A = Fabric Link Bandwidth between Aggregation and Access

UL BW = Uplink Bandwidth

VLTi A BW = VLTi Aggregation Bandwidth

Table 14. MXL Blade Two Tier Topologies for 10 GB MXL Blade Switch For Layer 2 and Layer 3 with Resiliency (Routed VLT)

MXL Blade Pairs Range	UL BW	Type	Fabric Type	FL BWBA & A	VLTi A BW	VLTi Access BW	MXL Inter-chassis BW	Possible Topologies	
								Aggregation	Access
2 - 27	10 Gb	Basic	Layer 2/ Layer 3 with Resiliency	20 Gb	2 * 40 Gb	NA	NA	S4810 or S4820T	MXL

MXL Blade Pairs Range	UL BW	Type	Fabric Type	FL BWBA & A	VLTi A BW	VLTi Access BW	MXL Inter-chassis BW	Possible Topologies	
								Aggregation	Access
			(Routed VLT)						
2 - 14	10 Gb	Basic	Layer 2/ Layer 3 with Resiliency (Routed VLT)	80 Gb	2 * 40 Gb	NA	NA	Z9000 or S6000	MXL
2 - 14	40 Gb	Basic	Layer 2/ Layer 3 with Resiliency (Routed VLT)	80 Gb	2 * 40 Gb	NA	NA	Z9000 or S6000	MXL
2 - 26	40 Gb	Basic	Layer 2/ Layer 3 with Resiliency (Routed VLT)	20 Gb	2 * 40 Gb	NA	NA	S4810 or S4820T	MXL
2- 27	10 Gb	Stacking	Layer 2/ Layer 3 with Resiliency (Routed VLT)	40 Gb	2 * 40 Gb	NA	NA	S4810 or S4820T	MXL
2 - 14	10 Gb	Stacking	Layer 2/ Layer 3 with Resiliency (Routed VLT)	160G	2 * 40 Gb	NA	NA	Z9000 or S6000	MXL
2 - 14	40 Gb	Stacking	Layer 2/ Layer 3 with Resiliency (Routed VLT)	160G	2 * 40 Gb	NA	NA	Z9000/ S6000	MXL
2 - 26	40 Gb	Stacking	Layer 2/ Layer 3 with Resiliency (Routed VLT)	40 Gb	2 * 40 Gb	NA	NA	S4810 or S4820T	MXL

MXL Blade Pairs Range	UL BW	Type	Fabric Type	FL BWBA & A	VLTi A BW	VLTi Access BW	MXL Inter-chassis BW	Possible Topologies	
								Aggregation	Access
2 -27	10 Gb	MXL - intra-Chassis resiliency	Layer 2/ Layer 3 with Resiliency (Routed VLT)	20 Gb	2 * 40 Gb	2 * 40 Gb	NA	S4810 or S4820T	MXL
2 - 14	10 Gb	MXL - intra-Chassis resiliency	Layer 2/ Layer 3 with Resiliency (Routed VLT)	80 Gb	2 * 40 Gb	2 * 40 Gb	NA	Z9000/ S6000	MXL
2 - 14	40 Gb	MXL - intra-Chassis resiliency	Layer 2/ Layer 3 with Resiliency (Routed VLT)	80 Gb	2 * 40 Gb	2 * 40 Gb	NA	Z9000/ S6000	MXL
2 - 26	40 Gb	MXL - intra-Chassis resiliency	Layer 2/ Layer 3 with Resiliency (Routed VLT)	20 Gb	2 * 40 Gb	2 * 40 Gb	NA	S4810 or S4820T	MXL
2 - 30 (for all even numbers only)	10 Gb	MXL - inter-Chassis resiliency	Layer 3 with Resiliency (Routed VLT)	20 Gb	2 * 40 Gb	2 * 40 Gb	40 Gb	S4810 or S4820T	MXL
2 - 14 (for all even numbers only)	10 Gb	MXL - inter-Chassis resiliency	Layer 3 with Resiliency (Routed VLT)	80 Gb	2 * 40 Gb	2 * 40 Gb	40 Gb	Z9000 or S6000	MXL
2 - 30 (for all even numbers only)	40 Gb	MXL - inter-Chassis resiliency	Layer 3 with Resiliency (Routed VLT)	20 Gb	2 * 40 Gb	2 * 40 Gb	40 Gb	S4810 or S4820T	MXL

BW = Bandwidth

DL = Downlink

FL BWB A & A = Fabric Link Bandwidth between Aggregation and Access

FL BWB C & A = Fabric Link Bandwidth between Core and Access

UL BW = Uplink Bandwidth

VCBW = VLTi Core Bandwidth

Table 15. Three Tier Deployment Topologies for MXL Blade Switch for Layer 2 and Layer 3 with Resiliency (Routed VLT)

MXL Blade Pairs Range	UL BW	Type	Fabric Type	FL BWB C & A	FL BWB A & A	VCBW	VLTi Aggregat-ion BW	Possible Topologies		
								Core	Aggregation	Access
28 - 336	10 Gb	Basic	Layer 2 or Layer 3 with Resiliency (Routed VLT)	80G	20 Gb	2 * 40 Gb	2 * 40 Gb	Z9000 or S6000	S4810 or S4820T	MXL
28 - 336	40 Gb	Basic	Layer 2 or Layer 3 with Resiliency (Routed VLT)	80G	20 Gb	2 * 40 Gb	2 * 40 Gb	Z9000 or S6000	S4810 or S4820T	MXL
15 - 196	10 Gb	Basic	Layer 2 or Layer 3 with Resiliency (Routed VLT)	80G	80G	2 * 40 Gb	2 * 40 Gb	Z9000	Z9000	MXL
15 - 196	10 Gb	Basic	Layer 2 or Layer 3 with Resiliency (Routed VLT)	80G	80G	2 * 40 Gb	2 * 40 Gb	S6000	S6000	MXL
15 - 196	40 Gb	Basic	Layer 2 or Layer 3 with Resiliency (Routed VLT)	80G	80G	2 * 40 Gb	2 * 40 Gb	Z9000	Z9000	MXL
15 - 196	40 Gb	Basic	Layer 2/ Layer 3 with Resiliency (Routed VLT)	80G	80G	2 * 40 Gb	2 * 40 Gb	S6000	S6000	MXL

MXL Blade Pairs Range	UL BW	Type	Fabric Type	FL BWB C & A	FL BWB A & A	VCBW	VLTi Aggreg at-ion BW	Possible Topologies		
								Core	Aggregation	Access
28 - 336	10 Gb	Stack-ing	Layer 2 or Layer 3 with Resiliency (Routed VLT)	80G	40 Gb	2 * 40 Gb	2 * 40 Gb	Z9000 or S6000	S4810 or S4820T	MXL
28 - 336	40 Gb	Stack-ing	Layer 2/ Layer 3 with Resiliency (Routed VLT)	80G	40 Gb	2 * 40 Gb	2 * 40 Gb	Z9000 or S6000	S4810 or S4820T	MXL
15 - 196	10 Gb	Stack-ing	Layer 2 or Layer 3 with Resiliency (Routed VLT)	80G	160G	2 * 40 Gb	2 * 40 Gb	Z9000	Z9000	MXL
15 - 196	10 Gb	Stack-ing	Layer 2/ Layer 3 with Resiliency (Routed VLT)	80G	160G	2 * 40 Gb	2 * 40 Gb	S6000	S6000	MXL
15 - 196	40 Gb	Stack-ing	Layer 2/ Layer 3 with Resiliency (Routed VLT)	80G	160G	2 * 40 Gb	2 * 40 Gb	Z9000	Z9000	MXL
15 - 196	40 Gb	Stack-ing	Layer 2/ Layer 3 with Resiliency (Routed VLT)	80G	160G	2 * 40 Gb	2 * 40 Gb	S6000	S6000	MXL
28 - 336	10 Gb	MXL - intra-Chassis resilienc y	Layer 2 or Layer 3 with Resiliency (Routed VLT)	80G	20 Gb	2 * 40 Gb	2 * 40 Gb	Z9000 or S6000	S4810 or S4820T	MXL
27 - 336	40 Gb	MXL - intra-Chassis	Layer 2 or Layer 3 with	80G	20 Gb	2 * 40 Gb	2 * 40 Gb	Z9000 or	S4810 or S4820T	MXL

MXL Blade Pairs Range	UL BW	Type	Fabric Type	FL BWB C & A	FL BWB A & A	VCBW	VLTi Aggreg at-ion BW	Possible Topologies		
								Core	Aggregation	Access
		resilienc y	Resiliency (Routed VLT)					S6000		
15 - 196	10 Gb	MXL - intra-Chassis resilienc y	Layer 2 or Layer 3 with Resiliency (Routed VLT)	80G	80G	2 * 40 Gb	2 * 40 Gb	Z9000	Z9000	MXL
15 - 196	10 Gb	MXL - intra-Chassis resilienc y	Layer 2 or Layer 3 with Resiliency (Routed VLT)	80G	80G	2 * 40 Gb	2 * 40 Gb	S6000	S6000	MXL
15 - 196	40 Gb	MXL - intra-Chassis resilienc y	Layer 2 or Layer 3 with Resiliency (Routed VLT)	80G	80G	2 * 40 Gb	2 * 40 Gb	Z9000	Z9000	MXL
15 - 196	40 Gb	MXL - intra-Chassis resilienc y	Layer 2 or Layer 3 with Resiliency (Routed VLT)	80G	80G	2 * 40 Gb	2 * 40 Gb	S6000	S6000	MXL

6

Discovering and Deploying an Existing Fabric

Use the **discover fabric** option to discover an existing fabric or an IOA blade switch in a M1000e chassis. For information about IOA, see Designing an IOA Fabric.

To discover and deploy an existing fabric:

Figure 11. Discovering and Deploying an Existing Fabric

1. Initiate discovery of an existing fabric at the **Network** > **Design** > **Discover Fabric** screen. See Step 1: Discover an Existing Fabric
2. Check the status of the discovered fabric at the **Network** > **Design Fabric** > **Discover Status** screen. See Step 2: View Discovery Status screen.
3. Deploy the successfully discovered fabric at the **Network** >**Design Fabric** screen. See Step 3: Deploy Discovered Fabric.

   NOTE: Once the discovered fabric is successfully deployed, the fabric can send alarms and events to AFM.

4. Perform maintenance operations, such as monitoring and software updates. See Maintenance and Performance Management.

Step 1: Discover an Existing Fabric

This section describes how to discover an existing fabric. For an overview about discovering and deploying an existing fabric, see Discovering and Deploying an Existing Fabric.

To discover an existing fabric:

1. Click on the **Network** and then the **Design Fabric** tab.
   The **Network Deployment Summary** screen displays.
2. Click **Discover Fabric**.
   The **Discover Fabric** wizard **Introduction** screen displays.
3. Read the introduction and click the **Next** button.
   The **Fabric Name and Type** screen displays.

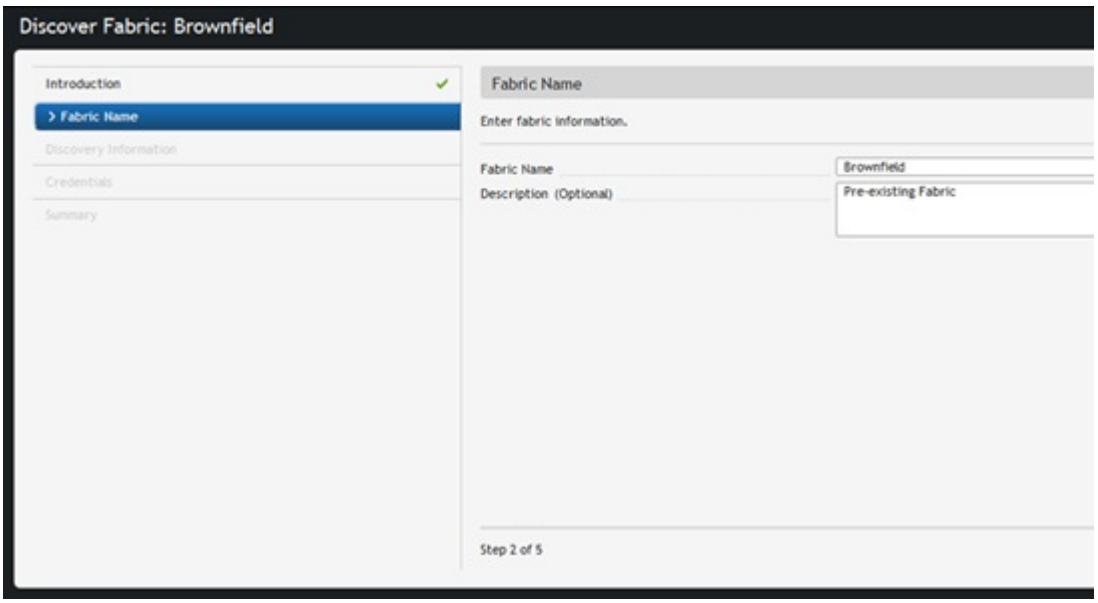


Figure 12. Discover Fabric Wizard — Fabric Name Screen

4. Enter the fabric name in the **Fabric Name** field.

   NOTE: The fabric name must be unique.
5. (Optional) Enter a description for the fabric in the **Description** field.

6. Click the **Next** button.

   The **Discovery Information** screen displays.

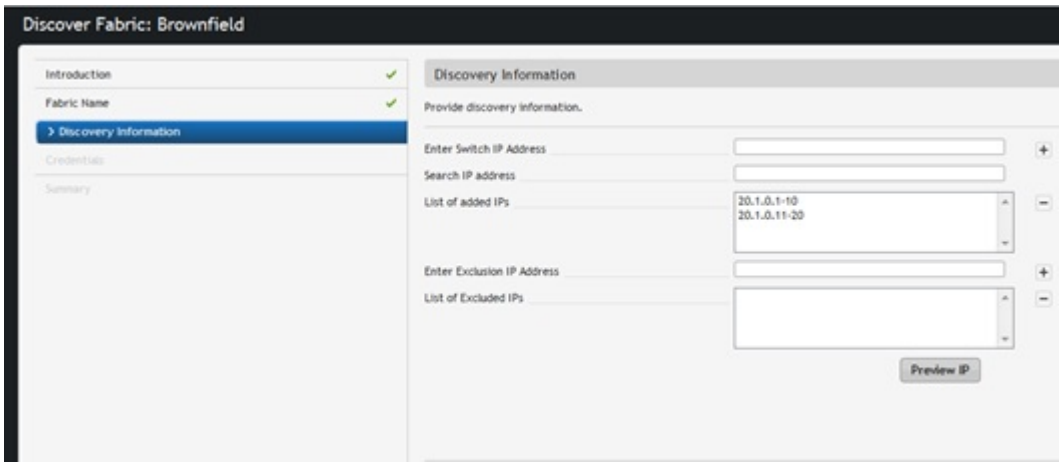


Figure 13. Discover Fabric Wizard — Discovery Information Screen

7. Enter the switch IP address in the **Enter the Switch IP Address** field and click the **+** button to add the IP address.

   NOTE: You can add an individual IP address, and IP address with a subnet, or a range. You must add at least one IP address to the **List of added IPs:** field before clicking **Next**.

   - **IP range example**

     10.16.133.1-150

   - **Network with mask example**

     10.16.132.0/24. Netmasks < 24 are not allowed.

8. (Optional) To search for a previously entered IP address, enter a portion of or the entire IP address in the **Search IP address list:** field.

   The software displays all IP addresses that match the search term in the **List of added IPs** field. If you do not enter a search term, all known IP addresses are displayed.

9. To remove an IP address from the displayed list, select the IP address and click the - button.

10. To exclude an IP address, enter it in the **Enter Exclusion IP Address** field.

Figure 14. Preview IP Address Window

11. To view a list of all IP addresses to be added, click the **Preview IP** button.
    The **Preview IP** screen displays only the inclusion list of devices: the devices that are participating in the discovery. The **Preview IP List** is paginated. Use the arrow buttons to view additional pages or enter the page number in the page number entry field to the left of the arrow buttons.
12. Click the **Next** button.
    The **Credentials** screen displays.

13. In the **SNMP** section, click the **Add** link.

    The **SNMP Credential** window displays.

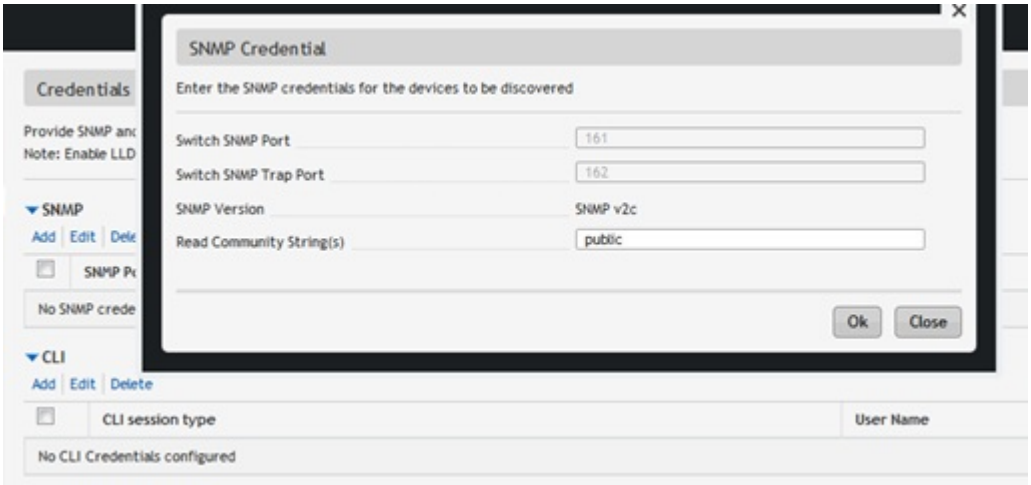


Figure 15. Discover Fabric SNMP Credential Screen

14. Enter the SNMP credential information and click **OK** to confirm the information or click **Close** to close the window. By default, the SNMP port number is 161 and the trap port number is 162. The maximum number of SNMP credentials is 5.
    - Enter the read community string in the **Read Community String(s)** field. You can only enter one read community string.

      NOTE: You must enter the read community string to add the SNMP credential information.

NOTE:

- To delete SNMP credentials, check the checkbox for the credentials you want to delete and click **Delete** in the SNMP section. There is no confirmation message before the credentials are deleted.
- To edit SNMP credentials, check the checkbox for the credentials you want to edit and click **Edit** in the SNMP section. Click the **OK** button to save changes or click **Close** to close the window.

15. Click **Add** in the **CLI Credentials** section.

    The **CLI Credential** window displays.

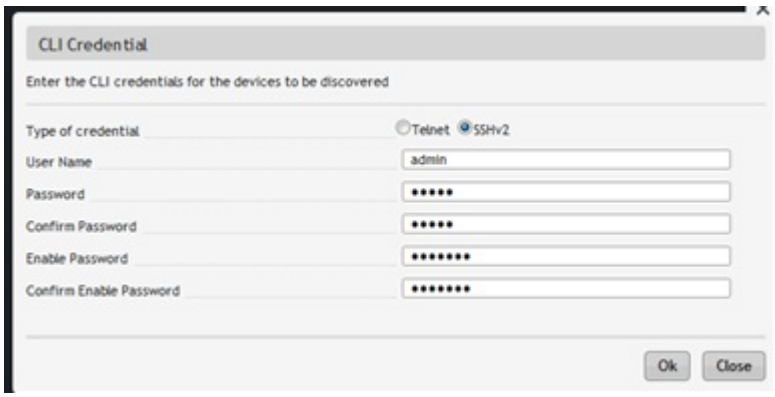


Figure 16. Discover Fabric CLI Credential Screen

NOTE: You can configure up to five CLI credentials for a single fabric and can be a combination of credential types (SSHv2 and Telnet).

16. Enter the CLI credential information.
    - Select the appropriate credential type (Telnet or SSHv2).
    - Enter the user name in the **User Name** field and enter the password in the **Password** and **Confirm Password** fields.
    - If you configured an enable password, enter it in the **Enable Password** and **Confirm Enable Password** fields.
    - Click **OK** to confirm the information or click **Close** to close the window.

NOTE:

- To delete CLI credentials, check the checkbox for the credentials you want to delete and click **Delete** in the CLI section. There is no confirmation message before the credentials are deleted.
- To edit CLI credentials, check the checkbox for the credentials you want to edit and click **Edit** in the CLI section. Click **Ok** to save changes or click **Close** to close the window.

17. Click the **Next** button.

    The **Summary** screen displays.

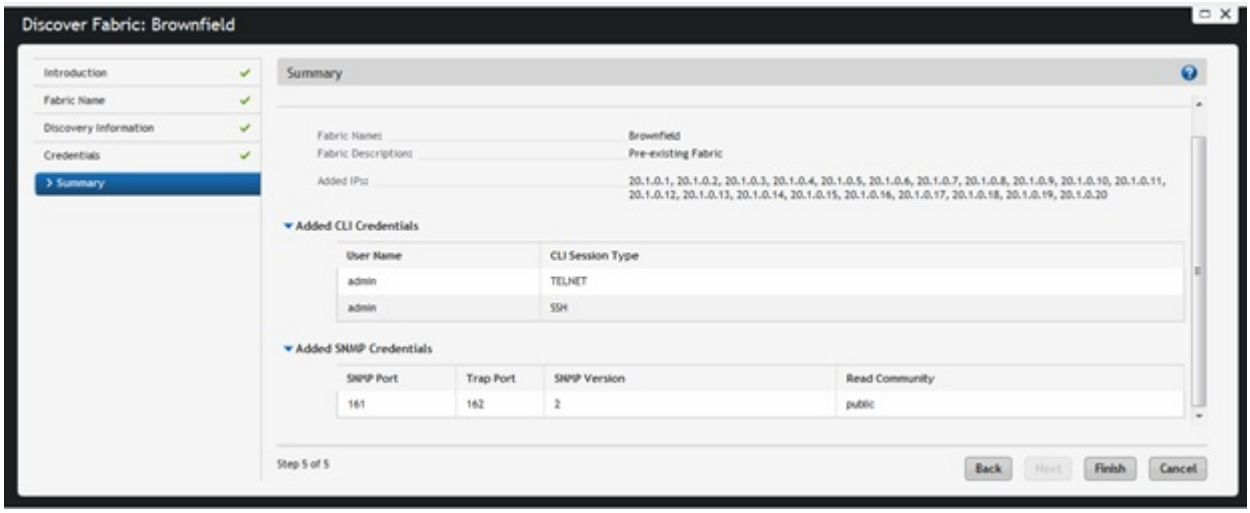


Figure 17. Discover Fabric Wizard — Summary Screen

18. In the **Summary** screen, review the discover summary information and then click **Finish** to start the fabric discovery process. AFM then displays the **Network Deployment Summary** screen.

    Next Steps

    Click the **Discover Status** link to check the status of discovered existing fabric. For information about the **Discover Status** screen, see Step 2: View Discovery Status Screen

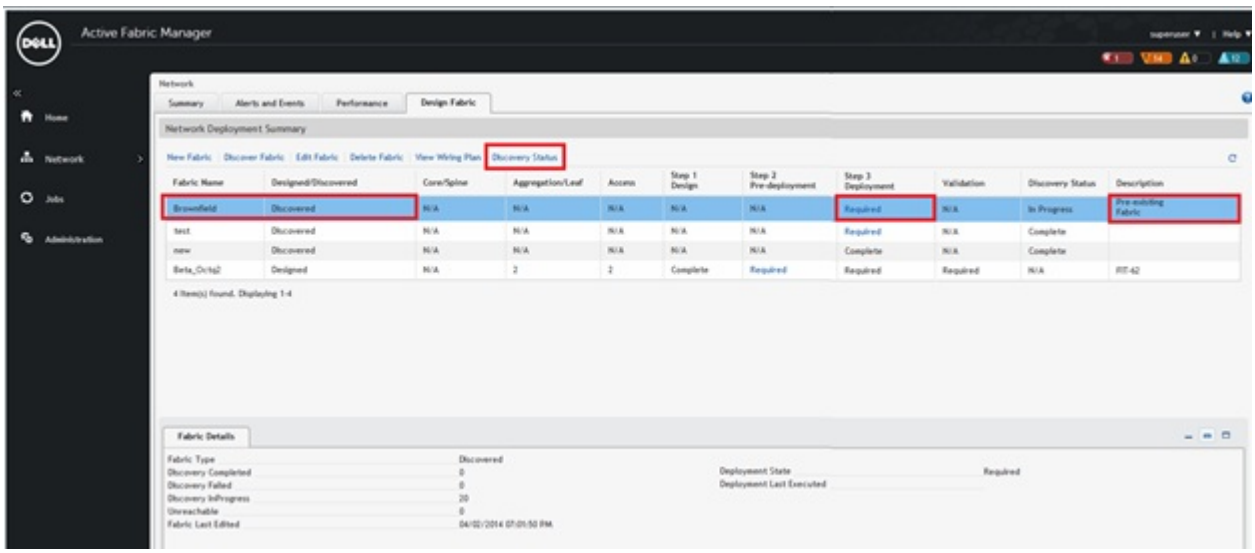


Figure 18. Discovery Status Link

Step 2: View Discovery Status of an Existing Fabric

Use the **Discovery Status** screen to do the following:

- Display the current fabric discovery status and details for switches and chassis used in the existing fabric or an IOA in a M1000e chassis.
- Verify that AFM has discovered all the switches in an existing fabric or IOA fabric.
- Rediscover an existing chassis or switch for troubleshooting.
- Remove a switch from the discovered fabric.

See also Discovering and Deploying an Existing Fabric.

The following discover options are available:

- **Rediscover Fabric** — Rediscovers an existing fabric.
- **Rediscovered Switches** — Rediscovers an existing chassis or switch for troubleshooting. If a device is not discovered, check the **Reason** column for a recommended action. To rediscover an existing chassis or switch, select the checkbox for the device and then click **Rediscover Switches** link to restart the discovery process for the selected devices. You can also select all devices by selecting the top left checkbox.
- **Remove Switches** — Removes a switch from the discovered fabric by excluding the switch IP from the fabric.

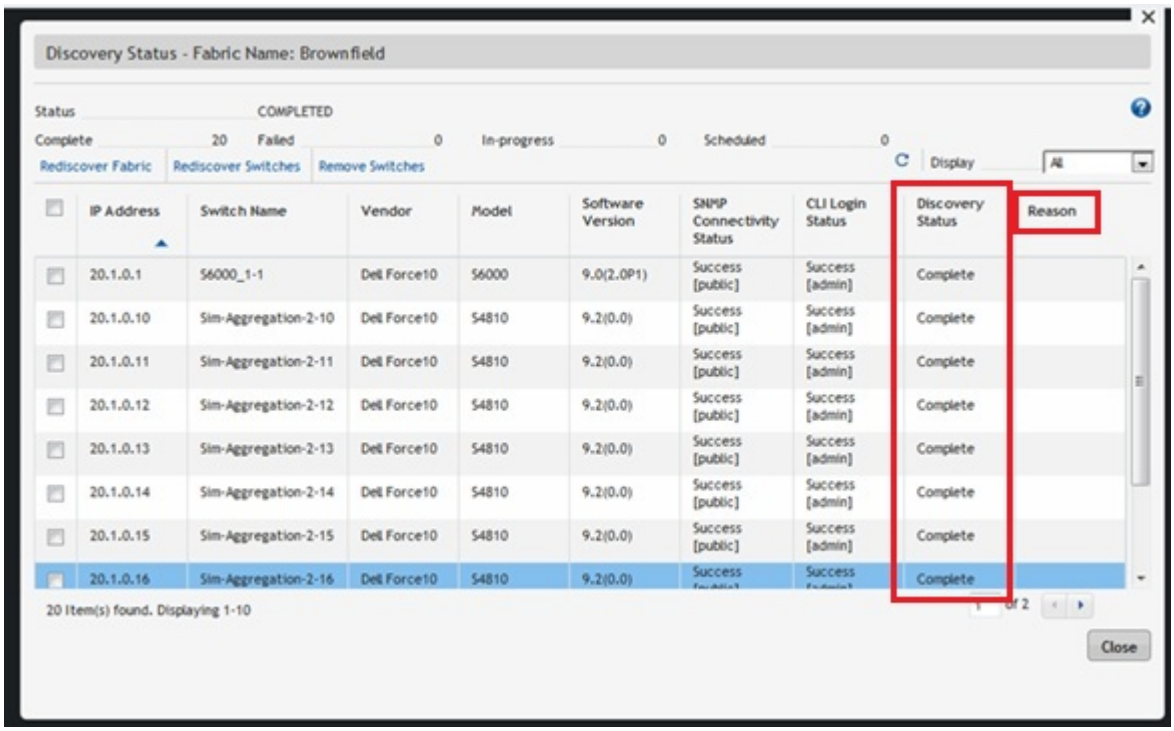


Figure 19. Successfully Discovered Fabric

The following information is displayed:

- IP address
- Switch name
- Vendor
- Model

NOTE: Only Dell IOA and MXL blades are identified. All other blade types are listed as "Unknown."

- Software version
- SNMP status
- CLI login status
- Discovery status
- Reason (Completed, In Progress, Failed, or Not Yet Started) — If a device is not discovered, check the **Reason** Column for a recommended action.

For information about how to discover a fabric, see Discovering an Existing Fabric.

You can also view the tabular wiring plan for a discovered fabric at the **Network** > **Design** > **View Wiring Plan** screen.

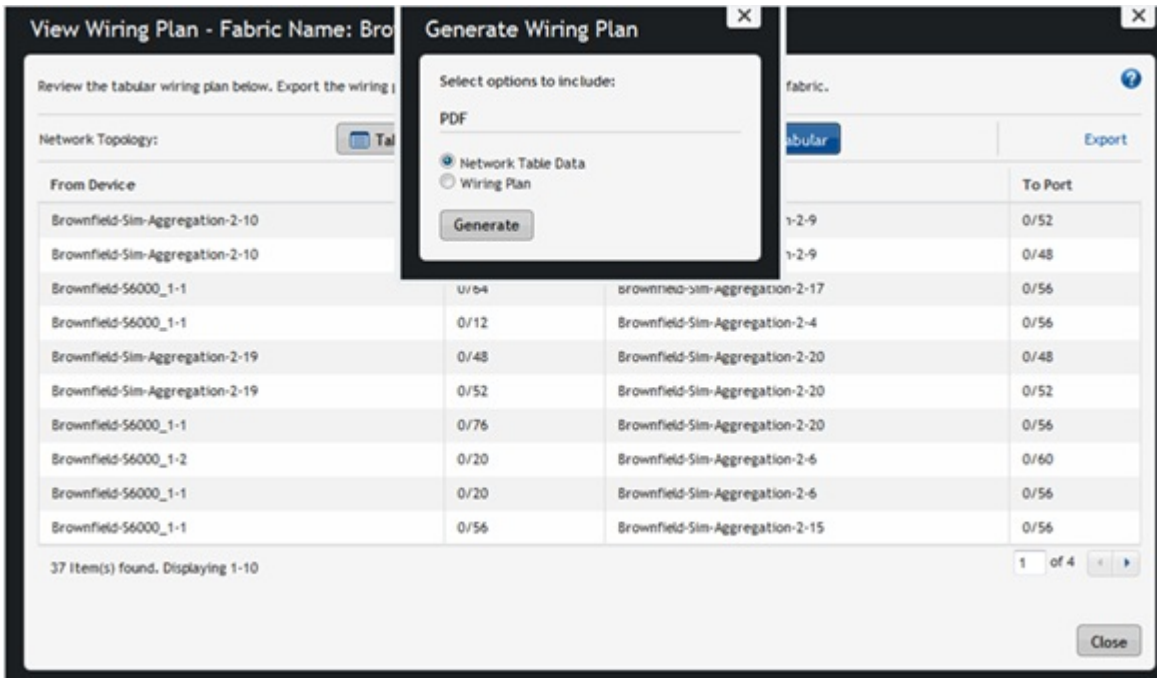


Figure 20. Discovered Fabric Wiring Plan

To view the discovery status of an existing fabric

1. Navigate to the **Network** > **Design Fabric** > **Discover Status** screen.

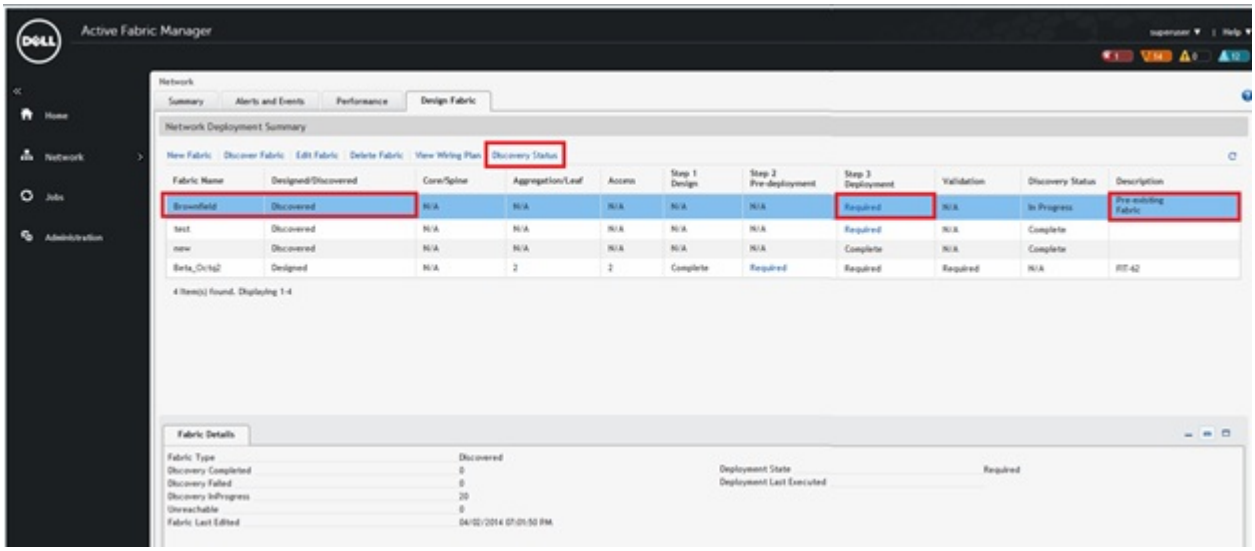


Figure 21. Discovery Status Link

NOTE:

To remove a chassis, navigate to the **Edit Fabric** screen and delete the IP address of the chassis.

2. Click the **Discover Status** link to check the discovery status of an existing fabric. Check for discovered failed devices and look for error messages in the **Reason** column for why the devices were not discovered, such as an authentication failure. In this case AFM will display the following reason: **Check CLI communication available from AFM server with the given credentials**.

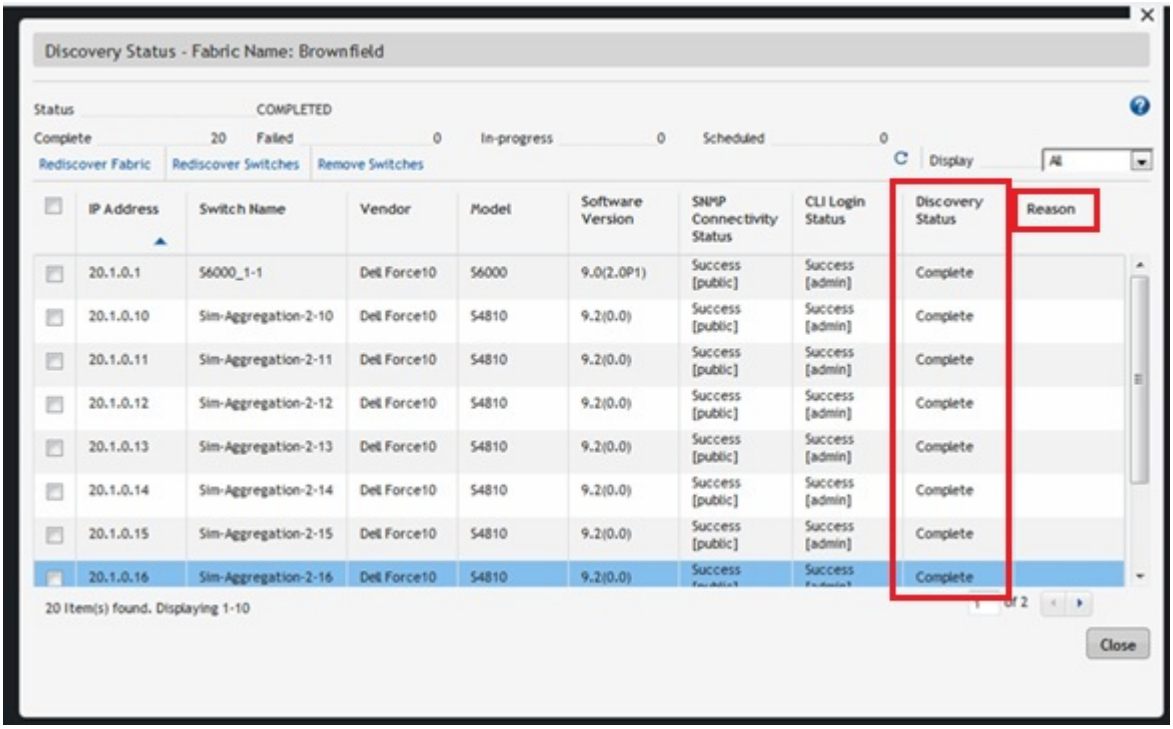


Figure 22. Successfully Discovered Fabric

Next Steps

1. Close the **Discovery Status** screen.

2. After you successfully discovered the existing fabric, deploy it. For information about deploying an existing fabric, see Step 3: Deploy Discovered Fabric.

Step 3: Deploy Discovered Fabric

This section describes how to deploy a discovered fabric. Once the discovered fabric is successfully deployed, the fabric can send alarms and events to AFM. The design, pre-deployment and validation fields at the **Network** > *Fabric Name* > **Configure and Deploy** screen are **not** applicable for discovering an existing fabric. See Discovering and Deploying an Existing Fabric.

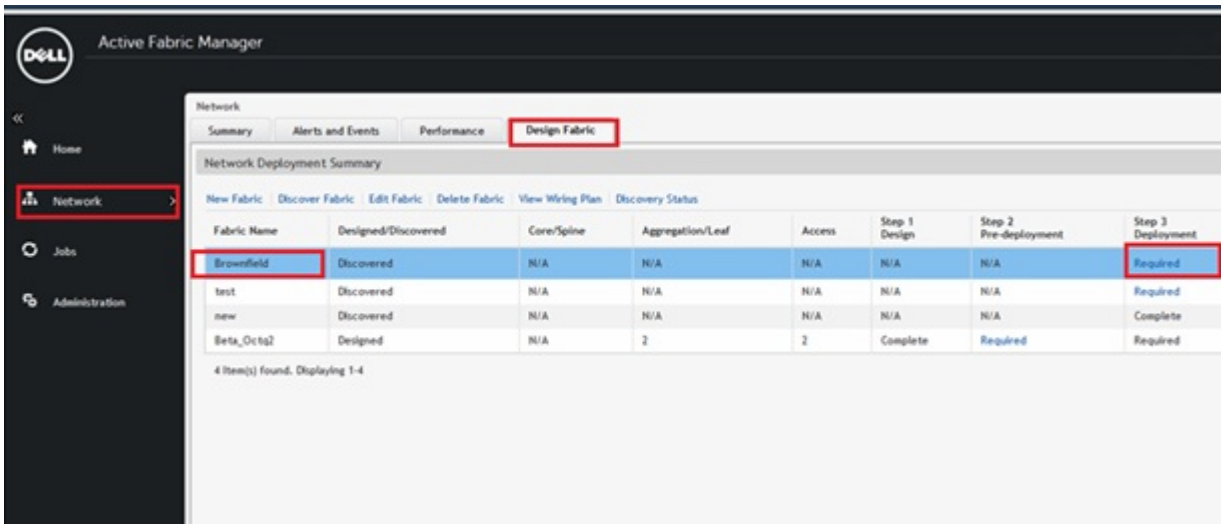


Figure 23. Deploy Successfully Discovered Existing Fabric

To deploy a discovered fabric:

1. Close the **Discovery Status** screen.
2. Navigate to the **Network** > **Design Fabric** screen.
3. Navigate to the **Step 3 Deployment** column and deploy the discovered fabric by clicking the **Required** link that is associated with the discovered fabric.

   The **Deploy and Validation** screen displays.
4. On the **Deploy** tab, select the switches in the fabric you want to deploy in the discovered fabric.
5. Click the **Deploy Selected** link.

   The **Configuration deployment option** screen displays.

   Figure 24. Apply Configuration Changes to the Switch Option
6. Select the **Apply configuration changes to the switch** option and then click the **OK** button.

Next Steps

Perform maintenance operations, such as monitoring and software updates.

7

IOA Fabric Designer Wizard

Use the IOA fabric design wizard to design a Layer 2 fabric that has an I/O Aggregator (IOA) blade switch in a M1000e chassis. AFM supports IOA in standalone mode only.

1. Make sure that the IOA blade switch is in standalone mode (default mode) using the following FTOS CLI command:

   show system *stack-unit* **iom-mode**

   For more information about this command, see the *Dell PowerEdge Command Line Reference Guide for the M I/O Aggregator*.
2. Navigate to the Fabric Design Wizard on the **Network** > **Design Fabric** screen.

   NOTE: If you are designing a fabric without an IOA blade switch, see Using the Fabric Design Wizard..
3. Click the **New Fabric** link.

   The **Introduction** screen displays.

   NOTE: You can click the **Save & Exit** button to save the current information and exit the wizard or click **Cancel** to exit the wizard without saving the current information.
4. Review the introduction and click the **Next** button.

   The **Fabric Name** screen displays.

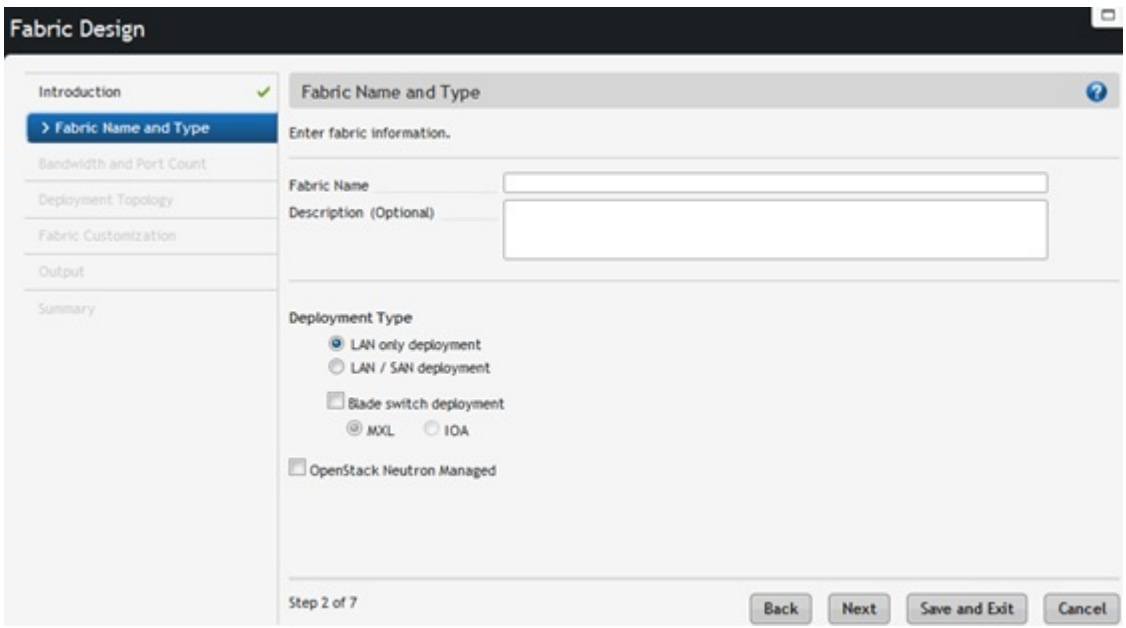


Figure 25. Fabric Design Wizard Screen

5. On the **Fabric Name and Type** screen, select the **Blade Switch Deployment** checkbox, then select the **IOA** radio button.

6. Click the **Next** button to display a Fabric Design Wizard that is for designing fabrics that only use IOA blades.

   The IOA **Fabric Designer** wizard displays.

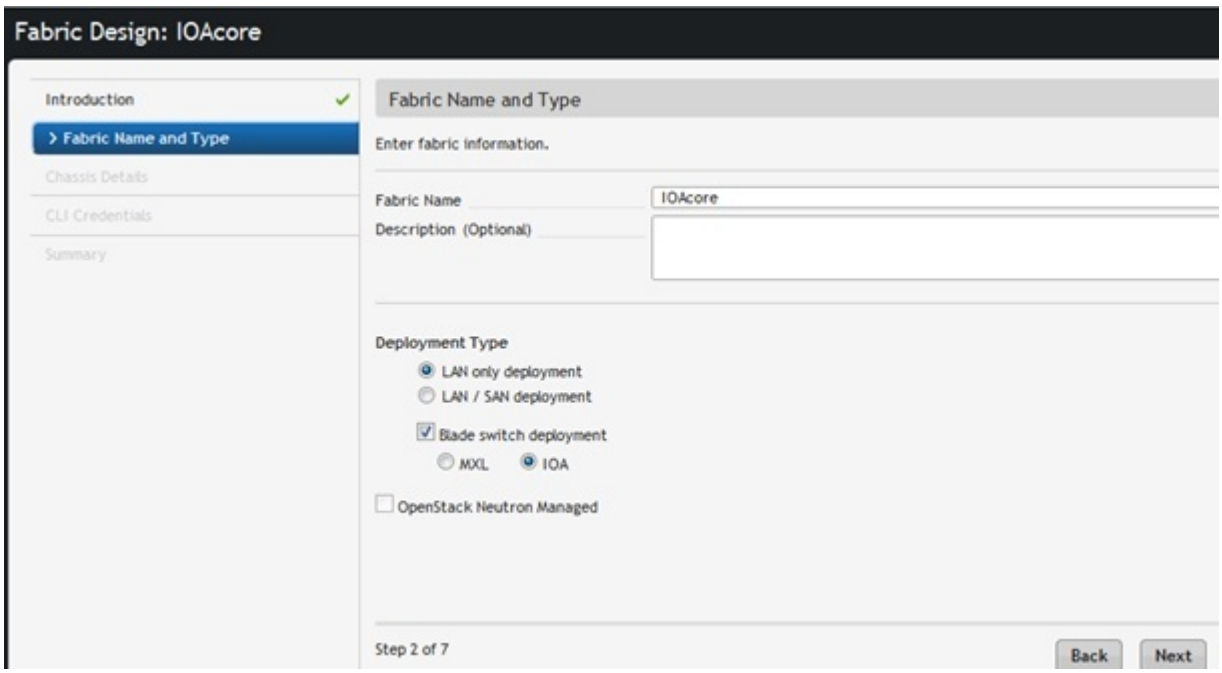
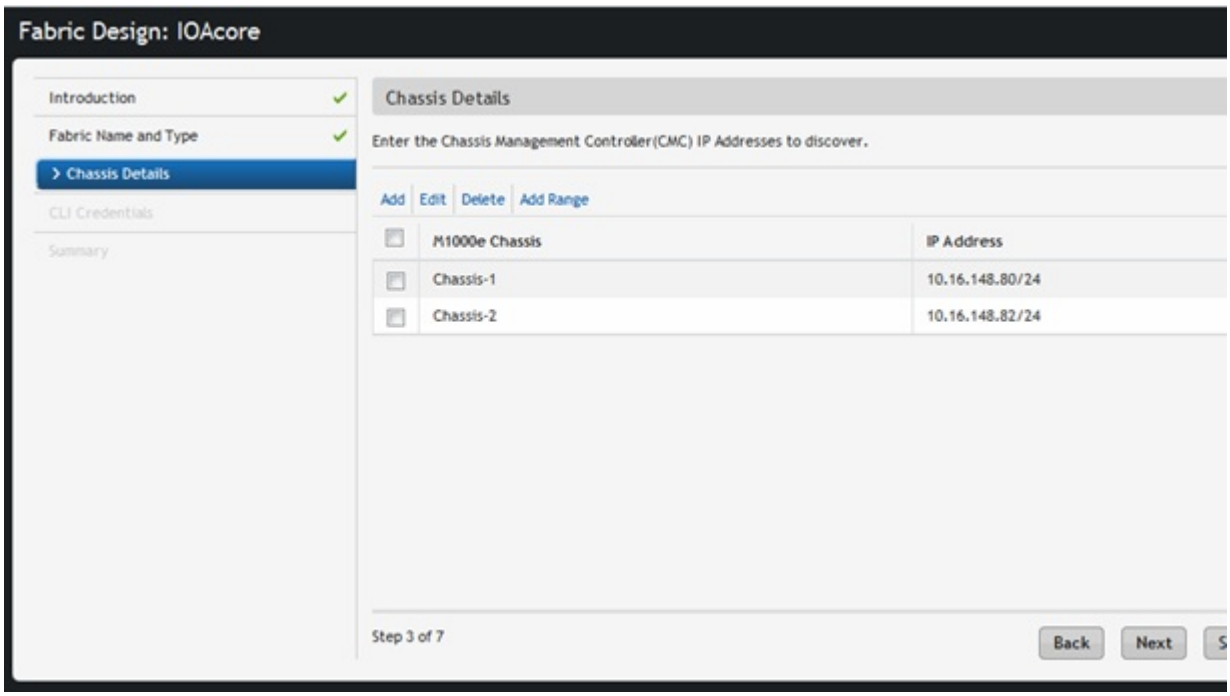


Figure 26. IOA Fabric Design Wizard — Fabric Name and Type Screen

7. Click the **Next** button.

   The **Chassis Details** screen displays.

   Figure 27. IOA Fabric Design Wizard — Chassis Details Screen



8. Enter the Chassis Management Controller (CMC) IP addresses to include in the fabric. The following options are available:

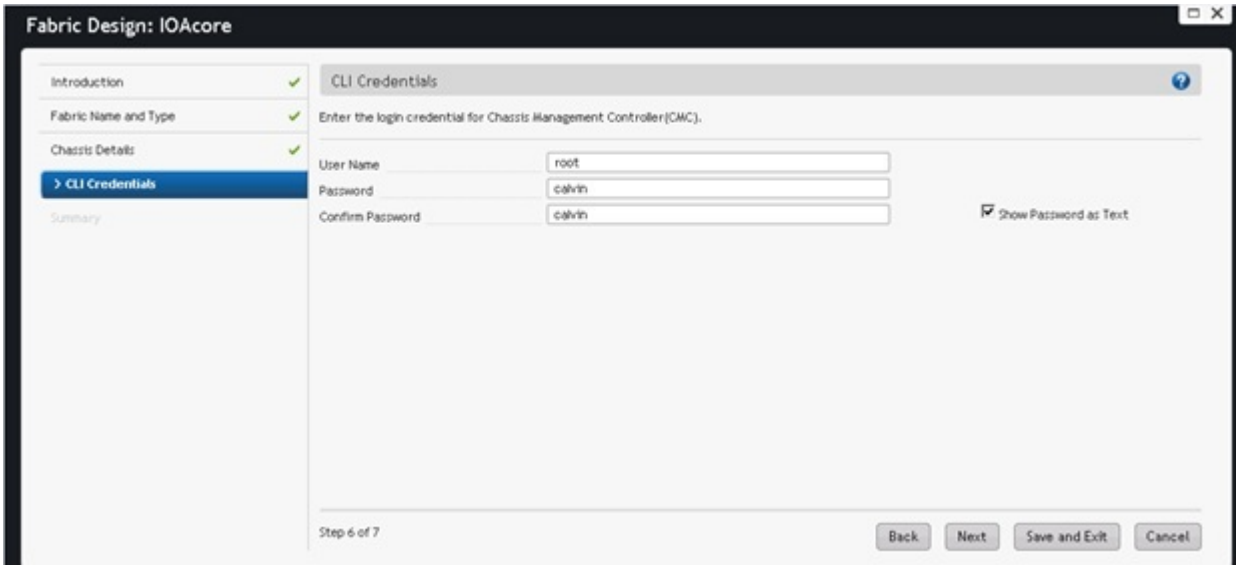
   - **Add:** Enter the chassis IP address in the first field and the prefix in the field after the slash and click **OK**. Click **Cancel** to close the Add window without adding the IP address.
   - **Add Range:** Enter the chassis ID in the **Number of M1000e Chassis:** field. Enter the first IP address in the range in the **Start IP Address/Prefix** field. Enter the prefix in the field after the slash and click **OK** to add the range or **Cancel** to close the Add Range window without adding the IP range.
   - **Edit:** To edit information for a specific chassis, select the checkbox for that chassis then click **Edit**. After changing the IP address, click **OK** to save changes or **Close** to close the **Edit Chassis IP** window without saving changes.

     NOTE: You cannot edit information for multiple chassis simultaneously.

   - **Delete:** Check the checkbox associated with the chassis that you want to delete, then click the **Delete link**. Click **Yes** to confirm the deletion or **No** to cancel the deletion.

9. Click the **Next** button.

   The **CLI Credentials** screen displays.



10. Enter the user credentials for the CMC. This information is used to log in to all CMCs in the fabric. By default, the **CLI Credentials** screen uses the following CLI credentials: username = **root** and password = **calvin**. If you have changed the CLI credentials, update these fields with the new user name and/or password.
    - Enter the user name in the **User Name** field.
    - Enter the password in the **Password** and **Confirm Password** fields.

11. Click the **Next** button.

    The **Summary** screen displays. The design summary screen shows the added chassis number and IP addresses, and CLI credentials.

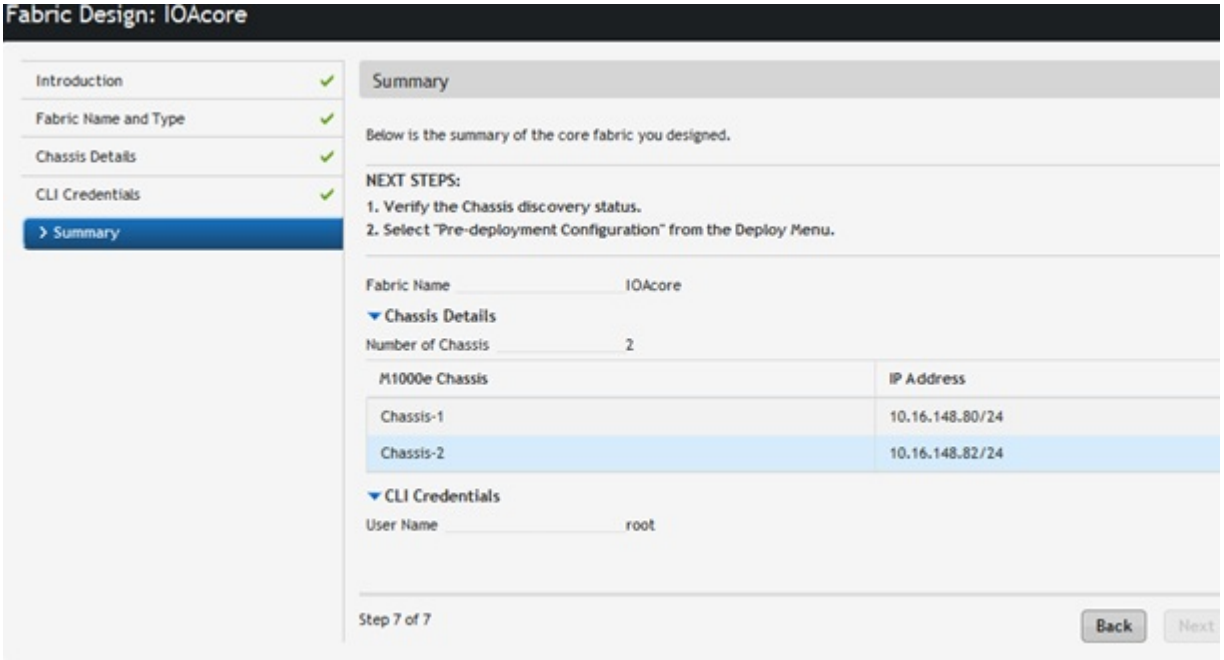


Figure 28. IOA Design Summary Screen

12. Review the fabric design information on the **Summary** screen. To confirm the information, click the **Finish** button. then click **OK** to go to the **Discovery Status** screen

    The discover **Confirmation** screen displays.

13. Click **Yes** to start the fabric discovery process. The **Discovery Status** screen displays detailed information about the installed IOA blade switch on the M1000e chassis. For information about the Discover Status screen, see Discovery Status Screen.

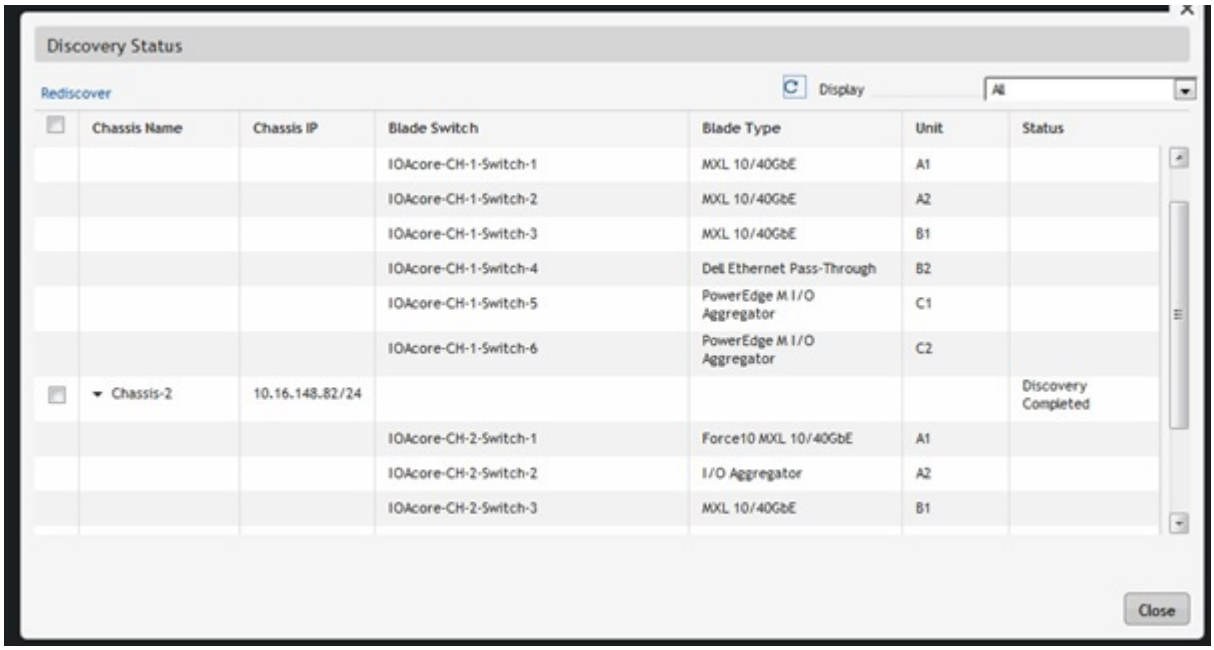


Figure 29. IOA Discover Status Screen

14. After the IOA fabric is successfully discovered, complete the pre-deployment configuration. For information about IOA pre-deployment configuration, see IOA Pre-deployment Wizard.

8

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.

NOTE: If you are designing a fabric using an IOA blade switch, see IOA Fabric Design Wizard.

This **Fabric Design Wizard** allows you to perform the following tasks:

- Create a fabric
- Edit and Expand an Existing Fabric
- Delete the Fabric
- Import an Existing Fabric Design
- View 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 and Type
2. Fabric Design – Step 2: Bandwidth and Port Count
3. Fabric Design – Step 3: Deployment Topology
4. Fabric Design – Step 4: Fabric Customization
5. Fabric Design – Step 5: Output
6. Fabric Design – Step 6: Summary

NOTE: After designing the fabric, prepare it for deployment. For more information, see Pre-deployment Wizard.

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 by comparing it to a 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 16. Fabric Configuration Phases and States

Phase	State	State Description
Design	Incomplete	Indicates that not all required information to complete the design was provided.
	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 number of switches successfully deployed versus the number of total switches in the design. NOTE: Deployment on any of the switches is not in-progress while in this state.

	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 17. Switch Level 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 the following types of customized fabrics based on your workload requirements for your current and future needs. If you are designing a Layer 2 fabric using a IOA blade deployment, see Using the IOA Pre-deployment Wizard.

- **Layer 2** — Use the Layer 2 VLT fabric for workload migration over virtualized environments. See VLT and Selecting a Layer 2 and Layer 3 with Resiliency (Routed VLT) fabric.
- **Layer 3 distributed core** — Use the Layer 3 distributed core for large fabric deployments. See Conventional Core Versus Distributed Core
- **Layer 3 with Resiliency (Routed VLT)** — Use the Layer 3 fabric to extend equal cost multi-pathing capabilities. See Selecting a Layer 2 and Layer 3 with Resiliency (Routed VLT).

This screen allows you to create, edit, delete, and view the fabric.

NOTE: You can also use the Fabric Design Wizard from the **Home** > **Design New Fabric** screen.

Use the following screens to design a fabric:

1. **Fabric Name and Type** — Displays the fabric name, type, and description. Enables Openstack Neutron Management, LAN, LAN/SAN, and Blade Switch deployments.
2. **Bandwidth and Port Count**— Displays 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.

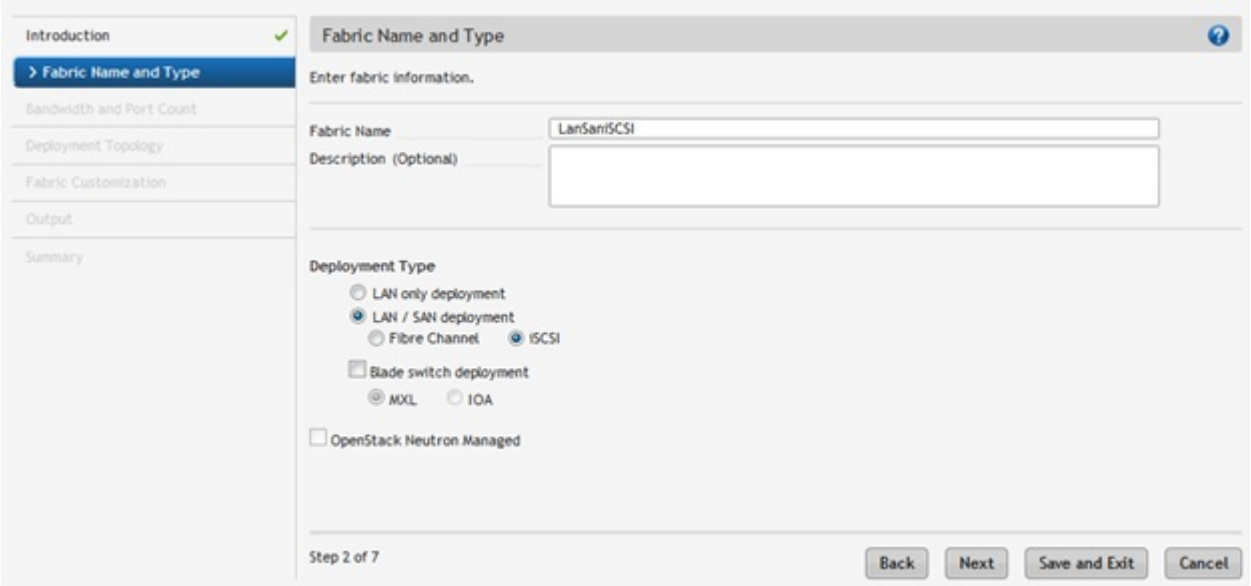
3. **Deployment Topology** — Displays the option to select between a Layer 2 or Layer 3 solution and a list of all applicable deployment topologies based on the workload requirements that you entered on the **Bandwidth and Port Count** and **Fabric Name and Type** screens. This screen also displays **Advanced options** for configuring VLTi links and fabric links. See also Deployment Topology Use Cases.
4. **Fabric Customization** — Displays switch names, model, and switch role (aggregation or access) and modifies the fabric link bandwidth for 2-tier and 3-tier fabrics. For a Layer 2 deployment topology, you can select S4810 or S4820T switches (mixed node) on the access side.
5. **Output** — Displays future switches and links and the fabric in the following formats:
   - graphical wiring plan
   - tabular wiring plan
   - graphical network topology
   - tabular network topology
6. **Summary** — Displays a summary of the fabric design. You can also export the design in XML format and then import the XML design back into AFM.

Fabric Design – Step 1: Fabric Name and Type

To simplify and automate the design process, AFM provides a fabric design wizard to help you design a Layer 2, Layer 3, or Layer 3 with Resiliency (Routed VLT) fabric based on the your current and future datacenter capacity requirements. See Designing the Fabric and Using the Fabric Design Wizard.

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 Layer 2 and Layer 3 with Resiliency (Routed VLT).

To configure the fabric name and type:



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** 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 **17** characters. Valid characters are as follows:
   - alphanumeric
   - underscore (**_**)
   - **+**

   When you specify the name of the fabric, AFM automatically names the switches 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. Navigate to the **Deployment Type** area.

   Select one of the following options:

   - **LAN only deployment** — Creates a Layer 2, Layer 3, or Layer 3 Routed VLT fabric.
   - **LAN/SAN deployment** – Creates a Layer 2 LAN/SAN converge fabric.
     - **Fibre Channel –** Supports a fibre channel (FC) interfaces. Uses the S5000 as a N_Port ID Virtualization (NPIV) Proxy Gateway. This option provides a gateway between the fibre channel switch and server. On the fiber channel you configure up to 8 VLANs with a VLAN ID range between **2**- **4094**. You can associate these VLANs to any FC port.
     - **iSCSI** – Supports iSCSI interfaces.
   - **Blade Switch Deployment —** Uses blade switches (MXL or IOA), This option is for a Layer 2 fabric or Layer 3 with Resiliency (Routed VLT) fabric LAN deployment. Select a blade switch type:
     - **MXL**: Select the **MXL** radio button to use an MXL blade switch.
     - **IOA**: Select the **IOA** radio button to use an IOA blade switch. This option is for a Layer 2 fabric.

       Attention: When you select the IOA blade switch blade deployment and then click the **Next** button, a different design wizard (IOA design wizard) is displayed.
   - **OpenStack Neutron Managed**: If you are using AFM Plug-in for OpenStack, select this option.

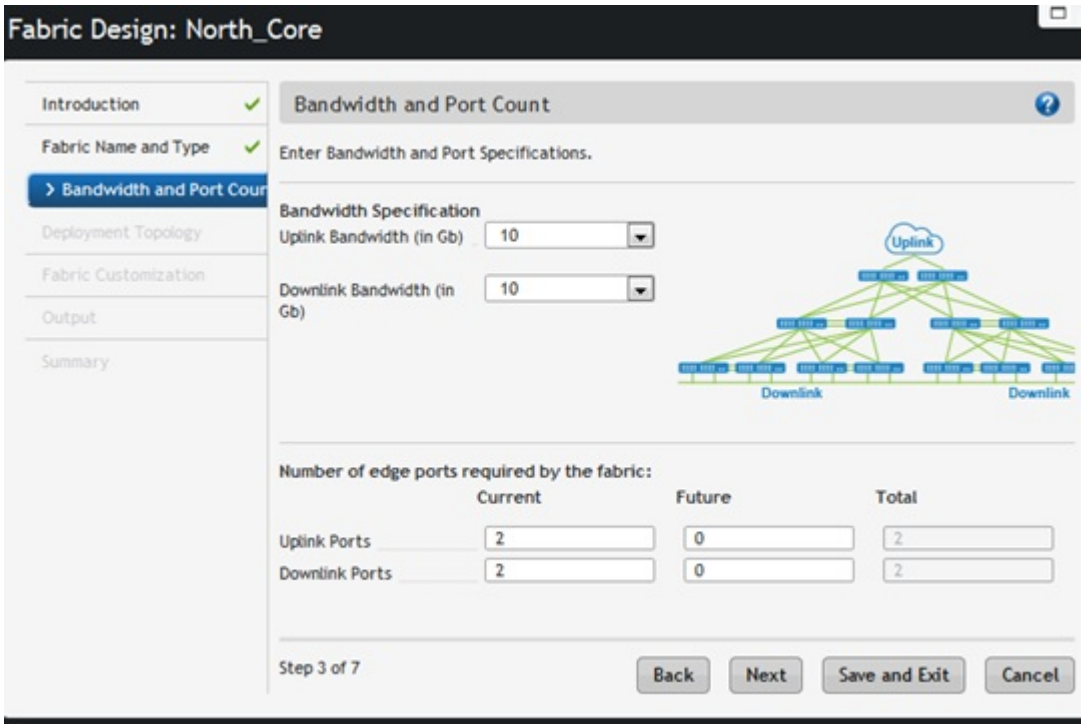
     NOTE: If you select this option, you cannot enter the VLAN configuration in the AFM Pre-Deployment Wizard. This is handled by OpenStack which requires the AFM Neutron Plug-in installation which orchestrates the Layer 2 VLAN configuration between OpenStack and AFM. See the *AFM Plug-in for Openstack Guide*.

7. Click **Next** to go to the **Bandwidth and Port Count** 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 and Port Count

The **Bandwidth and Port Count** 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. The minimum number of uplinks is 2. One uplink is the active link and one uplink is for redundancy. 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 options you have selected in the **Fabric Name and Type** screen. The number of uplink ports, downlink ports, and bandwidth you enter are the major input parameters in the design phase.

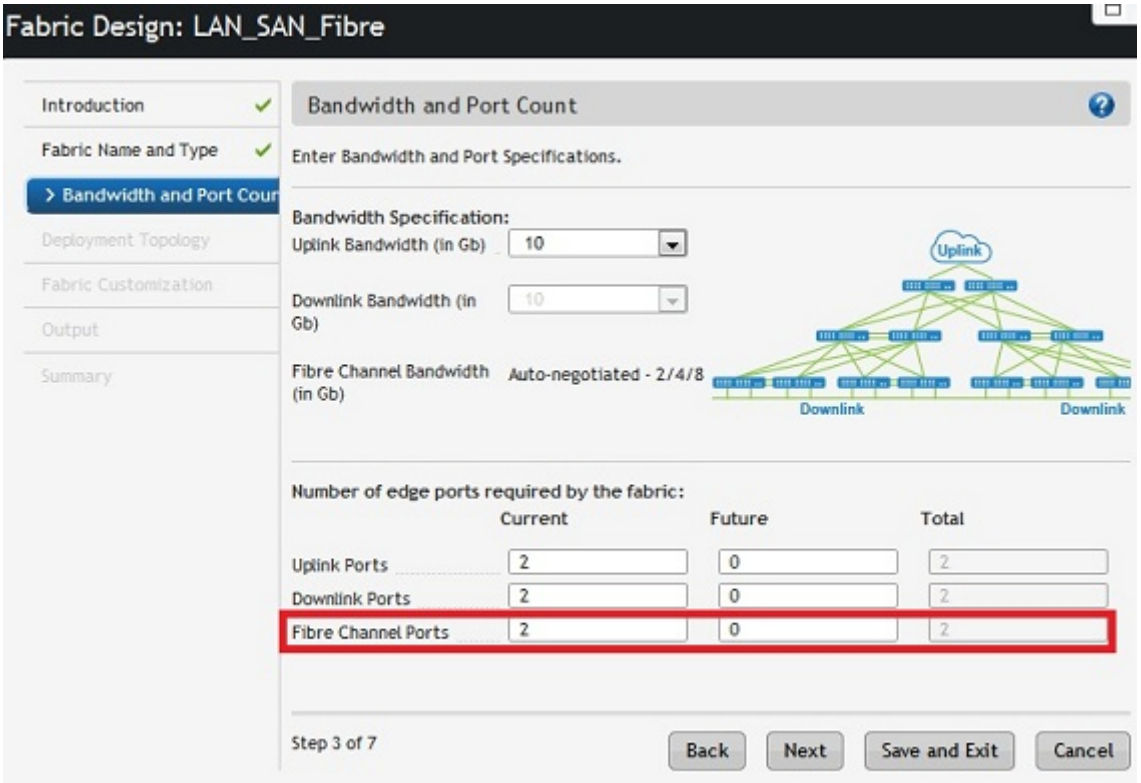

Fabric Design: North_Core
Introduction
Fabric Name and Type
Bandwidth and Port Cour
Deployment Topology
Fabric Customization
Output
Summary
Bandwidth and Port Count
Enter Bandwidth and Port Specifications.
Bandwidth Specification
Uplink Bandwidth (in Gb)
10
Downlink Bandwidth (in Gb)
10
Uplink
Downlink
Downlink
Number of edge ports required by the fabric:
Current
Future
Total
Uplink Ports
2
0
2
Downlink Ports
2
0
2
Step 3 of 7
Back
Next
Save and Exit
Cancel

T**o configure bandwidth and port count for the switches in the fabric**:

1. In the **Bandwidth Specification**:
   a. Select the uplink bandwidth (10 Gb or 40 Gb) using the **Uplink Bandwidth** pull-down menu.
   b. Select the downlink bandwidth (1 Gb, 10 Gb, or 40 Gb) using the **Downlink Bandwidth** pull-down menu.
   - When you select the **1 Gb Downlink Bandwidth** option, the AFM supports deployment topologies with the S55 and S60 switches on the access side.
   - When you select the **10 Gb Downlink Bandwidth** option, the AFM supports all the deployment topologies with the S4810 and S4820T switches on the access side.
   - When you select the **40 Gb Downlink Bandwidth** option, the AFM supports deployment topologies with the Z9000 and S6000 switches on the access side.
2. In the **Number of edge ports required by the fabric**
   a. In the **Uplink Ports Current** column, enter an even number of uplink ports (connections to the WAN) required by the fabric for initial deployment. The minimum number of uplinks is 2. One uplink is for redundancy. For a 10 Gb bandwidth, AFM supports 2 to 32 uplinks. For a 40 Gb Bandwidth, AFM supports 2 to 8 uplinks.
      - For a Layer 2 VLT fabric and Layer 3 with Resiliency (Routed VLT) fabric, an edge port link (uplinks) from the aggregation or core switches that connect outside the fabric. For a 3 tier it is core, for a 2 tier it is aggregation.
      - For Layer 3 distributed core, an edge port link (uplinks) on the first two leaves that connects to the edge WAN, which typically connects to an internet service provider (ISP).
   b. In the **Downlink Ports Current** column, enter an even number of downlink ports (**2** to the maximum number of available ports) required by the fabric for initial deployment. The default is **2** downlink ports.
   c. In the **Uplink Ports Future** column area, enter the number of uplink ports (connections to the WAN) required by the fabric for future expansion of the fabric. If the future ports are not reserved, you cannot expand the fabric in the future.
   d. In the **Downlink Ports Future** column area, enter an even number of downlink ports (connections to the servers, switches, or ToR) required by the fabric for future expansion of the fabric.

      NOTE: When you select the **Blade switch (MXL) deployment** option in the **Fabric Name and Type** screen, the **Bandwidth and Port Count** screen displays a **Blade Switch Pairs** option instead of a **Downlink Ports** option in the **Number of edge ports required by the fabric** area.
   e. If you are connecting to fibre channel ports, navigate to the **Fibre Channel Ports** area and then enter the number of current and future ports required for this interface in the **Current** and **Future**

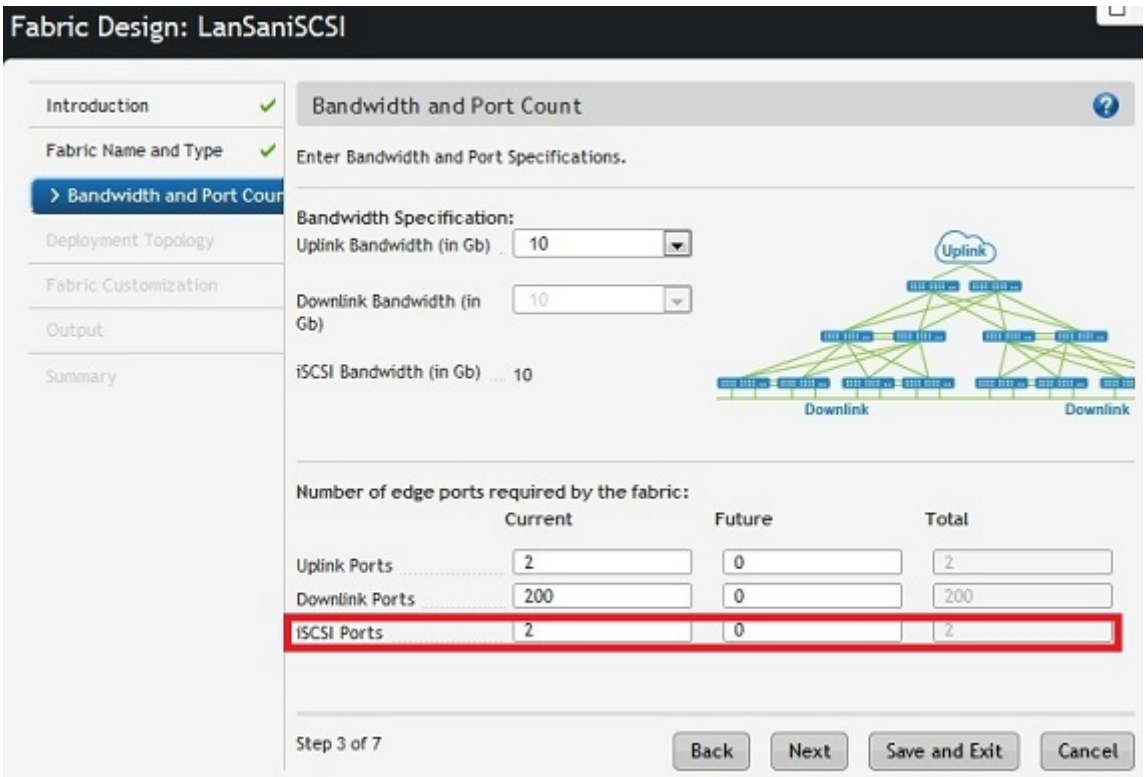
columns.



The minimum number of fibre channel ports is **2**

The maximum number of fibre channel ports (current and future) is **12 * number of S5000 access switches**.

f. If you are connecting to iSCSI ports, navigate to the **iSCSI ports** area and then enter the number of current and future ports required for this interface in the in the **Current** and **Future** columns.



The minimum number of iSCSI ports is **2**.

The maximum number of iSCSI ports (current and future) is **8**.

3. Review the values and then click the **Next** button to go to the **Deployment Topology** screen.

Deployment Topology Use Cases

Use the following use cases as a guide to select a deployment topology.

- Use Case 1: 1 Tier Layer 2 Fabric
- Use Case 2: 1 Tier Layer 3 with Resiliency (Routed VLT)
- Use Case 3: 2 tier Layer 3 Distributed Core
- Use Case 4: 2 Tier Layer 3 Resiliency (Routed VLT)
- Use Case 5: 3 Tier Layer 2
- Use Case 6: 3 Tier Layer 3 Resiliency (Routed VLT)

Use Case 1: 1 Tier Layer 2 Fabric

When you select a 1 Tier Layer 2 fabric:

- The uplinks between the 2 aggregation switches and external switch (WAN) supports the Layer 3 protocol (OSPF, iBGP or eBGP).
- The downlinks from the 2 aggregation switches supports the Layer 2 protocol (VLAN or VLAN/VRRP). The default setting on the pre-deployment screen is VLAN configuration which allows you to

configure downlink connections to servers. To support redundancy between the aggregation switches and ToR switches, select the **VLAN and VRRP Configuration** option.

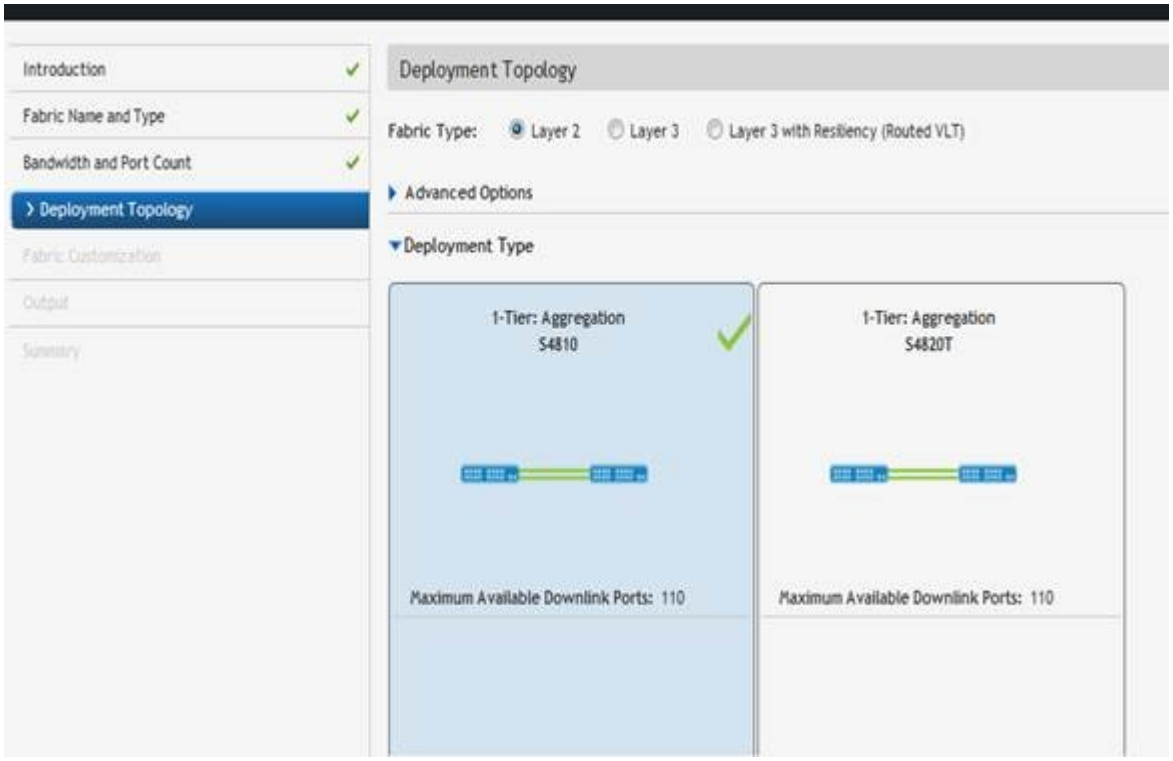


Figure 30. Example: Tier 1 with Layer 2 VLT fabric Deployment Topology

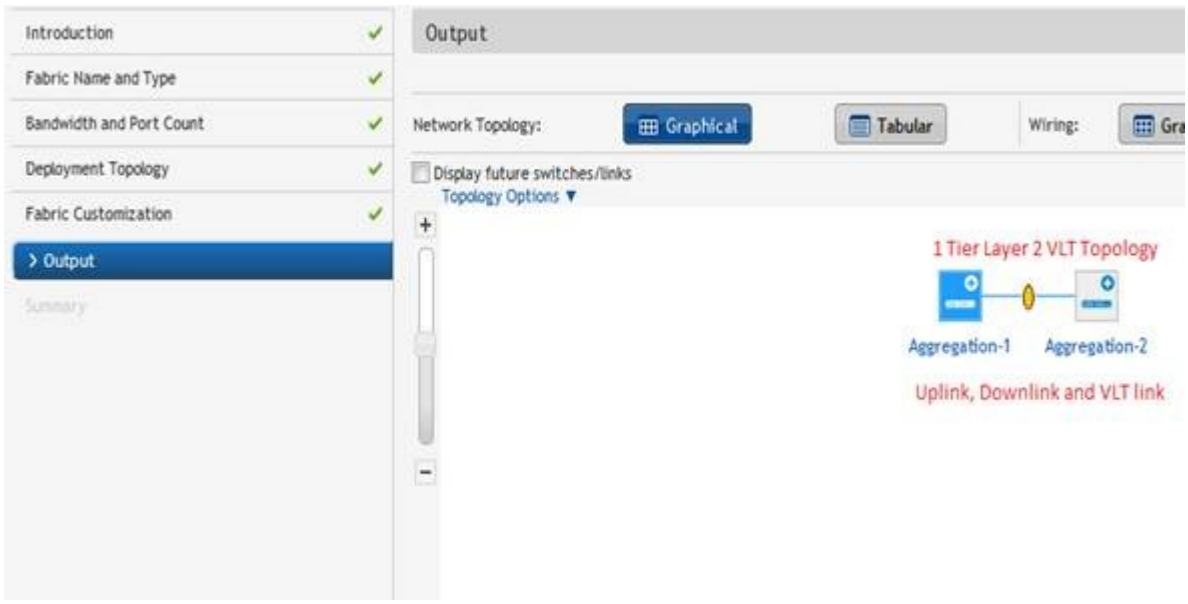


Figure 31. Example: Tier 1 with Layer 2 VLT fabric Graphical View

Use Case 2: 1 Tier Layer 3 with Resiliency (Routed VLT)

When you select a 1 tier Layer 3 with Resiliency (Routed VLT) fabric:

- The uplinks between the 2 aggregation switches and external switch (WAN) supports the Layer 3 protocol (OSPF, iBGP or eBGP).
- The downlinks from the 2 aggregation switches supports the Layer 2 protocol (VLAN/VRRP or VLAN IP). During the design phase at the **Deployment Topology** screen, you select the fabric type and deployment type (topology). In this example shown below, a Layer 3 with Resiliency (Routed VLT) fabric. Based on the deployment type option selected, different downlink options are configured in the access tier.

Use Case 3: 2 Tier Layer 2

When you select a 2 tier Layer 2 VLT fabric:

- The fabric links between aggregation and access switches supports the Layer 2 protocol.
- The uplinks between the aggregation switches and external switch (WAN) supports the Layer 3 protocol (OSPF, iBGP or eBGP).
- The downlinks from the access switches supports the Layer 2 protocol (VLAN or VLAN/VRRP). The default setting on the pre-deployment screen is VLAN configuration which allows you to configure downlink connections to servers. Select the "**VLAN and VRRP Configuration**" option to support redundancy between the access switch and ToR switches.

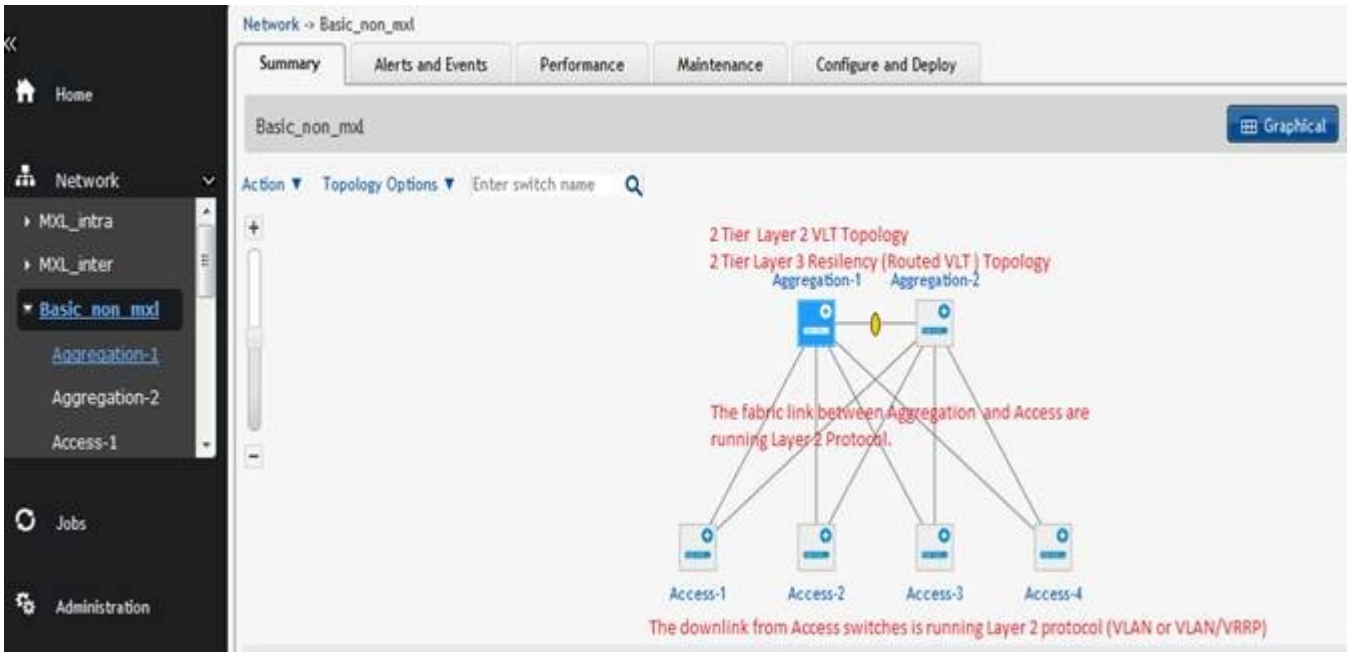


Figure 32. Example: 2 Tier Layer 2 VLT Fabric

Use Case 3: 2 tier Layer 3 Distributed Core

When you select a 2 tier Layer 3 distributed core fabric:

- The fabric links between the spine and leaf switches supports the Layer 3 OSPF routing protocol.
- The uplinks between spine switch and external switch (WAN) supports the Layer 3 protocol (OSPF, iBGP or eBGP).
- The downlinks from the access switches supports the Layer 2 protocol (**VLAN** or **VLAN** and **LAG**).
  - If the **VLAN** option is selected, the downlinks connecting to server is configured to use the VLAN protocol.
  - If the **VLAN and LAG** option is selected, the downlinks between the leafs and ToR is configured to use VLAN, VRRP, and LAG for redundancy.

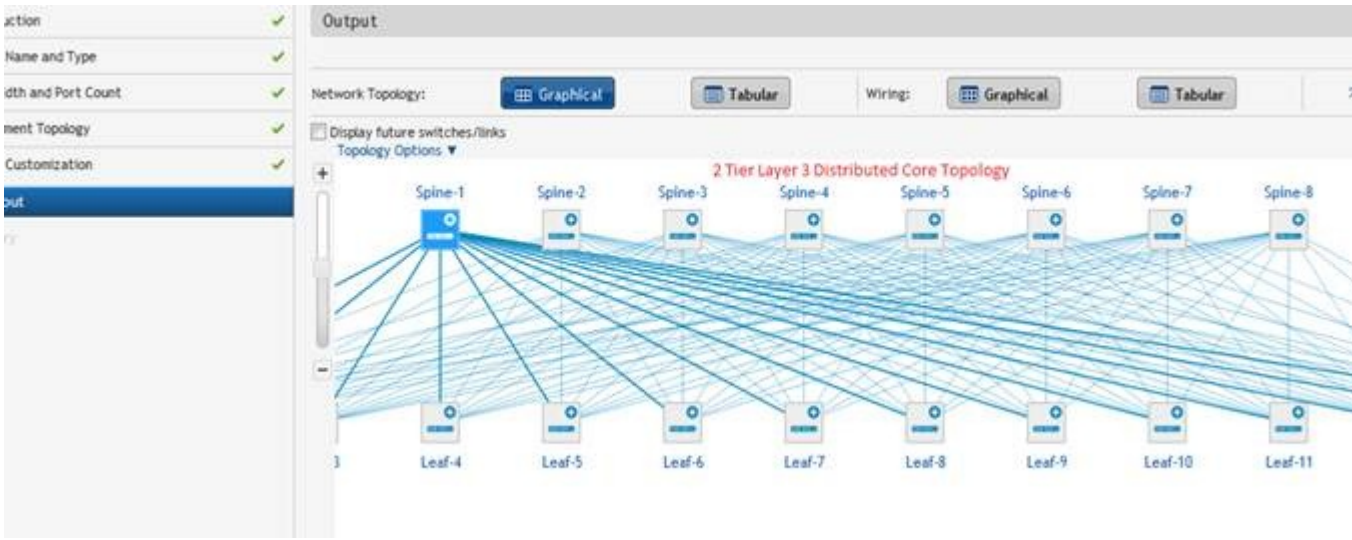


Figure 33. Example: 2 tier Layer 3 Distributed Core

Use Case 4: 2 Tier Layer 3 Resiliency (Routed VLT)

When you select a 2 tier Layer 3 with Resiliency (Routed VLT) fabric:

- The fabric links between the aggregation and access switches supports the Layer 3 protocol with OSPF in the VLAN interfaces.
- The uplinks between the aggregation switch and external switch (WAN) supports the Layer 3 protocol (OSPF, iBGP or eBGP).
- The downlinks from the access switches supports the Layer 2 protocol (VLAN/VRRP or VLAN IP). During the design phase at the Deployment Topology screen, you select the fabric type and deployment type (topology). In this example shown below, a Layer 3 with Resiliency (Routed VLT) fabric. Based on the deployment type option selected, the different options to be configured in downlink at the access tier.

The following section lists the topology types that you can select:

1. **Layer 3 with Resiliency (Routed VLT) with stacking option** – When you select the **Stacking** option, configure the VLAN with the primary and secondary IP addresses for each access switch.

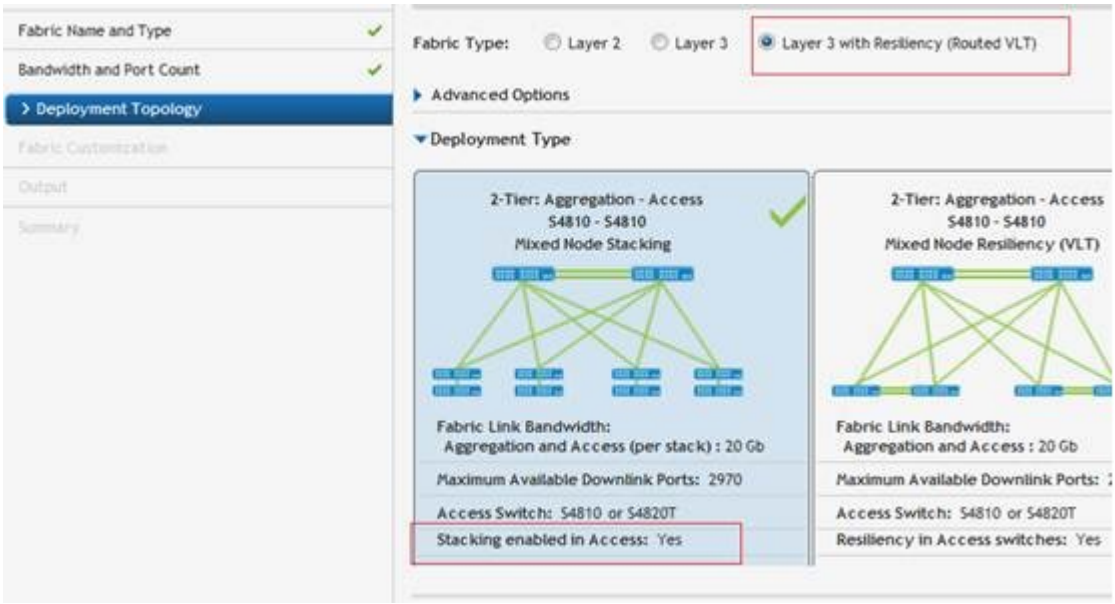


Figure 34. Example: 2 Tier Layer 3 with Resiliency (Routed VLT) with Stacking Option

2. **Layer 3 with Resiliency (Routed VLT) with VLT option** – When you select the **VLT** option, the default configuration is to enter the VLAN ID, Primary IP address and Secondary address. If you select the Enable Layer 3 Protocol in Access Switches option, configure the VLAN ID and then the IP Range. When you complete the pre-deployment configuration, the **Advanced VLAN IP Configuration** option is available at the **Configure and Deploy Summary** screen.

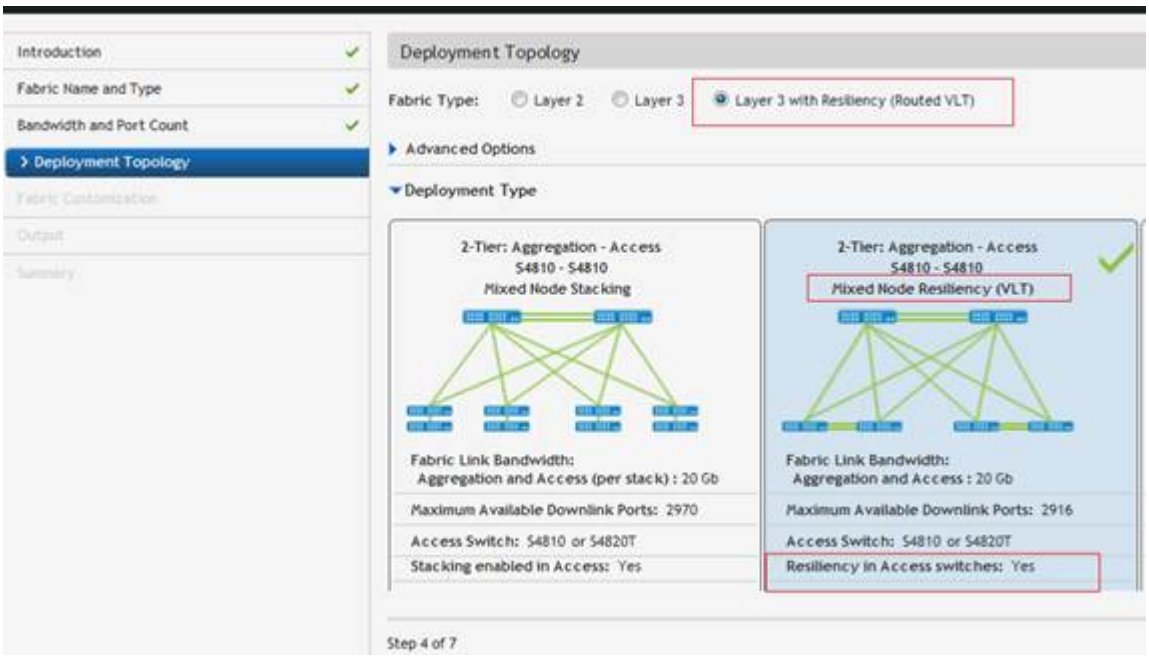


Figure 35. Layer 3 with Resiliency (Routed VLT) with VLT option

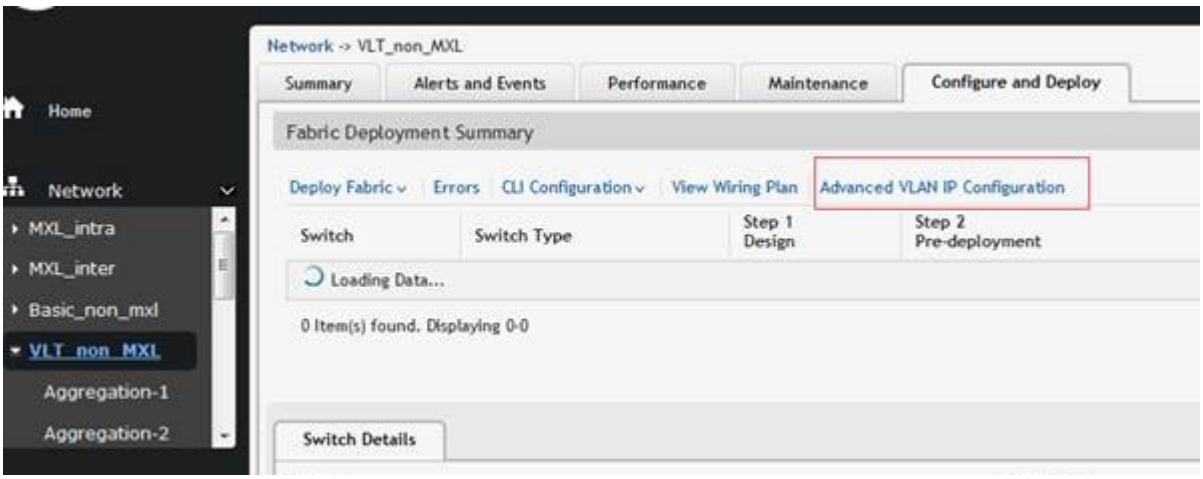


Figure 36. Layer 3 with Resiliency (Routed VLT) with VLT option + Advanced VLAN IP Configuration

3. **Layer 3 with Resiliency (Routed VLT) – Basic option** – When you select the **Basic** option, configure the VLAN with the primary and secondary IP addresses for each access switch.

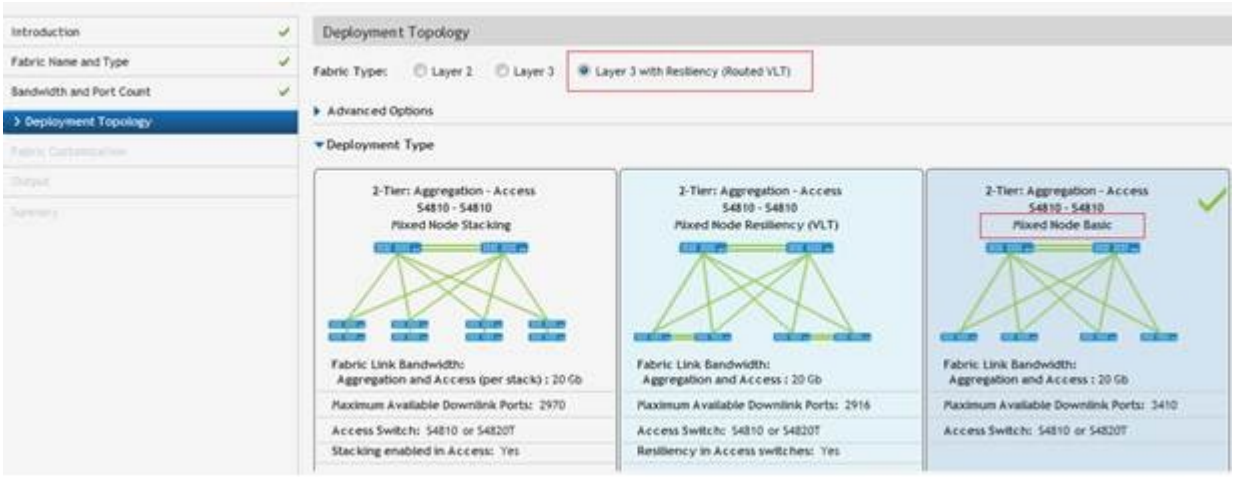


Figure 37. Layer 3 with Resiliency (Routed VLT) with Basic Option

4. **Layer 3 with Resiliency (Routed VLT) with MXL Blade with interChassis option** – With this topology , you select the Deployment Type that has a MXL Blade switch with Resiliency (VLT) and Interchassis (across Chassis) resiliency. Enter the VLAN ID and the IP range. When you complete the pre-deployment configuration, the **Advanced VLAN IP Configuration** option is available at the "Configure and Deploy" Summary screen.

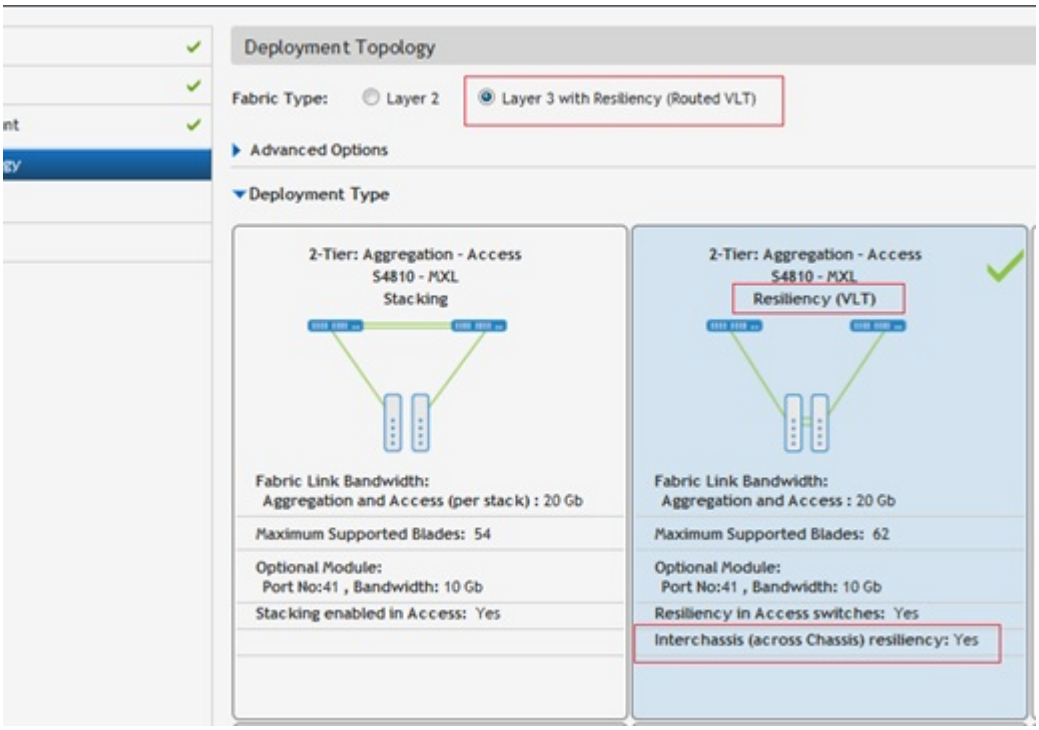


Figure 38. Layer 3 with Resiliency (Routed VLT) with MXL Blade with interChassis option

5. **Layer 3 with Resiliency (Routed VLT)** – **Blade MXL with IntraChassis option**: With this topology, you select the deployment type using that has a MXL Blade switch with Resiliency (VLT) and **Intrachassis (within the same chassis) resiliency** option. Enter the VLAN ID, primary and secondary IP addresses.

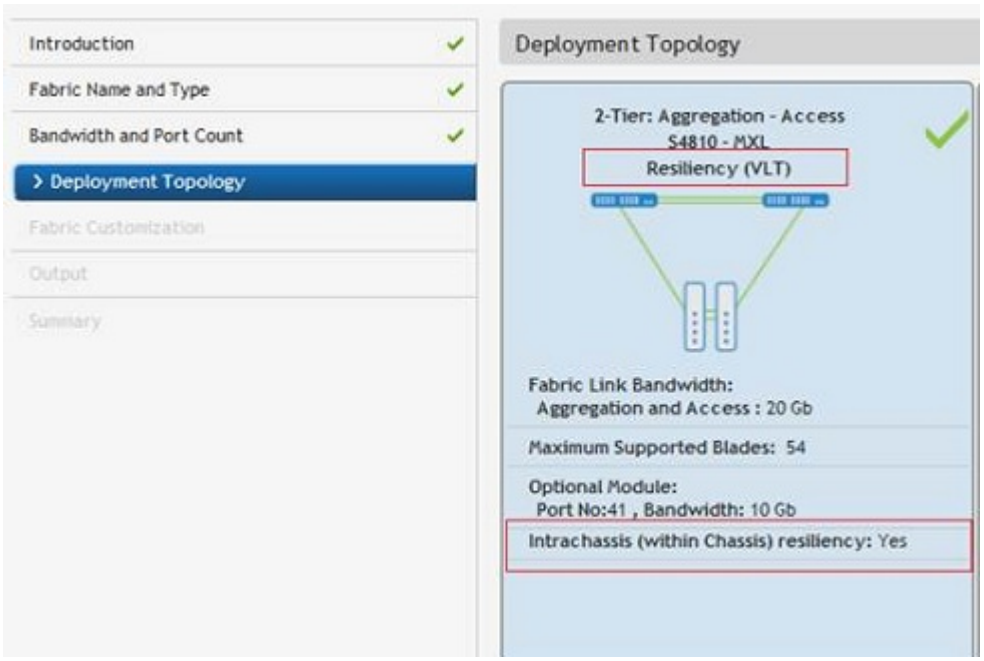


Figure 39. Layer 3 with Resiliency (Routed VLT) Blade MXL with IntraChassis option

Use Case 5: 3 Tier Layer 2

When you select a 3 tier Layer 2 fabric:

- The fabric links between core and aggregation switches supports the Layer 3 protocol.
- The fabric links between aggregation and access switches supports the Layer 2 protocol.
- The uplinks between the aggregation switches and external switch (WAN) supports the Layer 3 protocol (OSPF, iBGP or eBGP).
- The downlink from the access switches supports the Layer 2 protocol (VLAN or VLAN/VRRP). The default setting on the pre-deployment screen is VLAN configuration which allows you to configure downlink connections to servers. Select the **VLAN and VRRP Configuration** option to support redundancy between the access switch and ToR switches.

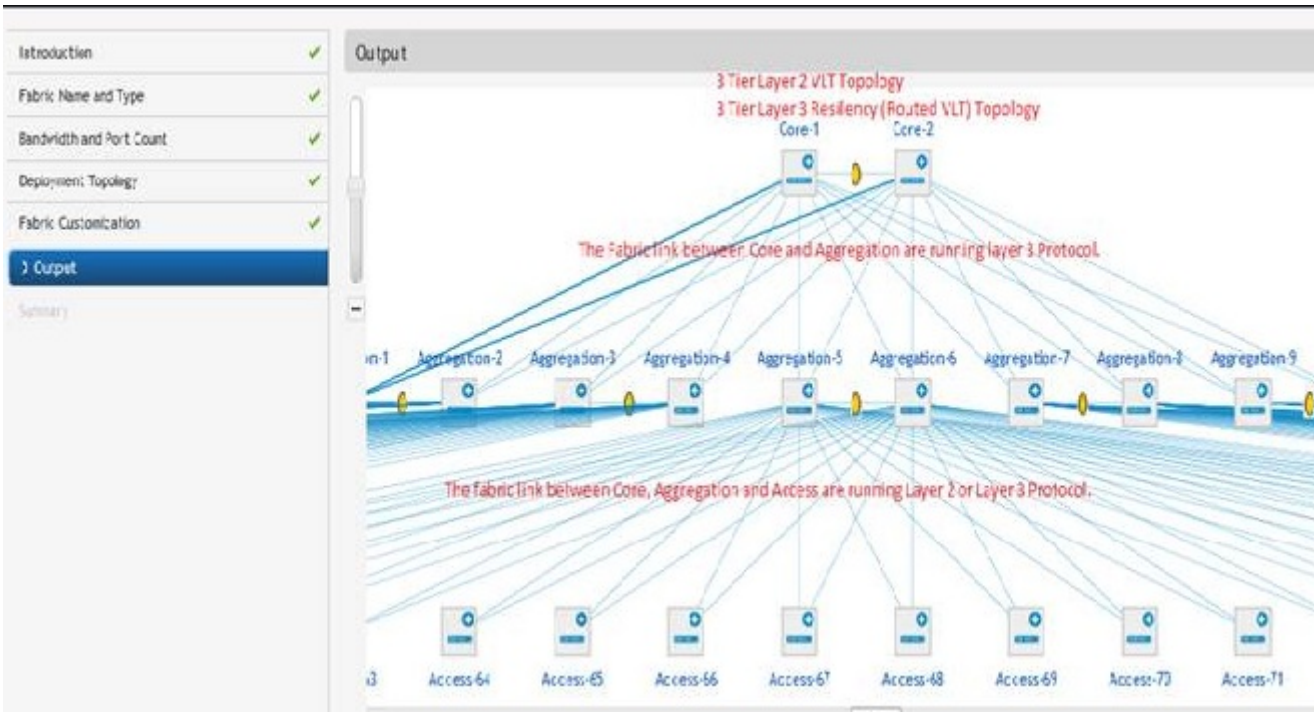


Figure 40. 3 Tier Layer 2 VLT Topology

Use Case 6: 3 Tier Layer 3 Resiliency (Routed VLT)

When you select a 3 tier Layer 3 with Resiliency (Routed VLT) fabric:

- The fabric links between core and aggregation switches supports Layer 3 protocol with OSPF in the VLAN interfaces.
- The fabric links between the aggregation and access switches supports the Layer 2 protocol the Layer 2 protocol.
- The uplinks between the aggregation switch and external switch (WAN) supports the Layer 3 protocol (OSPF, iBGP or eBGP).
- The downlinks from the access switches supports the Layer 2 protocol (VLAN/VRRP or VLAN IP). During the design phase at the **Deployment Topology** screen, you select the fabric type and deployment type (topology). In this example shown below, a Layer 3 with Resiliency (Routed VLT) fabric. Based on the deployment type option selected, different downlinks options are configured at the access tier.

The following section lists the topology types that you can select:

1. **Layer 3 with Resiliency (Routed VLT) with stacking option** – When you select the **Stacking** option, configure the VLAN with the primary and secondary IP addresses for each access switch.

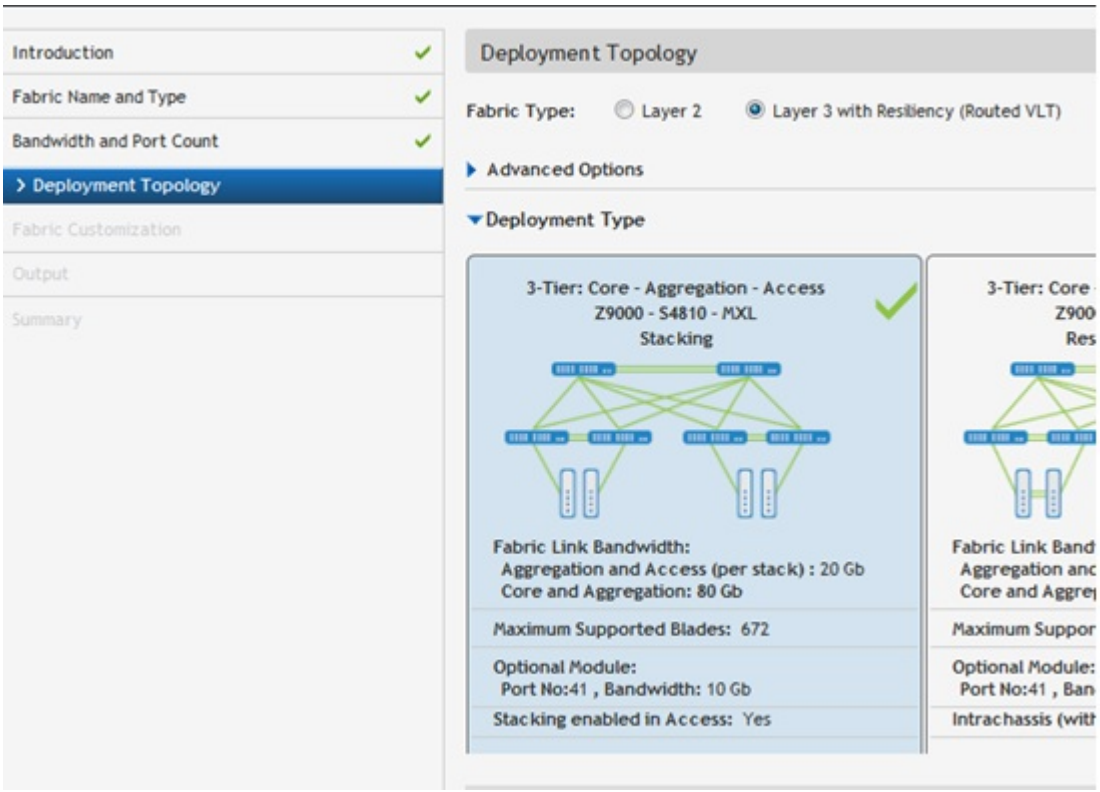


Figure 41. 3 Tier Layer 3 with Resiliency (Routed VLT) with Stacking Option

2. **Layer 3 with Resiliency (Routed VLT) with VLT option** – When you select the **VLT** option, the default configuration is to enter the VLAN ID, Primary IP address and Secondary address. If you select the **Enable Layer 3 Protocol in Access Switches** option, configure the VLAN ID and then the IP Range. When you complete the pre-deployment configuration, the **Advanced VLAN IP Configuration** option is available at the **Configure and Deploy** summary screen.

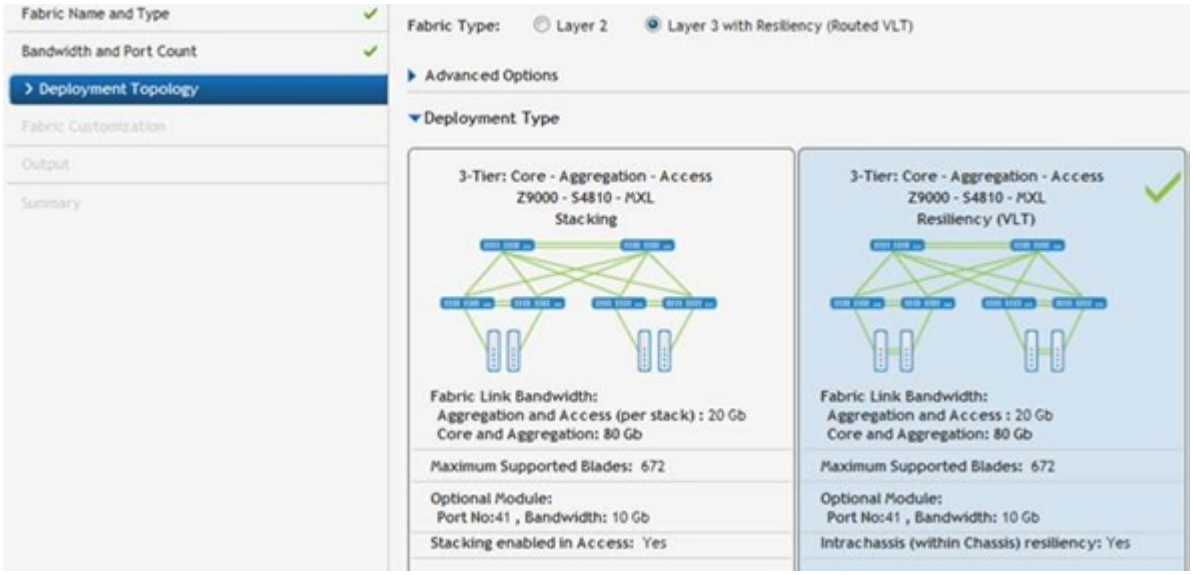


Figure 42. Example: 3 Tier Layer 3 with Resiliency (Routed VLT) with VLT option

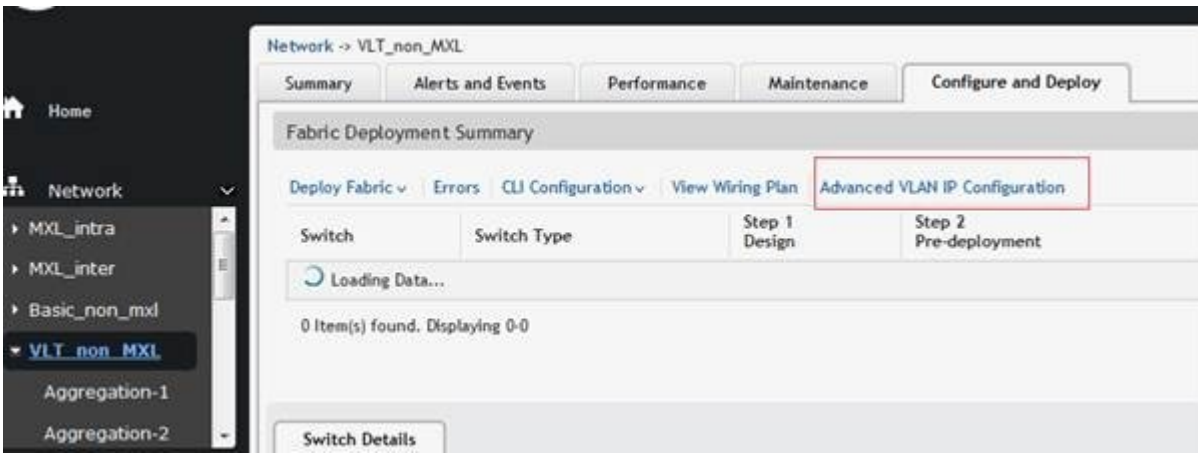


Figure 43. 3 Tier Layer 3 with Resiliency (Routed VLT) with VLT Option + Advanced VLAN IP Configuration

3. **Layer 3 with Resiliency (Routed VLT) – Basic option** – When you select the **Basic** option, configure the VLAN with the primary and secondary IP addresses for each access switch.

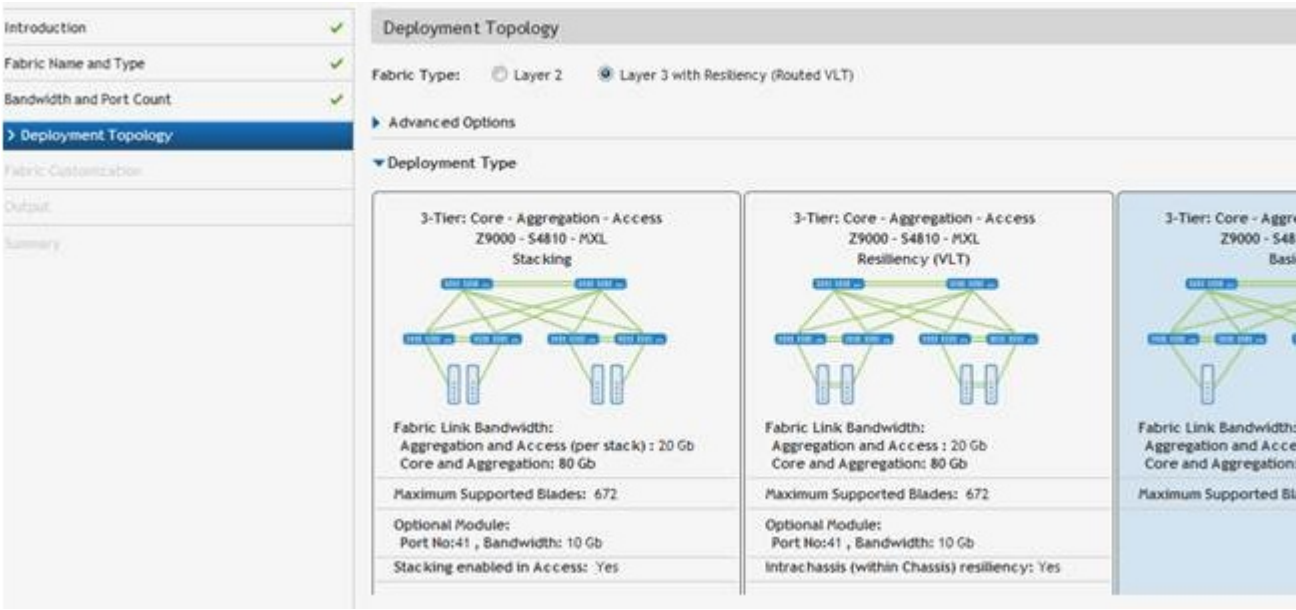


Figure 44. Example: 3 Tier Layer 3 with Resiliency (Routed VLT) with Basic Option

4. **Layer 3 with Resiliency (Routed VLT)** – **Blade MXL with IntraChassis option**: With this topology , you select the deployment type that has a MXL Blade switch with Resiliency (VLT) and **Intrachassis (within the same chassis) resiliency** option. Enter the VLAN ID, primary and secondary IP addresses.

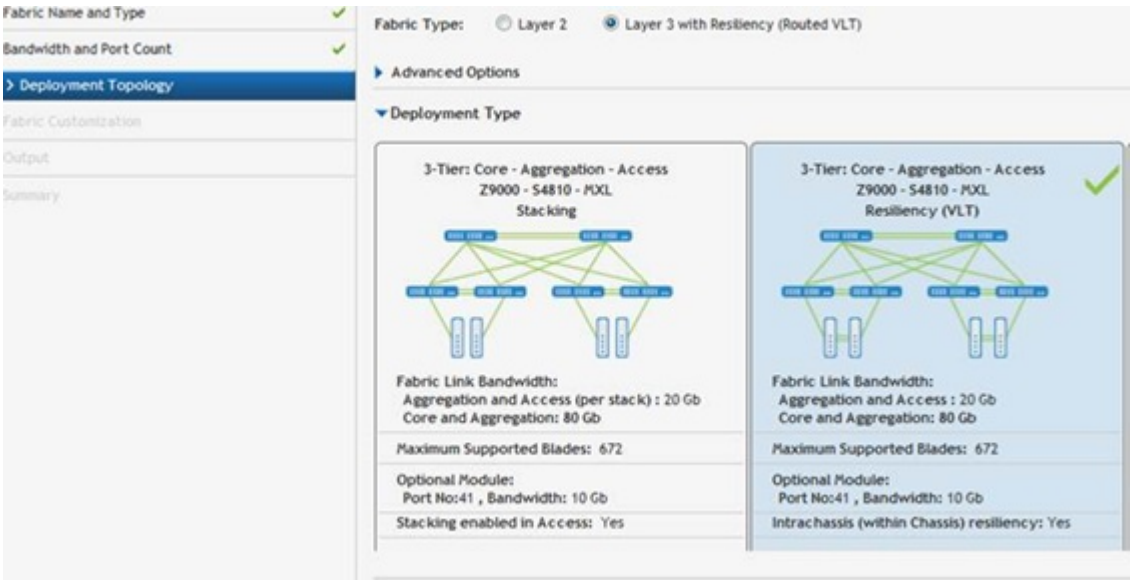


Figure 45. Tier 3 Layer 3 with Resiliency (Routed VLT) Blade MXL with IntraChassis option

Fabric Design – Step 3: Deployment Topology

The AFM displays applicable deployment topologies based your datacenter workload requirements specified in the **Fabric Name and Type** and **Bandwidth and Port Count** screens. By default, AFM selects

one of the topologies. Click the deployment topology filter icon on the top right of the screen to display additional deployment topology options. The output from these screens and the **Deployment Topology** and **Fabric Customization** screens create a network topology and the detailed wiring plan. See also Deployment Topology Use Cases.

Based on your design requirements you can create a 1, 2, or 3 tier topology as shown below

- **Tier 1 Topology** — Contains 2 switches and a downlink and uplink configuration. There are no fabric links.

Figure 46. VLT 1 Tier Topology: Aggregation Layer

For more information about the tier 1 topologies, see Designing a Layer 2 VLT and Layer 3 with Resiliency (Routed VLT) Fabric. See

- **Tier 2 Topology** — Contains 2 layers of switches, has fabric interlinks, uplinks and downlinks. Distributed Core (spine and leaf) or VLT (aggregation and access). For more information about tier 2 topologies, see Designing a Layer 2 VLT and Layer 3 with Resiliency (Routed VLT) Fabric and Selecting a Layer 3 Distributed Core Fabric Design.

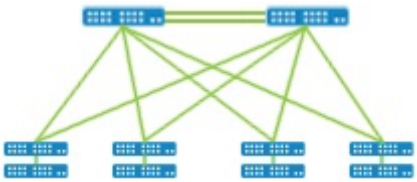


Figure 47. Tier 2 VLT Topology: Aggregation and Access Layer

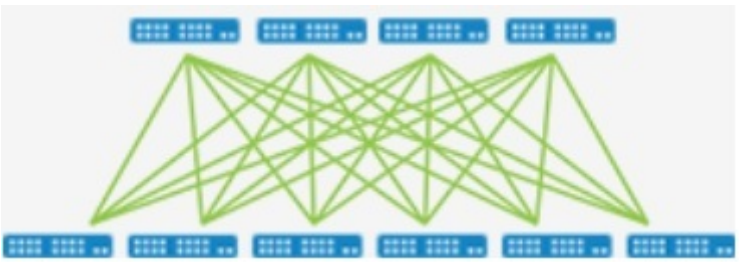


Figure 48. Tier 2 Distributed Core Topology: Spine and Leaf

- **Tier 3 Topology** — Layer 3 with Resiliency (Routed VLT) has 3 layers of switches, fabric interlinks, uplinks and downlinks. For more information about the tier 3 topologies, see Designing a Layer 2 VLT and Layer 3 with Resiliency (Routed VLT) Fabric .

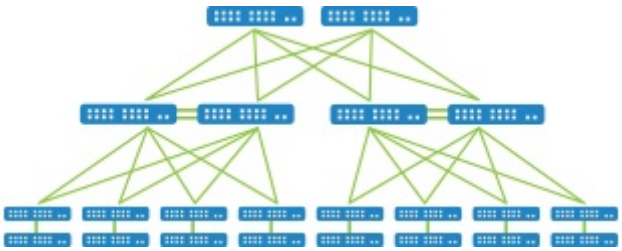


Figure 49. Tier 3 VLT Topology Core: Aggregation - Access Layer

The following illustration and table describes the deployment types for a fabric.

NOTE: For topologies, refer to the Designing a Layer 2 VLT and Layer 3 with Resiliency (Routed VLT) Fabric and Selecting a Layer 3 Distributed Core Fabric Design.

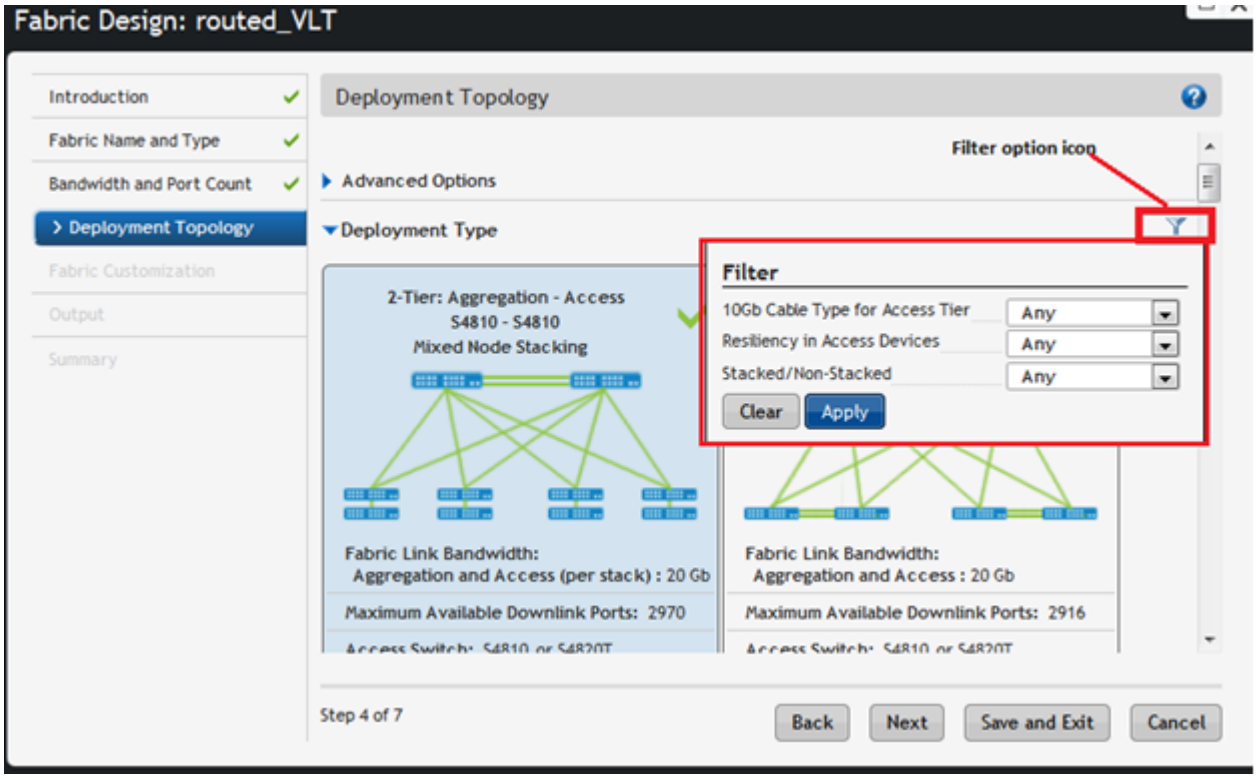


Table 18. Deployment Topology (Filter) Options

Deployment Options	Description
Over Subscription Ratio (Layer 3 distributed core deployment topology only)	For the layer 3 deployment the following over-subscription ratios are available: • 1:1 • 3:1 • 4:1 • 5:1

Resiliency in Access Devices	Configures Virtual Router Redundancy Protocol (VRRP) on the downlink.
10 Gb Cable Type for Access Tier	This option is applicable only for the topologies in which S4810 and S4820T can be swapped with each other. • **SFP+** • **RJ-45**
Stacked/Non-Stacked	Selects stacking for the topologies that are applicable. When you select stacking, you can use VLTi.
High Stream Buffering	• **high stream buffering** — The access layer uses S60 switches. • **low latency** — The access layer uses S55 switches
Resiliency In MXL (Routed VLT)	• **Intra-chassis** — Within the chassis (mVLT) • **Inter-chassis resiliency** — Across 2 chassis (VLT)

This section contains the following topics:

- (Optional) Configuring Advanced Options
- Selecting the Fabric Deployment Type

(Optional) Configuring Advanced Options

For a Layer 2 or Layer 3 with Resiliency (Routed VLT) fabric, you customize the bandwidth between the aggregation and access switches. When you configure the fabric link bandwidth between aggregation and access switches from the **Enabled Link Bandwidth Customization** option from the **Deployment Topology** screen, the bandwidth selected is shared equally by 2 redundant links. For example, if you select a fabric link bandwidth of 80 Gb between the aggregation and access switches, you can configure 40 GB for each redundant link on the **Fabric Customization** screen.

Attention: When you select LAN/SAN deployment with a iSCSI or fibre channel storage facing ports using the Fabric Designer wizard, AFM automatically selects a Layer 2 fabric. As a result, the Layer 2, Layer 3, and Layer 3 options in the **Deployment Topology** screen are **not** displayed.

To configure the deployment type so that you can customize the fabric link bandwidth between the aggregation and access switches:

1. In the **Deployment Topology**, check one of the following options:
   - **Layer 2**
   - **Layer 3 with Resiliency (Routed VLT)**
2. Check the **Enabled Link Bandwidth Customization** option.

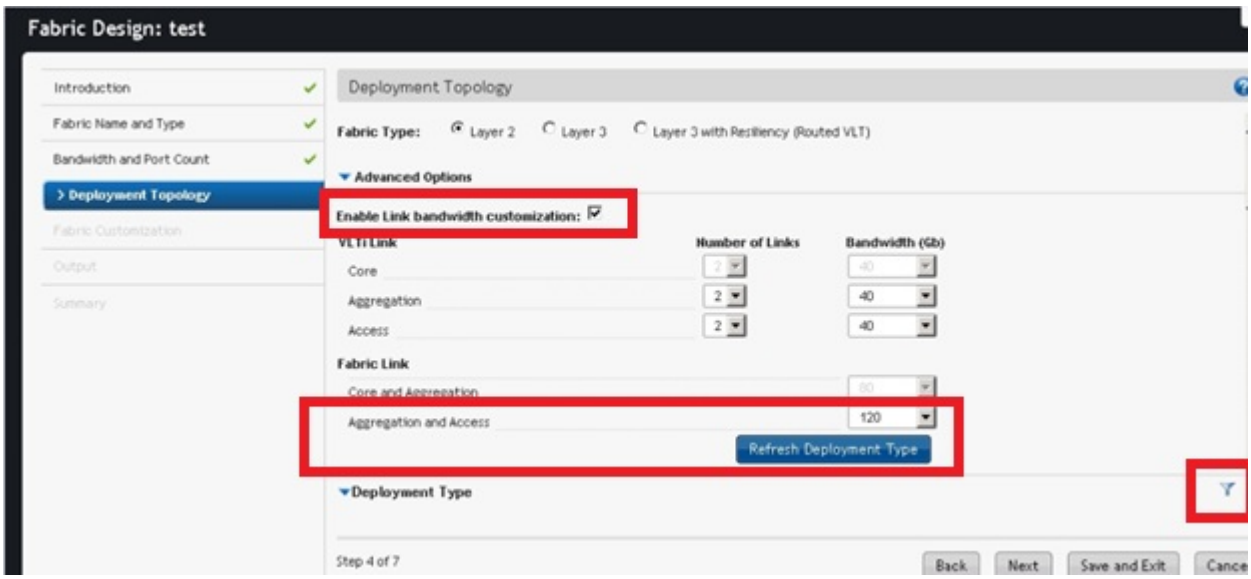


Figure 50. Enabled Link Bandwidth Customization Option

3. In the **Fabric Link Core Aggregation and aggregation and Access** option (only the applicable options for a select topology are configurable), select the fabric bandwidth value from the **Aggregation and Access** pull-down menu. For example, for 2 tier topology, selecting the **120 Gb** bandwidth option allows you to later customize the bandwidth from 20 to 120 Gb in increments of 20 Gb in the **Fabric Customization** screen.
4. Click the **Refresh Deployment Type** button.
5. On the **Deployment Type**, select the appropriate deployment type.
6. Click the deployment topology filtering icon on the top right of the screen to display deployment topology options. Only applicable options are displayed.
7. Configure the filter options for the deployment topology and click the **Apply** button.
8. Click the **Next** button to go to the **Fabric Customization** screen.
9. (Optional) From the **Fabric Link Bandwidth** pull-down menu, select the fabric link bandwidth for each switch that you want to customized.

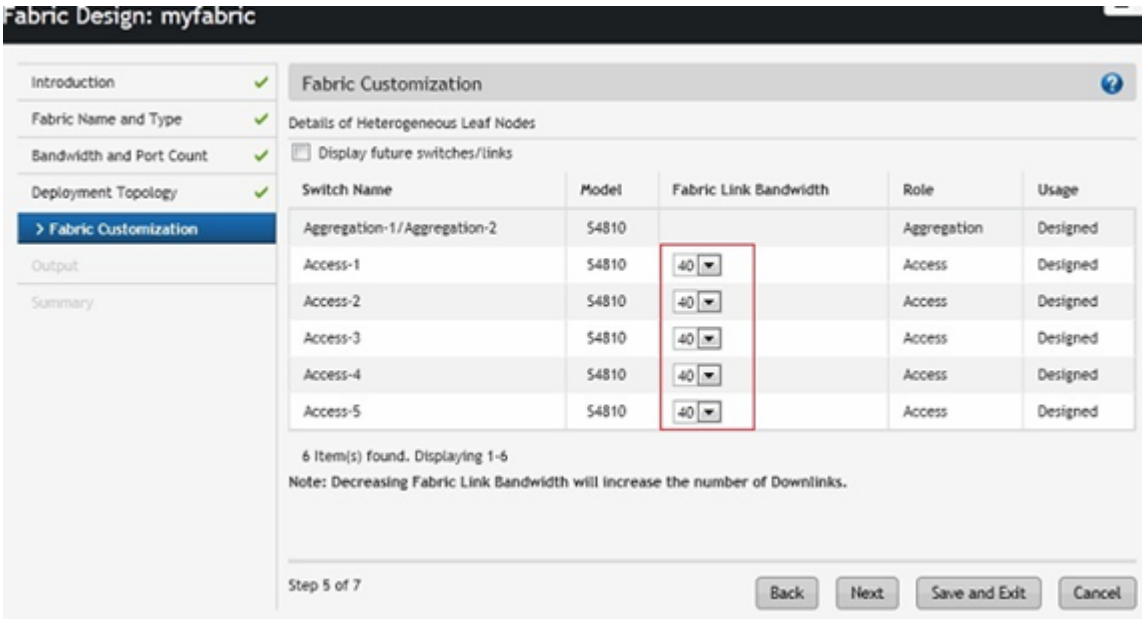


Figure 51. Customizing Fabric Link Bandwidth between Switches

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

Selecting the Fabric Deployment Type

To select the fabric deployment type:

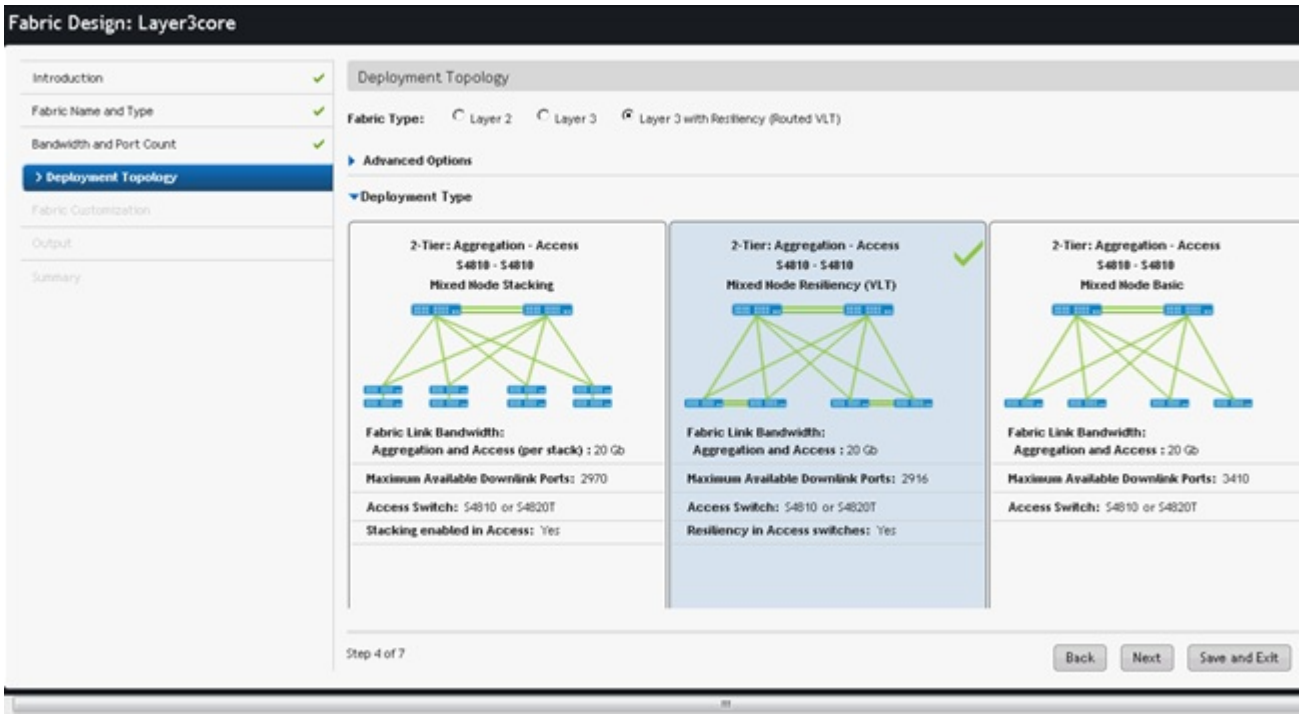
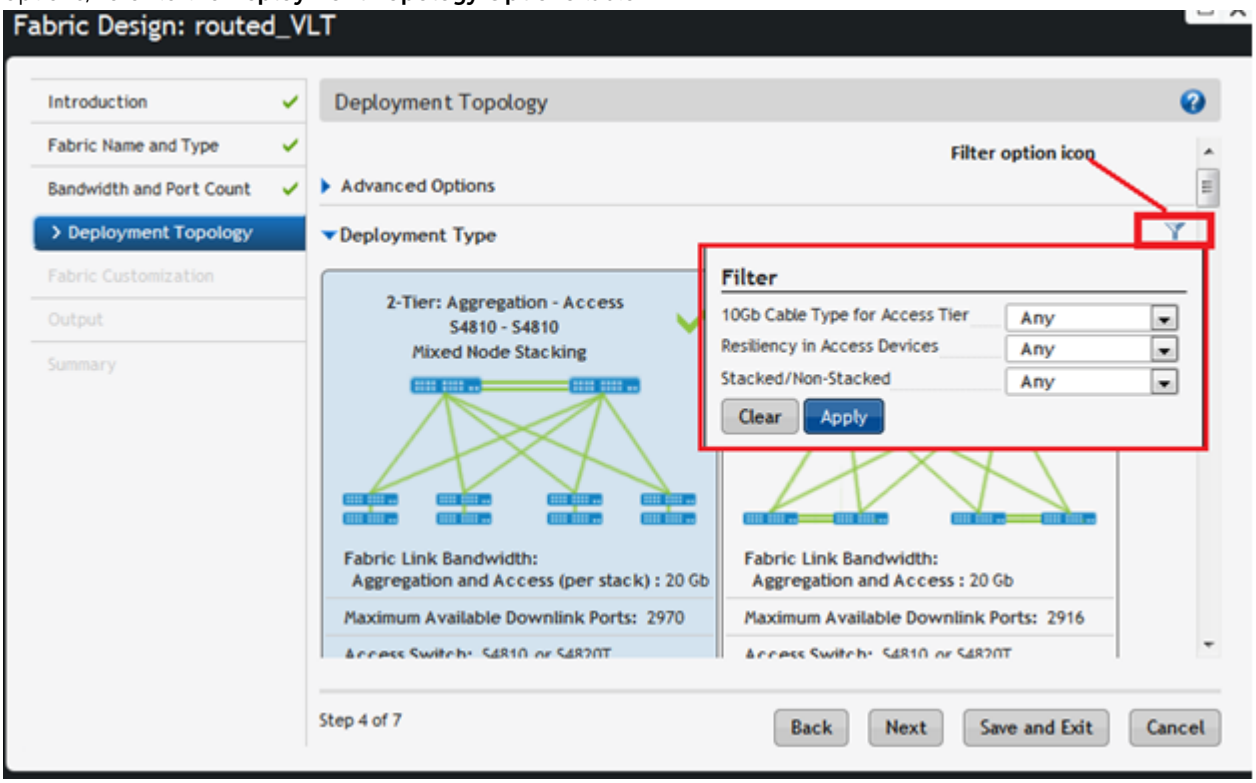


Figure 52. Layer 3 with Resiliency (Routed VLT) : Deployment Type screen

1. Navigate to the **Network** > **Design Fabric** > **New Fabric** > **Deployment Topology** screen.
2. In the **Fabric Type** area, select one of the following fabric types:
   a. **Layer 2** — Use the Layer 2 VLT fabric for workload migration over virtualized environments. See VLT and Selecting a Layer 2 VLT and Layer 3 with Resiliency (Routed VLT) Fabric Design.
   b. **Layer 3** — Use the Layer 3 distributed core for large fabric deployments. See Conventional Core Versus Distributed Core.
   c. **Layer 3 with Resiliency** (Routed VLT) — Use the Layer 3 fabric to extend equal cost multi-pathing capabilities. See Selecting a Layer 2 VLT and Layer 3 with Resiliency (Routed VLT) Fabric Design.

   Attention: When you select LAN/SAN deployment with a iSCSI or fibre channel storage facing ports using the Fabric Designer wizard, AFM automatically selects a Layer 2 fabric. As a result, the Layer 2, Layer 3, and Layer 3 options in the **Deployment Topology** screen are **not** displayed.
3. Click on the deployment topology that contains the appropriate core switches and aggregation switch type that you want in your fabric and for a Layer 3 distributed core fabric, the over-subscription ratio.

4. (Optional) Click the **Advanced Options** to configure VLTi links and fabric links.
   a. VLTi and Fabric Link options
      - **VLTi link**
        - **Core** — Specify the number of links and bandwidth.
        - **Aggregation** — Specify the number of links and bandwidth.
        - **Access** — Specify the number of links and bandwidth.
      - **Fabric Link**
        - **Core and Aggregation** — Specify the bandwidth.
        - **Aggregation and Access** — Specify the bandwidth.
   b. Click the **Refresh Deployment Type** button to apply the **Advanced Options** to view the new deployment topologies.
5. Click the deployment topology filter icon on the top right of the screen to display deployment topology options. Only applicable filter options are displayed. For a description about the filtering options, refer to the **Deployment Topology Options** table.



6. Configure the filter options for the deployment topology and click the **Apply** button.
7. Click the **Next** button to go to the **Fabric Customization** screen.

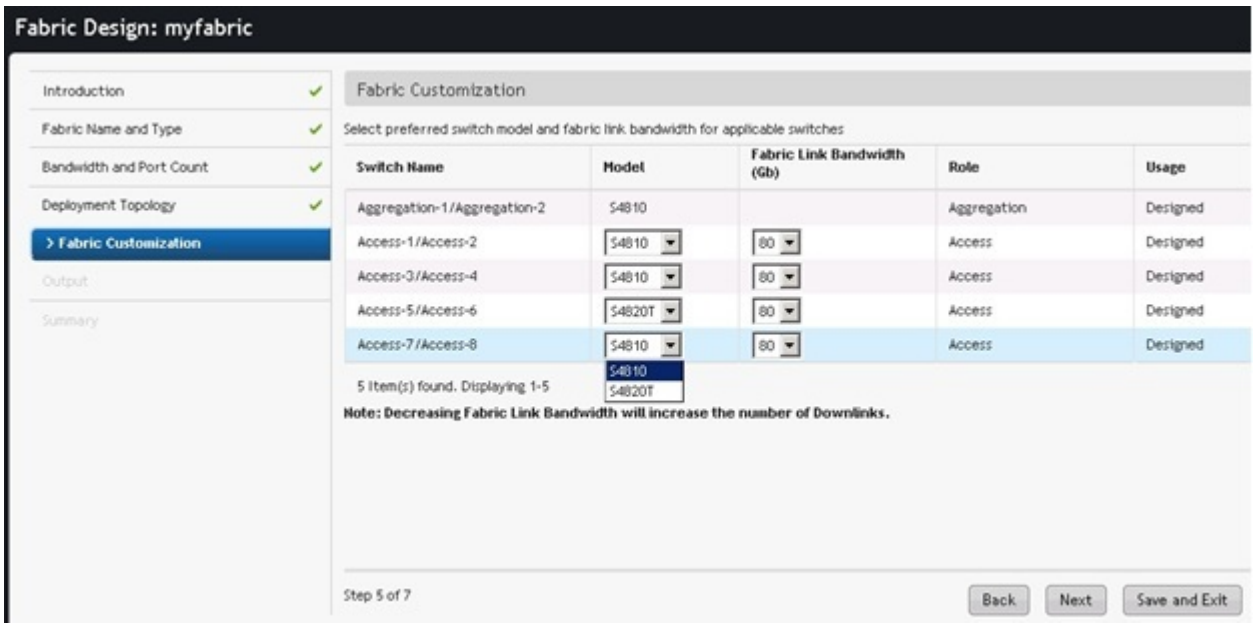
Fabric Design – Step 3: Fabric Customization

To modify the fabric link bandwidth (between the aggregation and access switches) for 2-tier and 3-tier fabrics, use the **Fabric Customization** screen. This screen displays the switch names, model, and switch role (spine, leaf, aggregation or access). For a Layer 2 or Layer 2 with Resiliency (Routed VLT) deployment topology, you can select S4810 or S4820T switches (mixed node) on the access side.

Pre-requisites

To use this feature, you must first configure the **Advance Configuration** option, **Fabric Link between Aggregation and Access**, to the maximum bandwidth for each access switch; for example, 120 Gb, at the **Network** > **Design Fabric** > **New Fabric** > **Deployment Topology** screen. If you do not configure this option, the **Fabric Customization** screen will be a read-only screen. For information about the **Advanced Options**, see the section at Configuring Advanced Options. For information about tiers, see Deployment Topology. See also Deployment Topology Use Cases.

1. Navigate to the **Network** > **Design Fabric** > **New Fabric** > **Deployment Topology** > **Fabric Customization** screen.
2. From the F**abric Link Bandwidth** pull-down menu, select the fabric link bandwidth for each access switch.



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

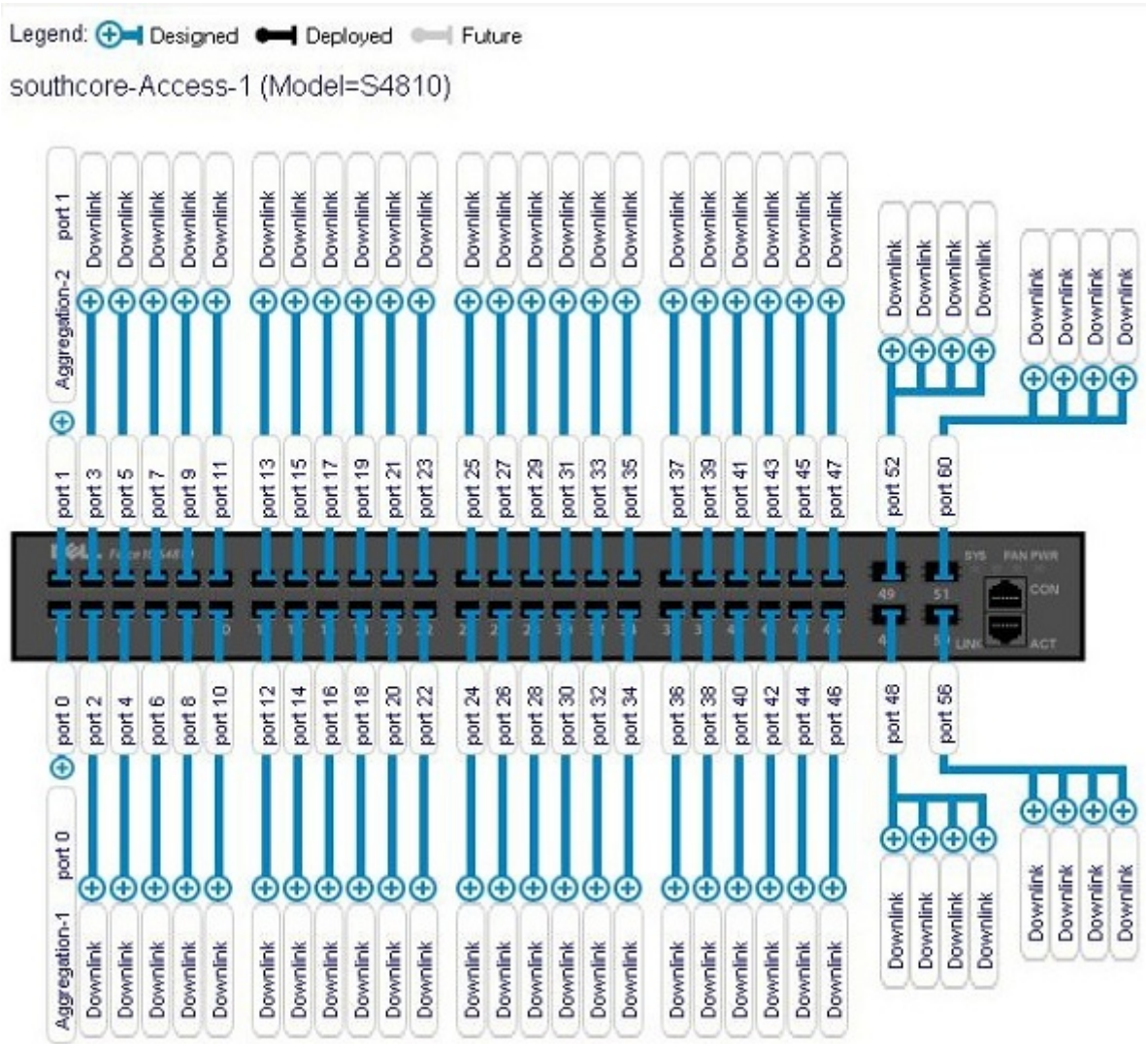
Fabric Design – Step 5: Output

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 fabric. Based on the configuration, the AFM calculates the number of switches required for the design and displays the physical wiring plan which you can export and print in PDF or Microsoft Visio® 2010. The wiring plans display the cabling maps (the connections between the switches) and the switches and links for current and future expansion. Review the wiring plan and then export it 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.

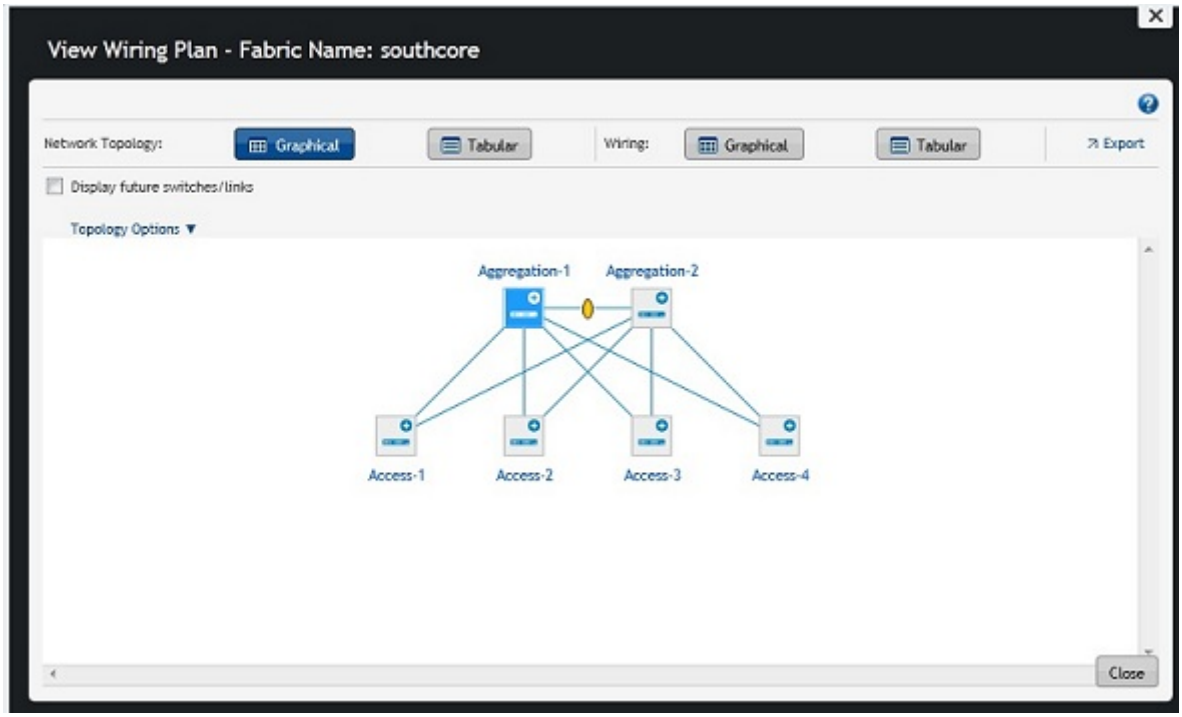
The fabric design is displayed in the following formats:

- **Graphical Wiring Plan** — Displays information about how the switches are connected graphically.



- **Network Topology** — Displays information about how the switches 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 switch, all the fabric interlinks are displayed. When you select a spine switch the links to the leaf switches are displayed. When you select an aggregation switch, the links to the access switches are displayed. Similarly, when you select a leaf switch, the links to the spine switches are displayed. When you select the access switches, the links to aggregation switches are displayed. When you select the core switches, the links to all the switches in the fabric (aggregation

and access) are displayed.



- **Tabular Wiring Plan** — Displays information about how the switches are connected in the fabric 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 in the fabric.

Wiring Plan

FROM SPINE	FROM PORT	TO LEAF	TO PORT	LINK TYPE	USAGE STATUS
southcore-Aggregation-1	0/0	southcore-Access-1	0/0	Fabric Link	Designed
southcore-Aggregation-1	0/1	southcore-Access-2	0/0	Fabric Link	Designed
southcore-Aggregation-1	0/2	southcore-Access-3	0/0	Fabric Link	Designed
southcore-Aggregation-1	0/3	southcore-Access-4	0/0	Fabric Link	Designed
southcore-Aggregation-1	0/48	southcore-Aggregation-2	0/48	VLTi Link	Designed
southcore-Aggregation-1	0/52	southcore-Aggregation-2	0/52	VLTi Link	Designed
southcore-Aggregation-2	0/0	southcore-Access-4	0/1	Fabric Link	Designed
southcore-Aggregation-2	0/1	southcore-Access-1	0/1	Fabric Link	Designed
southcore-Aggregation-2	0/2	southcore-Access-2	0/1	Fabric Link	Designed
southcore-Aggregation-2	0/3	southcore-Access-3	0/1	Fabric Link	Designed

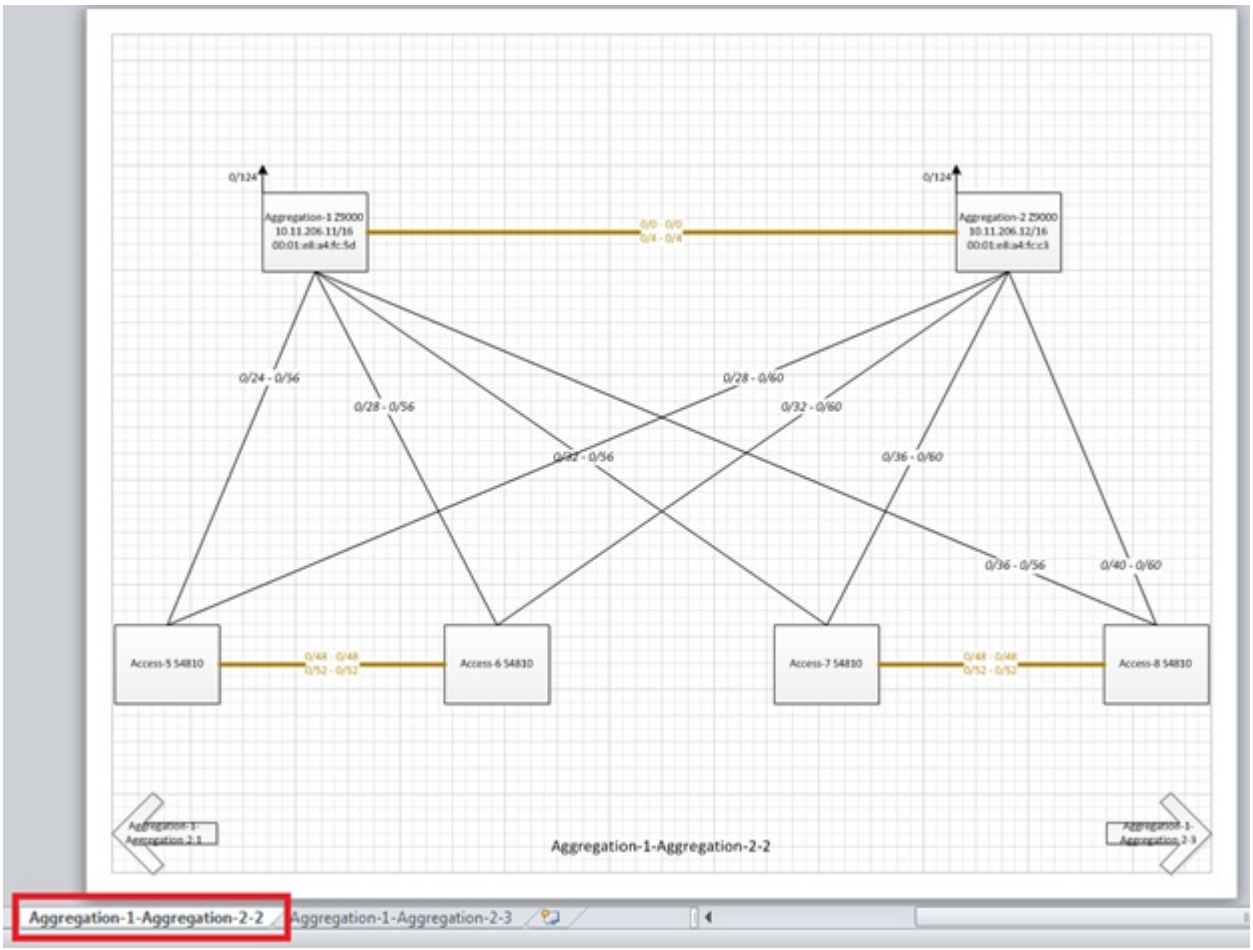


Figure 53. Example: Visio Output

Table 19. Tabular Wiring Plan Output Descriptions

Field Name	Description
From Device (Switch)	Displays the name of the device — from the side.
From Port	Displays the port number on the switch — from the side.
To Device (Switch)	Displays the name of the device— to the side.
To Port	Displays the port number on the device — 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 and future 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: **Wiring** (Graphical or Wiring) , or **Network Topology** (Graphical or Tabular format).

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.
5. Click the **Generate** button.

Fabric Design – Step 6: Summary

The **Summary** screen displays a summary of your fabric design.

To export the fabric design:

1. Click one of the following export options:
   - **Export Wiring Plan**
   - **Export Summary**
   - **Export Design**
2. Select a display format: **PDF** (**Table Data**, **Graphical Wiring Plan**, **Both**) or **Visio**.
3. Click the **Generate** button.
4. Carefully review the design before you commit the changes.
5. Click **Finish** to commit your changes.

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 provided from Dell manufacturing, if available. If not available, consult Dell customer support. If you do not have this file, record the system MAC addresses of the switches in the fabric so that you can then map (associate) the address to the appropriate switch before you rack the switches.
5. Print out the wiring plan and use it 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. 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** screen.
2. Select the **Design Fabric** tab.
3. Select the fabric to delete.
4. Click the **Delete Fabric** link.

Viewing the Wiring Diagram

To view and export the wiring diagram of the fabric:

1. Navigate to the **Network** > Design Fabric screen.
2. Select the fabric and then 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**
   d. **Network Topology Tabular Plan**
5. Click the **Export** link to export the wiring plan.

9

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 deploys the configuration to the switches in the fabric. You can deploy auto-generated and custom configurations. This screen contains the following options:

- **Deploy Fabric** — Prepares the fabric for deployment and deploys the fabric.
  - Pre-deployment Configuration

    For information about using the pre-deployment wizard for an IOA fabric, see IOA Pre-deployment Wizard
  - 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. For information about using the pre-deployment wizard for an IOA fabric, see IOA Pre-deployment Wizard.

Fabric Deployment Summary

Switch Configuration Phases and States

Table 20. 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 21. 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

Pre-deployment Configuration

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. Protocol Configuration for a Layer 2 VLT fabric: **Step 1**
   - Pre-deployment – Step 1a: Uplink Configuration
   - Pre-deployment – Step 1b: VLAN Configuration
   - Pre-deployment – Step 1c: Port Channel Configuration
   - Pre-deployment – Step 1d: Storage Facing Ports
   - Pre-deployment – Step 1e: VLAN Mapping
2. Pre-deployment – Step 2: Assign Switch Identities
3. Pre-deployment – Step 3: Management IP
4. Pre-deployment – Step 4: SNMP and CLI Credentials
5. Pre-deployment – Step 5: Software Images
6. Pre-deployment – Step 6: DHCP Integration
7. Pre-deployment – Step 7: Summary

IOA Fabric Pre-deployment

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

1. Pre-deployment IOA – Step 1: Management IP
2. Pre-deployment IOA – Step 2: VLAN Configuration
3. Pre-deployment IOA – Step 3: SNMP and CLI Credentials
4. Pre-deployment IOA – Step 4: Software Images
5. Pre-deployment IOA – Step 5: 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. Protocol Configuration for Layer 3 fabric: **Step 1**
    - Pre-deployment – Step 1a: Fabric Link Configuration
    - Pre-deployment – Step 1b: Uplink Configuration
    - Pre-deployment – Step 1c: Downlink Configuration
2. Pre-deployment – Step 2: Assign Switch Identities
3. Pre-deployment – Step 3 Management IP
4. Pre-deployment – Step 4: SNMP and CLI Credentials
5. Pre-deployment – Step 5: Software Images
6. Pre-deployment – Step 6: DHCP Integration
7. Pre-deployment – Step 7: Summary

Layer 3 with Resiliency (Routed VLT) Pre-deployment

To prepare the with Resiliency (Routed VLT) fabric for deployment, complete the following tasks using the **Pre-deployment Configuration** wizard.

1. Protocol Configuration for Layer 3 fabric: **Step 1**
    - Pre-deployment – Step 1a: Fabric Link Configuration
    - Pre-deployment – Step 1b: Uplink Configuration
    - Pre-deployment - Step 1c: VLAN Configuration
    - Pre-deployment – Step 1d: Port Channel Configuration
    - Pre-deployment – Step 1e: VLAN Mapping
2. Pre-deployment – Step 2: Assign Switch Identities
3. Pre-deployment – Step 3 Management IP
4. Pre-deployment – Step 4: SNMP and CLI Credentials
5. Pre-deployment – Step 5: Software Images
6. Pre-deployment – Step 6 DHCP Integration
7. Pre-deployment – Step 7: Summary

IOA Pre-deployment Wizard

IOA Pre-Deployment Screens

Use the following IOA **Pre-deployment** screens to provide the fabric the minimum configuration for a IOA fabric. These screens automate the IOA deployment process. See also Using the Pre-deployment Configuration Wizard.

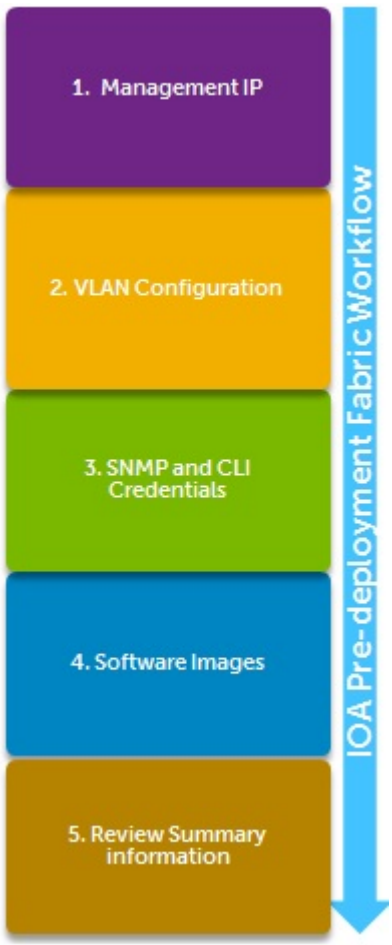


Figure 54. IOA Pre-deployment Workflow

- **Management IP** — Displays all the IOA blades available in the discovered chassis. If the discovered chassis is configured with an IP address, AFM populates with the IP address that you can edit.
- **VLAN Configuration** — Apply a VLAN to the Layer 2 VLT. Include at least one VLAN configuration.
- **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.
- **SNMP and CLI Credentials** — Configures SNMP and CLI credentials at the fabric level. Configure SNMP so that AFM can perform SNMP queries on the switches in the fabric. It is prepopulated with default IOA credentails - **root/calvin.**

- **Summary** — Displays the fabric name and location of the software image.

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

- Pre-deployment IOA - Step 1: Management IP
- Pre-deployment IOA - Step 2: VLAN Configuration
- Pre-deployment IOA - Step 3: SNMP and CLI Credentials
- Pre-deployment IOA - Step 4: Software Images
- Pre-deployment IOA - Step 5: Summary

For information about IOA pre-deployment error messages, see IOA Pre-deployment Error Messages.

Pre-deployment (IOA) – Step 1: Management IP

Before you begin:

1. Review the IOA Pre-deployment Wizard information.
2. Insert the IOA blade switch into the M1000e chassis.
3. Make sure that the IOA blade switch is in standalone mode (default mode) using the following FTOS CLI command:

   show system stack-unit <*unit-number*> **iom-mode**

   For more information about this command, see the *Dell PowerEdge Command Line Reference Guide for the M I/O Aggregator*.
4. Obtain the Chassis Management Controller (CMC) M1000e chassis IP address. Use this address to discover all the IOA switch blades in the CMC chassis.

   NOTE: For a description of each IOA Pre-deployment screen, see IOA Pre-deployment Wizard

To assign a management IP address to IOA blade switch deployment, use the Management IP screen.

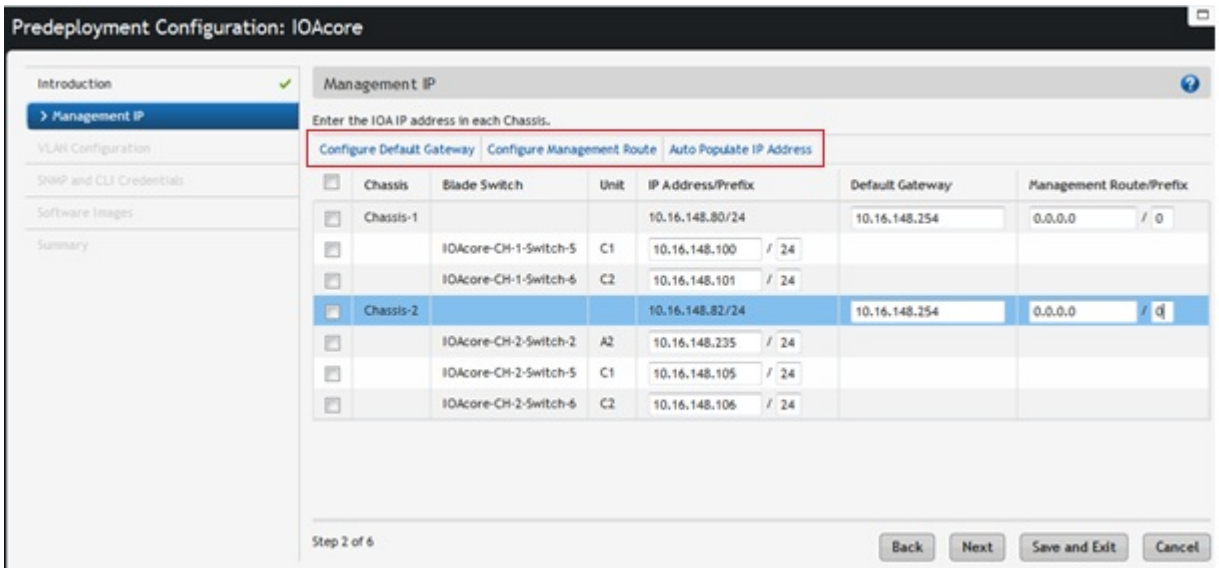


Figure 55. IOA Pre-deployment Management IP Address Screen

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 pre-deployment **Introduction** screen displays.
3. In the **Introduction** screen, review the useful information that you need to gather before you begin.
4. Click the **Auto Populate IP Address** link and in the **Start IP Address/Prefix** field enter the starting IP address and prefix.
5. Click the **Configure Default Gateway** link and then enter the address of the default gateway for the management interface.
6. Click the **Configure Management Route** link and enter the IP address used by the management route and enter the gateway prefix in the field after the slash.
7. Click the **Next** button to go to the **VLAN Configuration** screen.

Pre-deployment (IOA) – Step 2: VLAN Configuration

To specify a VLAN to be applied to the Layer 2 fabric manually or automatically for an IO Aggregator (IOA) blade deployment:

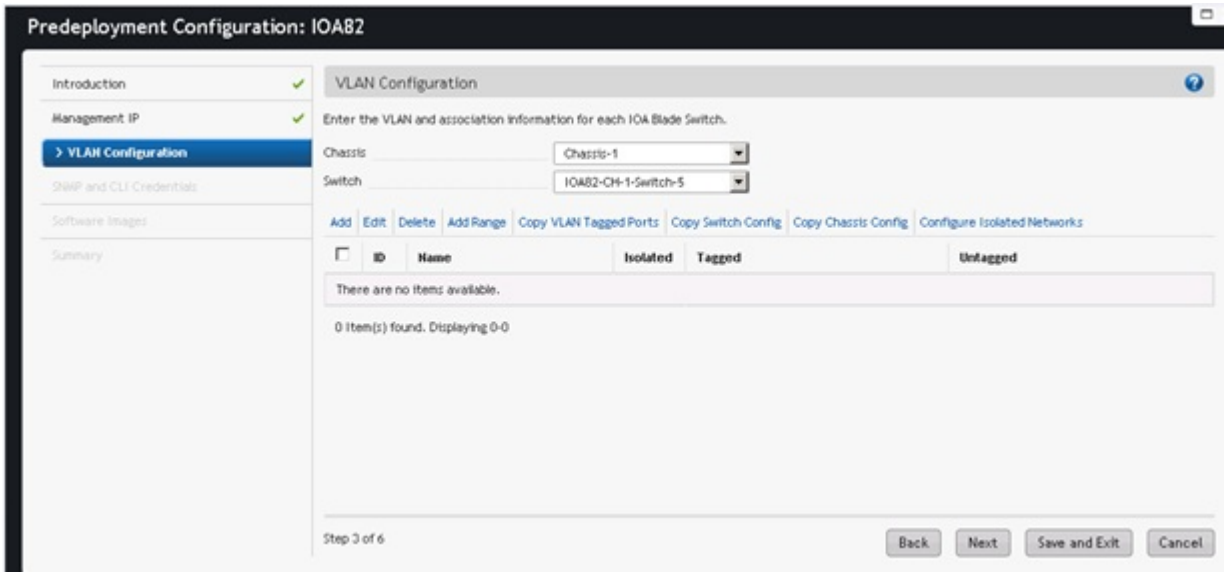


Figure 56. IOA Pre-deployment VLAN Configuration

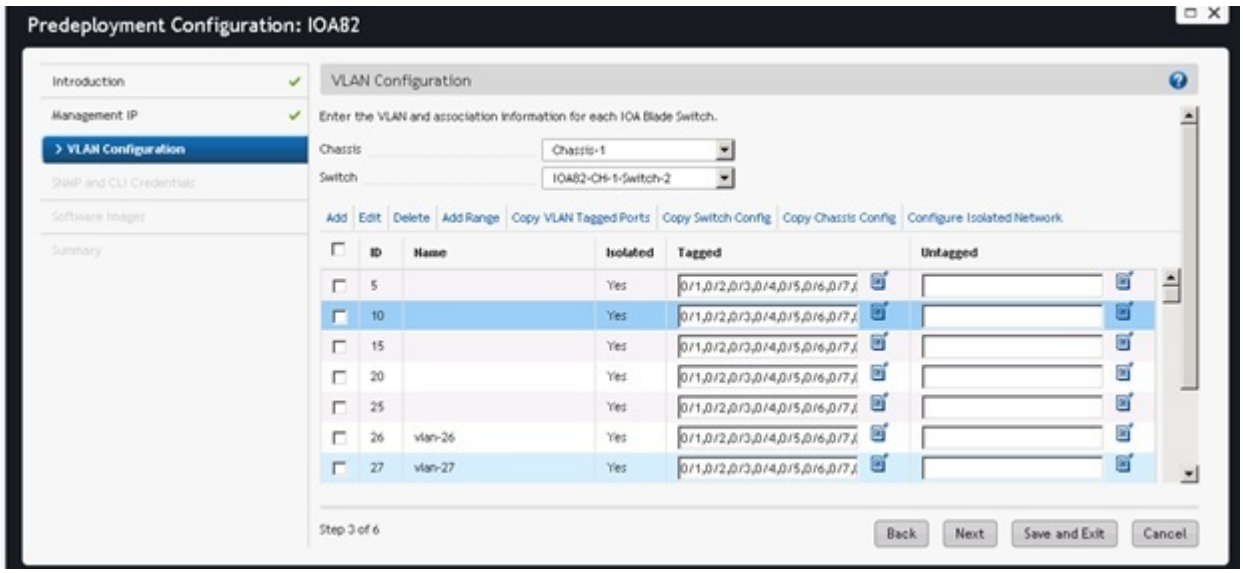
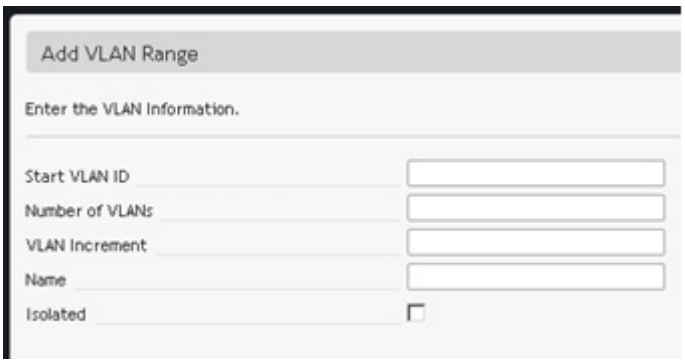
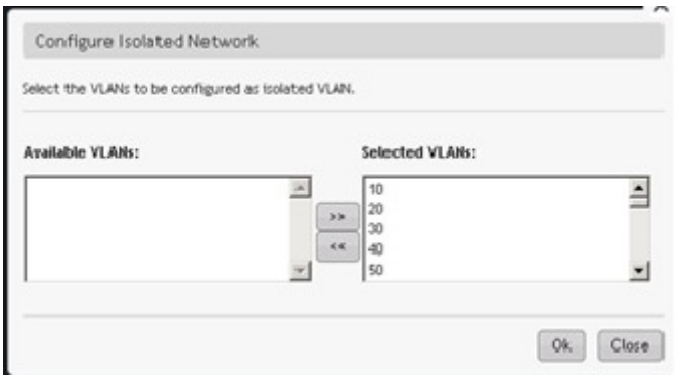


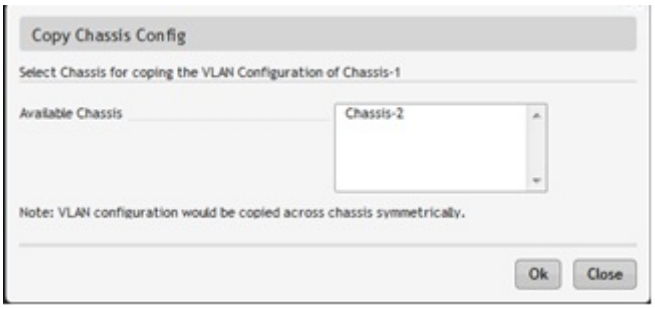
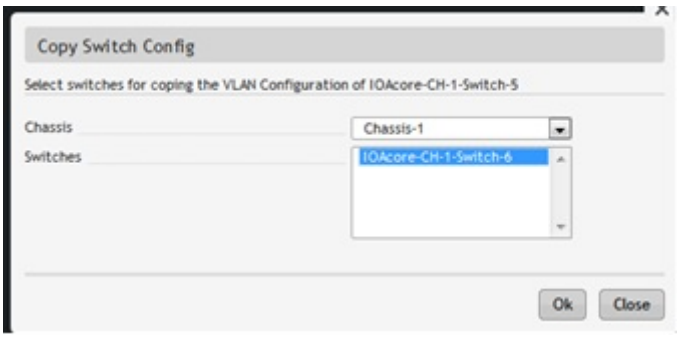
Figure 57. IOA Pre-deployment VLAN Configuration with Populated Data

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 pre-deployment **Introduction** screen displays.
3. Navigate to the **VLAN Configuration** screen.
4. From the **Chassis** pull-down menu, select a chassis name that you want to configure.

5. From the **Switch** pull-down menu, select the name of the switch that you want to configure.
   The following Pre-deployment IOA VLAN configuration options are available:

Table 22. IOA VLAN Pre-deployment Options

VLAN Option	Description
Add VLAN	Creates a VLAN. The range is from **2** to **4094**.  NOTE: VLAN ID **1003** is reserved.
Add VLAN Range	Creates a VLAN range. 
Configure Isolated Network	Provides security that can be enabled on a a VLAN or a range of VLANs. Only standalone mode is supported. For more information about this option, see Isolated Networks. 

Copy Chassis Configuration	Copies the chassis configuration from the current chassis to another chassis in the fabric. **NOTE:** The VLAN configuration is copied symmetrically to the new chassis. For example, the port assigned as Port 1 on the source chassis is also assigned as Port 1 on the destination chassis. 
Copy Switch Config	Copies IOA VLAN configuration to any IOAs inserted in same or different M1000e chassis. 
Copy VLAN Tagged Ports	Copies the VLAN tagged port configuration from a selected port to other port (s) within a switch.
Edit	Edits the VLAN configuration.
Delete	Removes the VLAN configuration.

6. Click the **Next** button to go to the **SNMP and CLI Credentials** screen.

Isolated Networks

Isolated networks is a security feature that can be enabled on a a VLAN or a range of VLANs. Only standalone mode is supported (there is only one single LAG uplink).

When you enable this feature:

- Server-to-server communication is disabled on the isolated network enabled VLANs.
- Servers on those VLANs can only communicate through the uplink LAG (Core).
- The uplink core (TOR) applies all the required security measures and other services before it switches or routes the traffic.

- The VLAN is configured only on the server side interfaces, which is specified as the isolated network. All traffic coming arriving on this interface from the server is sent out to the associated uplink.
- Multiple servers belonging to the same VLAN **cannot** communicate with each other over the IO Aggregator (IOA) because all the traffic is sent to the single uplink LAG and is "not" switched locally
- For security, unknown unicast and multicast traffic received at the IOA uplink LAG is blocked towards the server side interfaces over that VLANs that have isolated network feature enabled.

The following illustration shows multiple servers (server M620A and server M620B) belonging to the same VLAN (VLAN 5). For security, the servers cannot communicate with each other over the IO Aggregator because all the traffic is sent to the single uplink LAG (ToR) and is "not" switched locally. There is no switching between the server ports.

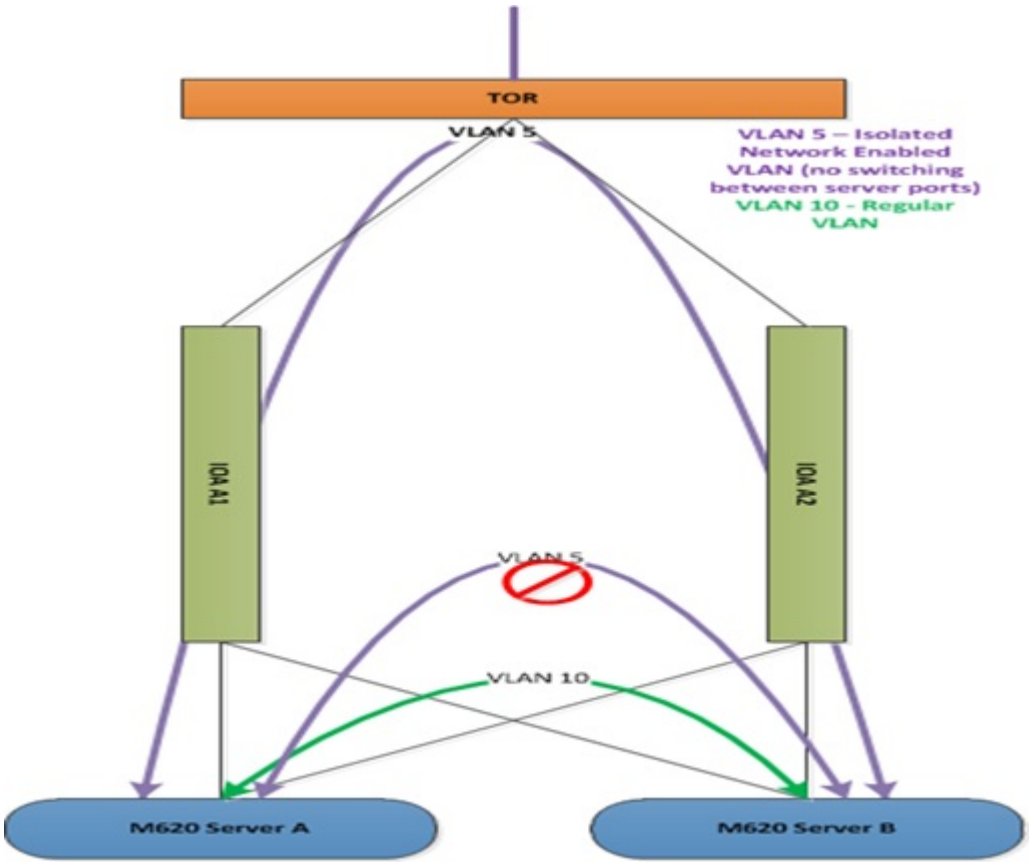


Figure 58. Isolated Networks Enabled on VLAN 5

Pre-deployment (IOA) — Step 3: 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 from this site. To change the address of the TFTP or FTP site, navigate to the **Administration** > **Settings** > **TFTP/FTP** 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.

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.

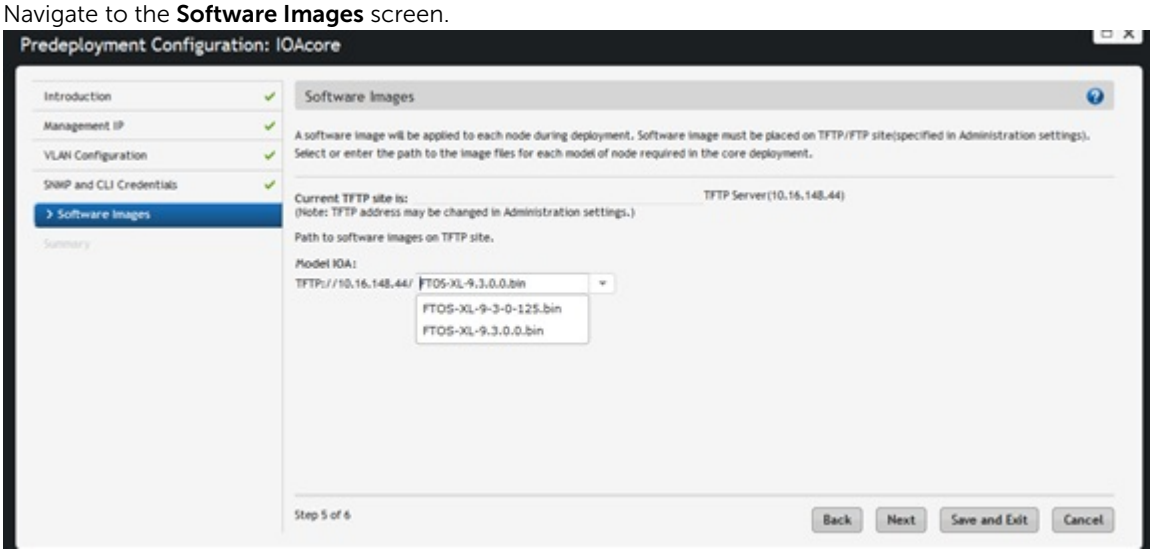


Figure 59. IOA Pre-deployment Software Images Screen

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 **Summary** screen.

Pre-deployment (IOA) – Step 4: SNMP and CLI Credentials

Configure SNMP and CLI credentials at the fabric level. Configure SNMP so that the AFM can perform SNMP queries on the switches in the fabric.
To configure SNMP and CLI Credentials for an IOA blade deployment:

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 **SNMP and CLI Credentials** screen.

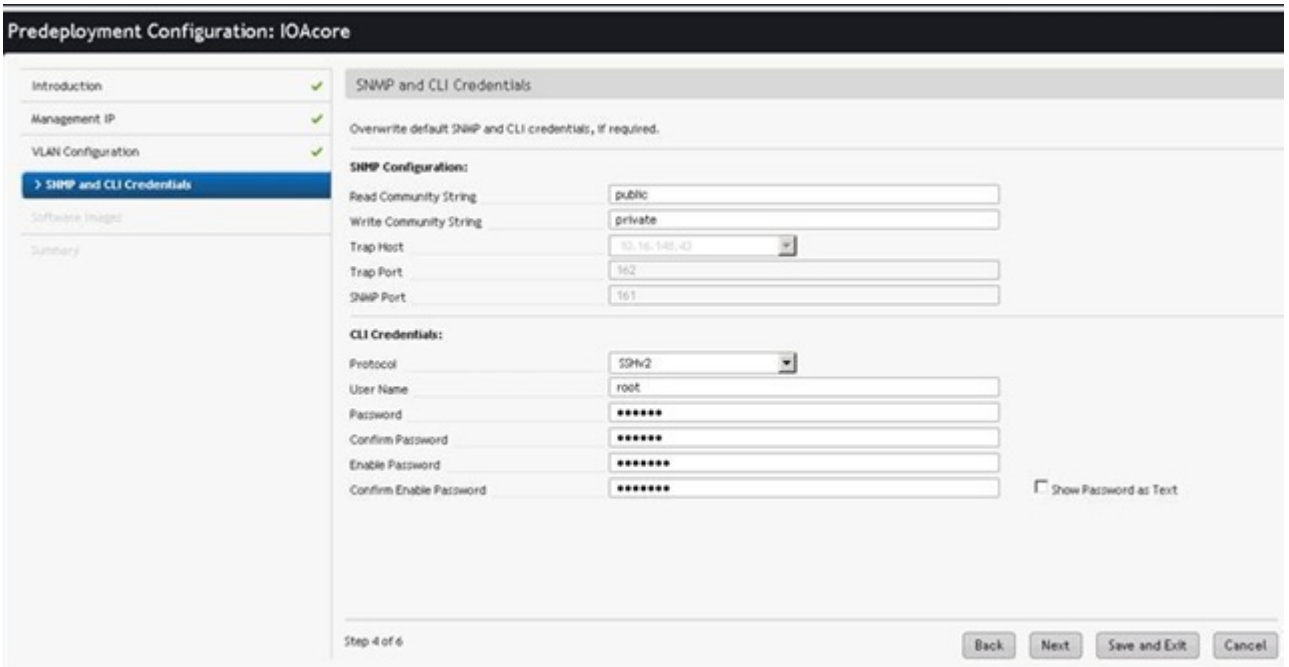


Figure 60. IOA SNMP and CLI Credentials Screen

4. In the **Read Community String** field, enter the read community string; for example, "public".
5. In the **Write Community String** field, enter the write community string; for example, "private".
6. From the **Protocol** pull-down menu, select one of the following protocols: **Telnet** or **SSHv2**.
   Note: AFM populates the default IOA credential with **root/calvin**.
7. In the **User Name** field, enter the user name.
8. In the **Password** field, enter the password.
9. In the **Confirm Password** field, enter confirm the password.
10. In the **Enable Password** field, enter the enable password.
11. In the **Confirm Enable Password** field, confirm the enable password
12. Click the **Next** button to go to the **Summary** screen.

Pre-deployment (IOA) – Step 5: Summary

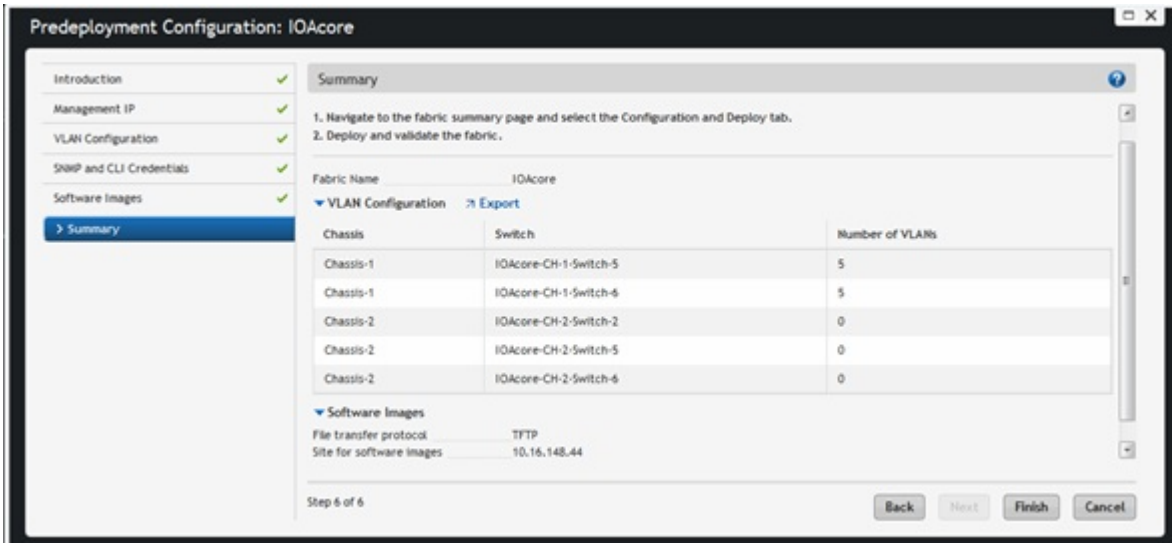
Use the **Summary** screen to review the IOA pre-deployment configuration. This screen displays the specified IP and protocol settings for the fabric, uplink, and downlink configuration. It also displays the software image information for each type of switch and configuration file transfer status to the remote or local TFTP or FTP server.

To view the pre-deployment IOA Summary screen:

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. Review the IOA pre-deployment summary information. To export configure VLAN information, click the **Export** link.

Figure 61. IOA Pre-deployment Summary Information



5. Click the **Finish** button.

Next Steps

a. Deploy the IOA switches from the **Network** > *Fabric* > **Configuration and Deploy** > **Deploy and Validate** > **Deploy** screen.

NOTE:
Before you deploy the IOA switches, make sure that the IOA switches are standalone mode using the following FTOS CLI command:

show system stack-unit <*unit-number*> **iom-mode**

For more information about this command, see the *Dell PowerEdge Command Line Reference Guide for the M I/O Aggregator*.

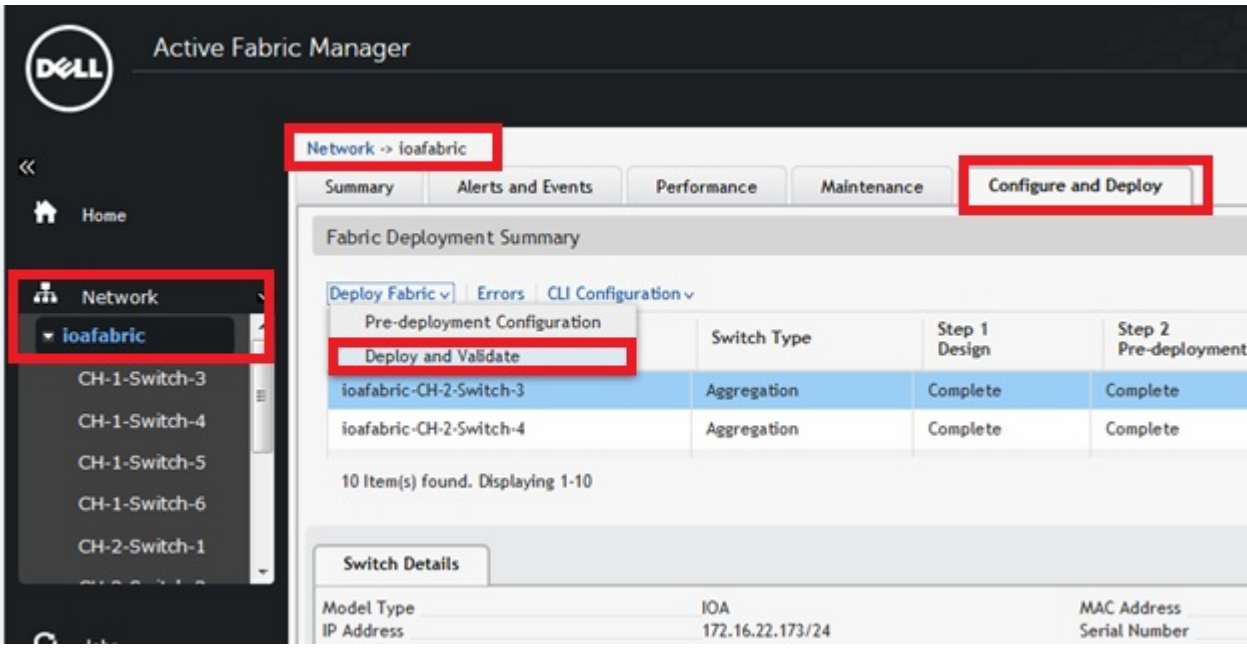


Figure 62. IOA Deploy and Validate

b. During deployment, check for IOA deployment failures such as **Not being in Standalone Mode** in the **Response Actions** column. To correct this issue, set the IOA to standalone mode and then redeploy it. For information about IOA pre-deployment error messages, see IOA Pre-deployment Error Messages.

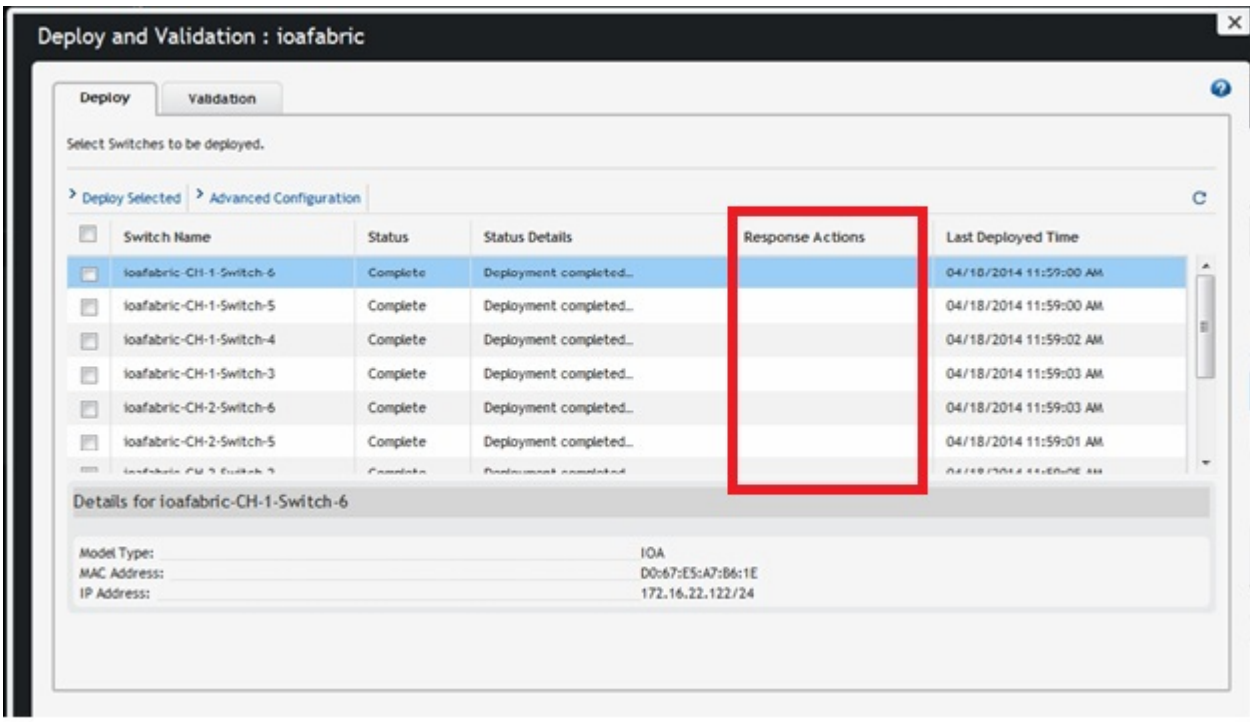


Figure 63. Deploy IOA Fabric and Check for Response Actions

IOA Pre-deployment Error Messages

Use the following table to troubleshoot the IOA pre-deployment.

Error	Recommended Action
Discovered MAC is different from planned MAC	Make sure the MAC provided for this device is correct.
Discovered model is different from planned model	Make sure the model provided for this device is correct.
IOA is not in standalone mode	Put the IOA in standalone mode.
IOA Software Upgrade task: Failed	• Power cycle device • Make sure the image is present in TFTP or FTP site • Verify Telnet/SSH connectivity from AFM server and deploy again
Ping verification: Failed	From the AFM server, verify reachability to the IOA device
Telnet/SSH session verification: Failed	Make sure Telnet/SSH session available from the AFM server has the correct credentials.
Racadm Set IP error - The specified switch operation is not supported by stacked switches	Change the switch mode to standalone mode and then complete predeployment.

Unable to get the MAC Address through Racadm	Verify that the chassis/device is reachable and then rediscovery it.
Unable to set the Management IP in IOA device	Verify that the chassis/device is reachable or a valid management IP/subnet mask/gateway IP is specified.
Unable to upgrade required software version	Make sure the IOA using the required software release

VLT/Distributed Core Pre-Deployment Wizard

To prepare the VLT or Distributed Core 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.

Attention: If you are designing a fabric using an IOA blade switch, see IOA Pre-deployment Wizard.

Prerequisites

Before you begin:

1. Rack the equipment in the fabric.

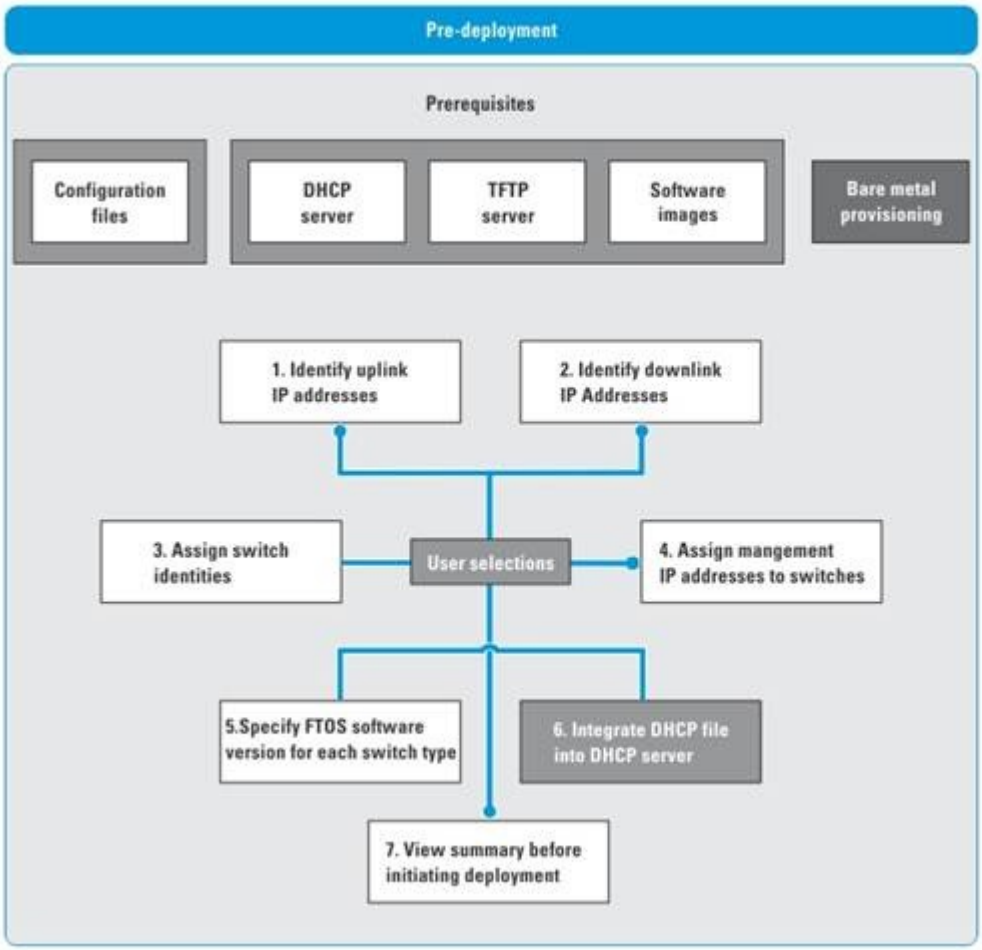
   NOTE: Before racking the switches, make sure that you have the **.csv** file that contains the system MAC addresses for each switch in the fabric. If you do not have this file, record the system addresses before you rack the switches.

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 Gathering Useful Information for a Layer 2 VLT Fabric, or Gathering Useful Information for a Layer 3 with Resiliency (Routed 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 Prerequisites.

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.

- **Assign Switch Identities**— Assigns a system media access control (MAC) address to each switch in the fabric. You can optionally assign serial numbers and service tags to each switch.
- **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.
- **VLAN Mapping** — (for a Layer 2 VLT fabric or Layer 3 with Resiliency (Routed VLT)) Associates each of the ports of a access switch to one or more VLANs. You can associated one or more tagged VLANs and for an untagged VLAN only one is allowed.

- **Downlink Configuration** — (for a Layer 3 Distributed Core or Layer 3 with Resiliency (Routed VLT) fabric) An edge port that connects to the access layer; for example, servers or a ToR.
- **Fabric link Configuration** — (for a Layer 3 or Layer 3 with Resiliency (Routed VLT) fabric. For a Layer 3 fabric, configures options for the spine and leaf to communicate in the fabric. For a Layer 3 with Resiliency (Routed VLT) fabric, the links that connect the core, access, and aggregation switches in the fabric.
- **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.
- **Output** — Displays the uplink and downlink configuration on the leaves or access. Verify that this information is correct before deploying the switches.
- **Port Channel Configuration** — Add, edit, delete, and automatically populate the port channel configuration. You can also copy a switch port channel configuration onto another port.
- **SNMP and CLI Credentials** — Configures SNMP and CLI credentials at the fabric level. Configure SNMP so that the AFM can perform SNMP queries on the switches in the fabric.
- **Summary** — Displays the fabric name, location of the software image, and DHCP configuration file.
- **VLAN Configuration** — Specify a VLT VLAN to be applied to the Layer 2 VLT or Layer 3 with Resiliency (Routed VLT) fabric. Include at least one VLAN configuration.
- **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 or Layer 3 with Resiliency (Routed VLT), an edge port link (uplinks) on the first two aggregation devices that connect outside the fabric.

Protocol Configuration — Layer 2 VLT Fabric: Step 1

The pre-deployment protocol configuration for Layer 2 fabric consists of the following tasks.

NOTE:

Before you begin, review the pre-deployment workflow for a Layer 2 fabric at Using the Pre-deployment Configuration Wizard.

- Pre-deployment – Step 1a: Uplink Configuration
- Pre-deployment – Step 1b: VLAN Configuration
- Pre-deployment – Step 1c: Port Channel Configuration
- Pre-deployment – Step 1d: Storage Facing Ports

  (For LAN\SAN deployments only)
- Pre-deployment – Step 1e: VLAN Mapping

NOTE: For pre-deployment, the Layer 2 VLT and Layer 3 Distributed Core fabrics use the same pre-deployment configuration screens from step 2 through step 7.

Pre-deployment – Step 1a: Uplink Configuration

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.

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

Figure 64. 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 **Type of Uplink Ports** area, select one of the following options:
   - **static routes —** When you select the **static routes** option, AFM displays the **Adds Static Route** window. You can configure up to 10 static routes for each aggregation device. When you check the of **Default Route** option , AFM automatically populates the destination network field to **0.0.0.0/0**. For static routes, enter the destination network and the next hop.
   - **L2** — Configures Layer 2 uplinks for a Layer 2 fabric.
   - **L3** — Configures uplinks for a Layer 2 VLT or Layer 3 Distributed Core fabric. When you select the **L3** option, the **Uplink Configuration** screen displays additional options to configure the Layer 3 protocol settings.
5. (Layer 3 uplinks only) In the **Protocol Settings**, select a routing protocol (OSPF, IBGP, or eBGP) or static route for the edge port uplinks. The **Bandwidth and Port Count** 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.
6. In the **Loopback IP Address Range/Prefix**, enter the loopback IP address and prefx.
7. Click **Next** to go the **VLAN Configuration** screen.

Pre-deployment - Step 1b: VLAN Configuration

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

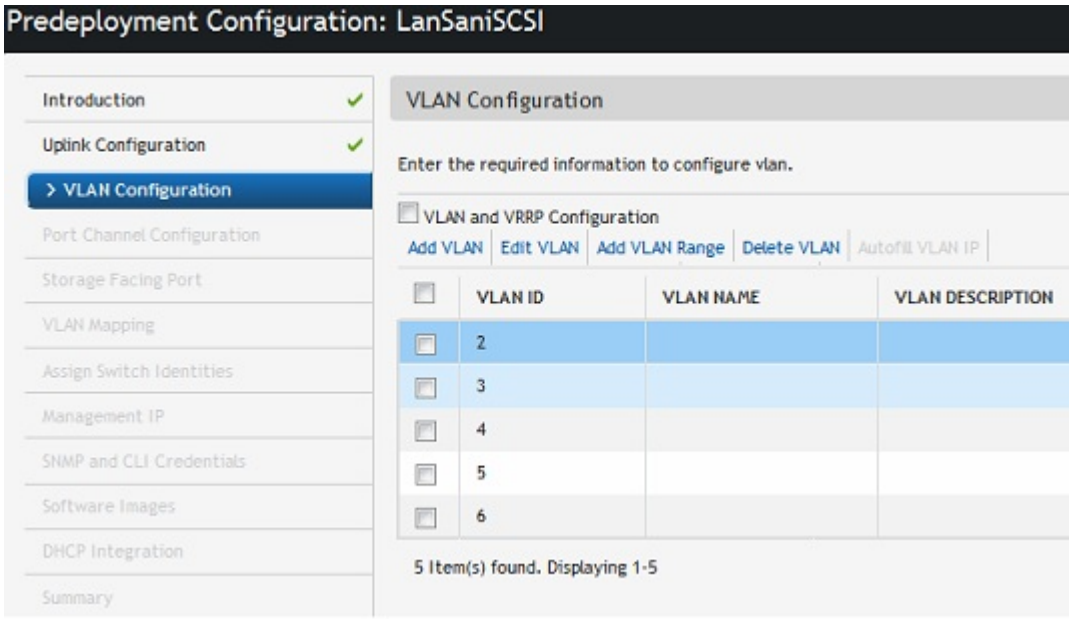


Figure 65. VLAN Configuration without VLAN and VRRP Configuration

Table 23. VLAN Configuration Options

VLAN Option	Description
Add VLAN	Enter the VLAN ID.
Add VLAN Range	Automates VLAN creation and automatically populates IP addresses. Enter the following VLAN information: • **Starting VLAN ID** — Enter the Starting VLAN ID. The range is **2** to **4094**. • **Number of VLANs** — Enter the Number of VLANs. • **VLAN Increment**. If you do not specify an increment, the VLAN is incremented by 1. • **Start Subnet IP Address/Prefix:** — IP range to automatically populate VLAN IP addresses. IP addresses include primary, secondary peer VLAN, and VRRP IP. NOTE: You must check the **VLAN and VRRP Configuration** option to view this option.
VLAN and VRRP Configuration	Configures IP address with VRRP protocol. When the **VLAN and VRRP Configuration**option is selected the following fields are displayed. • Primary IP • Secondary IP • Virtual IP
Autofill VLAN IP (For VLAN and VRRP Configuration only)	Enter the starting subnet IP address/prefix for the range of selected VLANS. The IP addresses are automatically populated.

Delete VLAN	Removes selected VLAN row.
Edit VLAN	Change the VLAN ID or VLAN ID, primary IP address, secondary IP address.
VLAN ID	Enter the VLAN ID. Range: **2** 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 address 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 address Prefix range: from **8** to **29** **Default** Virtual IP: <Blank> **Default** Prefix: **24**

To configure a 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 **VLAN Configuration** screen.

   Check the **VLAN and VRRP Configuration** option to the VLAN ID, primary IP address, secondary IP address, and virtual address.

   Click the **Add VLAN** link.

   The **Add VLAN Window** is displayed.

   NOTE: When you add a VLAN and do not enable the **VLAN and VRRP Configuration** option, you can only enter the VLAN ID and IP address range.

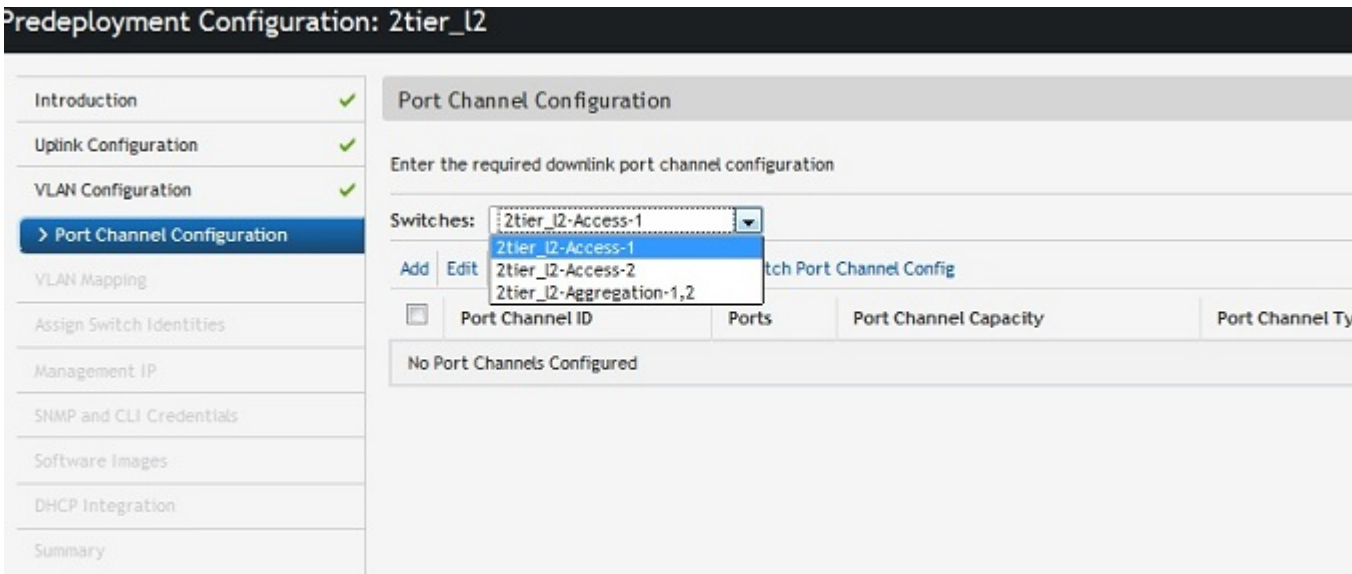
4. In the **VLAN ID** field, enter the VLAN ID.
5. In the **Primary IP address** field, enter the primary IP address.
6. In the **Secondary IP** address field, enter the secondary IP address.
7. In the **Virtual IP** address field, enter the virtual IP address
8. Click the **Next** button to view the **Port Channel Configuration** screen.

Pre-deployment – Step 1c: Port Channel Configuration (Layer 2)

Use this screen to optionally add, edit, delete, and automatically populate the port channel configuration. Once you add a port channel configuration you can copy it. You also configure uplink LAGs on the Port Channel Configuration screen.

Table 24. Layer 2 Port Channel Configuration Options

Field Name	Description
Add	Enter port channel information and enable LACP.
Auto Populate	Enter port channel information to automatically assign port channels to switches in the fabric and enable LACP. • Number of Ports per Port Channel • Start Port Channel ID • Number of Port Channel • Port Channel Increment • Enable LACP (optional)
Copy Switch Port Channel Configuration	Copies over switch port channel configuration from another switch. You first create a port channel configuration and then you can copy over to another switch.
Delete	Deletes a selected port channel configuration.
Edit	Enter the port channel configuration.



To create port channels to increase bandwidth and redundancy:

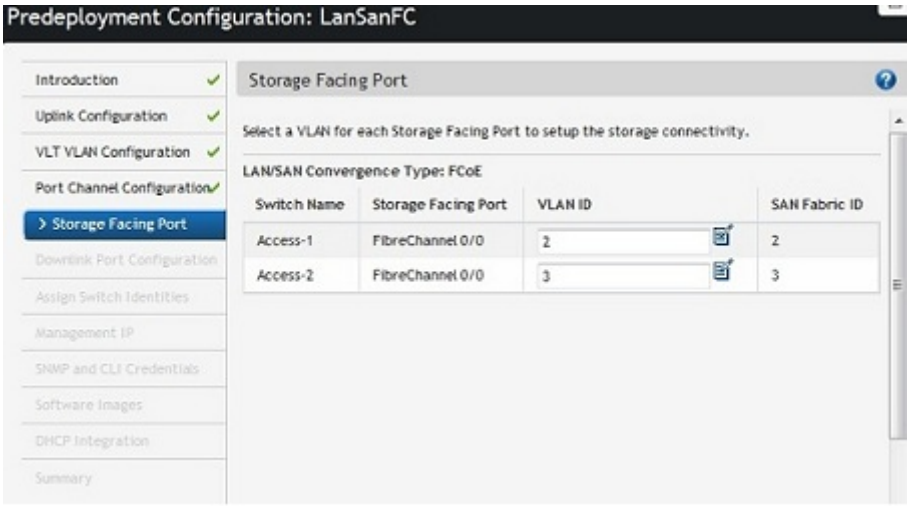
1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **Deploy Fabric** pull-down menu, select the **Pre-deployment Configuration** option.
3. Navigate to the **Port Channel Configuration** screen.
4. From the **Switch** pull-down menu, select a switch to apply the port channel configuration.
5. Click the **Add** link to manually add a port channel or the **Auto populate** link to automatically populate the port channels. For more port channel configuration options, refer to the Port Channel Configuration Options table for more information.
6. Click **Next** to go to the **VLAN Mapping** screen.

Pre-deployment — Step 1d: Storage Facing Port

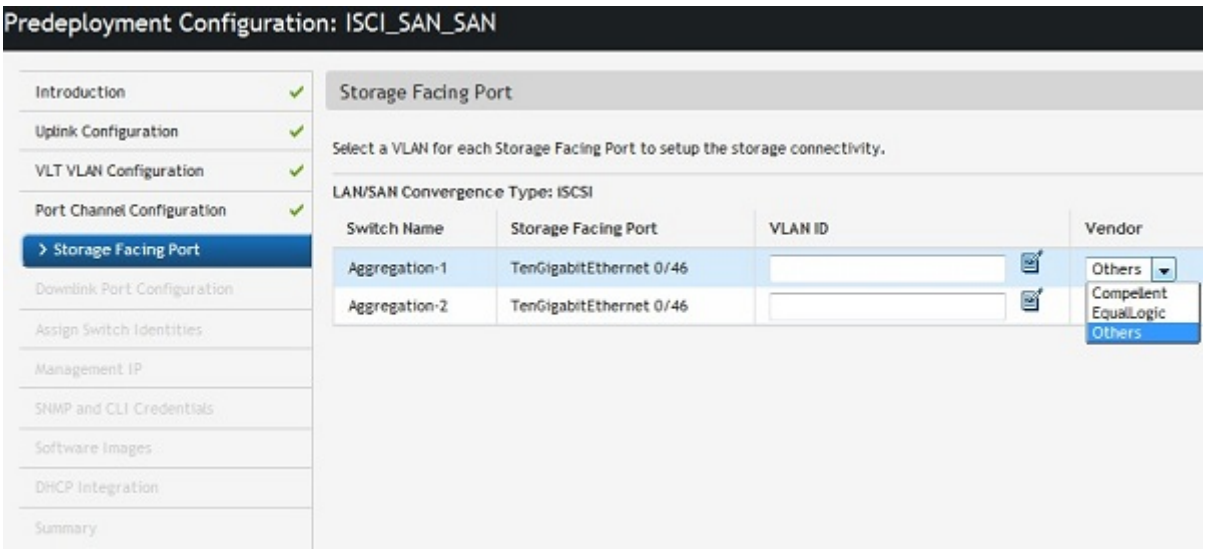
Use the **Storage Facing Port** screen to establish storage connectivity to iSCSI or fibre channel port. The **Storage Facing Port** pre-deployment screen is only available for LAN/SAN deployments that use iSCSI or fibre channel ports.
To establish storage connectivity to a storage facing port:

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 **Storage Facing Port** screen.
4. Navigate to the **VLAN ID** column.

5. To the right of the VLAN ID field, click the VLAN ID icon and select one VLAN ID and then associate it with the storage facing port.
   a. If you are connecting to fibre channel storage facing ports, AFM automatically populates the SAN Fabric ID when you select the VLAN ID.



   b. If you are connecting to iSCSI storage facing ports, select a VLAN ID and associated it with Vendor. Navigate to the **Vendor** pull-down menu and select one of the following options:



   - **Compellent**
   - **EqualLogic**
   - **Other**

   NOTE: Only one vendor can be associated to a unique VLAN. If a VLAN is associated to multiple Storage Facing ports, then AFM will automatically set the vendor to be the same across all associated entries.

6. Click the **Next** button to configure the VLAN Mapping configuration.

Pre-deployment – Step 1e: VLAN Mapping (Layer 2 VLT)

To add VLANs and associate ports on the different switches for a Layer 2 fabric, 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.

Table 25. VLAN Mapping 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. NOTE: VLANs previously associated with storage facing ports are part of the selection list.
Untagged VLANs	Select a VLAN to associate with the port. Validation Criteria: Tagged VLAN field should be empty. Default: <Blank> NOTE: VLANs previously associated with storage facing ports are part of the selection list.

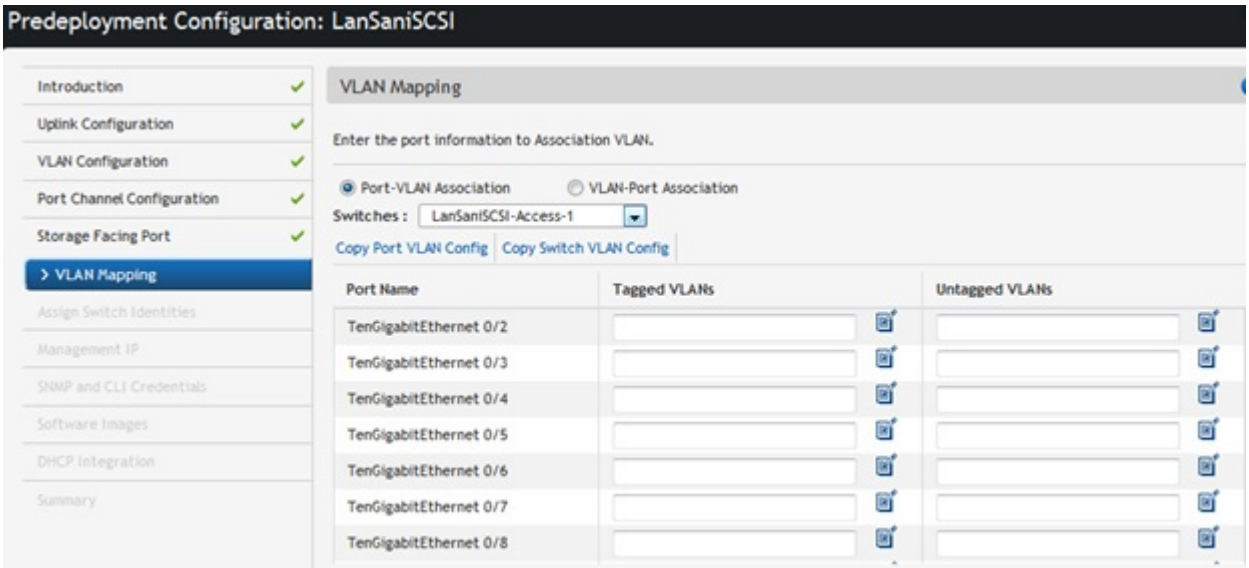
Table 26. Layer 2 VLAN Mapping Options

Option	Description
Auto-fill Tagged Port	For selected VLANs, sequential tagging is applied to the available ports and the number of ports specified on a VLAN.
Auto-fill Untagged Port	For selected VLANs, untagging is applied. Based on available ports, only one port per VLAN is associated. **Note**: **The number of Port/VLAN Port** option is disable on the **Autofill Tagged/Untagged Port** screen.
Copy Switch VLAN Config	Copies the VLAN association from the current switch to other switch (es) in the fabric.

Copy VLAN Port Config	Copies the VLAN association from a selected port to other port (s) within a switch.
Port-VLAN Association	Maps the physical port to the VLAN ID. For example, maps 1 port to multiple VLANs.
VLAN-Port Association	Maps the VLAN ID to physical port interfaces. For example, maps 1 VLAN to multiple ports.
Copy VLAN Tagged Port Config	Copies the VLAN tagged port configuration from a selected port to other port (s) within a switch.

To configure the downlinks on the access switches and uplinks on the aggregation 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 **VLAN Mapping** screen.



4. From the **Switche**s pull-down menu, select an access or aggregation switch.
5. In the **Tagged VLANs** field, click on the icon to the right and then enter one or more VLANs to be associated with the port.
6. When you are finished, click the **Next** button to go to the **Assign Network Identities** screen.

Protocol Configuration — Layer 3 Distributed Core Fabric: Step 1

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

NOTE:

Before you begin, review the pre-deployment workflow for a Layer 3 distributed core fabric at Using the Pre-deployment Configuration Wizard.

- Pre-deployment – Step 1a: Fabric link Configuration

- Pre-deployment – Step 1b: Uplink Configuration
- Pre-deployment - Step 1c: : Downlink Configuration

NOTE: For pre-deployment, the Layer 2 VLT, Layer 3 Distributed Core, and Layer 3 with Resiliency (Routed VLT) fabrics use the same pre-deployment configuration screens from step 2 through step 7.

Pre-deployment – Step 1a: Fabric link Configuration

Before you begin, review the Using the Pre-deployment Configuration Wizard and Pre-deployment Wizard: Introduction sections.

To configure the links that connect the leaves and spines for a Layer 3 distributed core fabric or the links that connect the core, access, and aggregation switches for a Layer 3 with Resiliency (Routed VLT) fabric using the OSPF routing protocol, use the **Fabric link Configuration** screen. The **Port Bandwidth** (a read-only field) is automatically determined by the selected fabric type and fabric oversubscription ratio. 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**.

Important: The area ID for the interconnect link must **not** be the same as the area ID for the uplink.

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 1b: Uplink Configuration

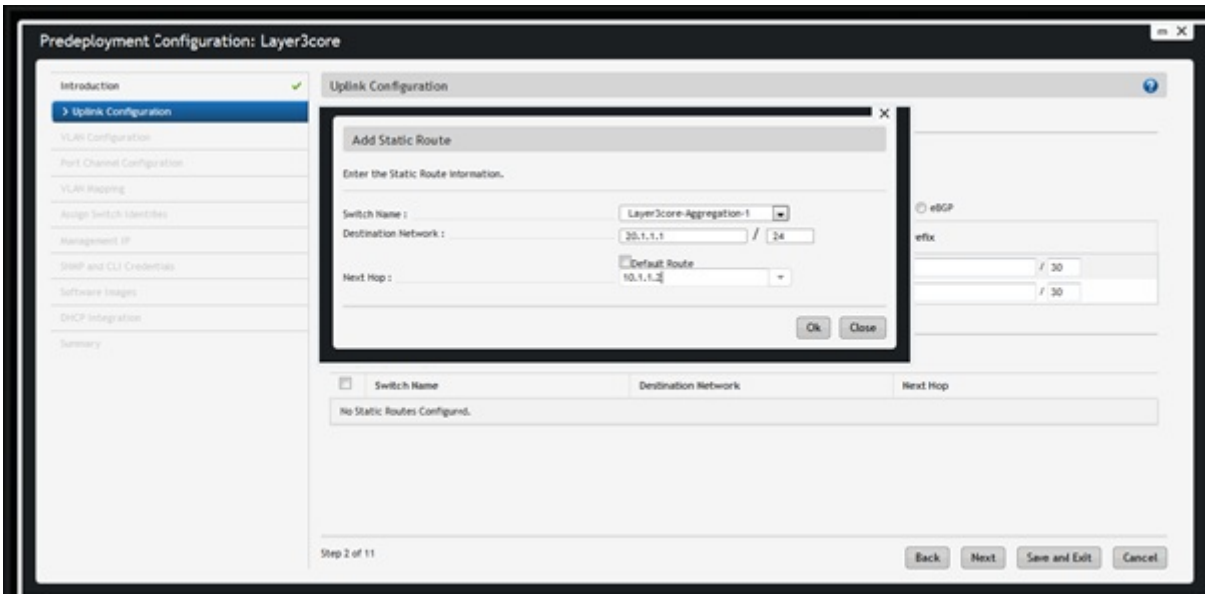
The **Uplink Configuration** screen for a Layer 3 and Layer 3 with Resiliency (Routed VLT) fabric displays the port bandwidth and the number of specified ports (read-only fields) entered on the **Bandwidth and Port Count** screen. To configure the uplink protocol for the edge port uplinks to the WAN,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

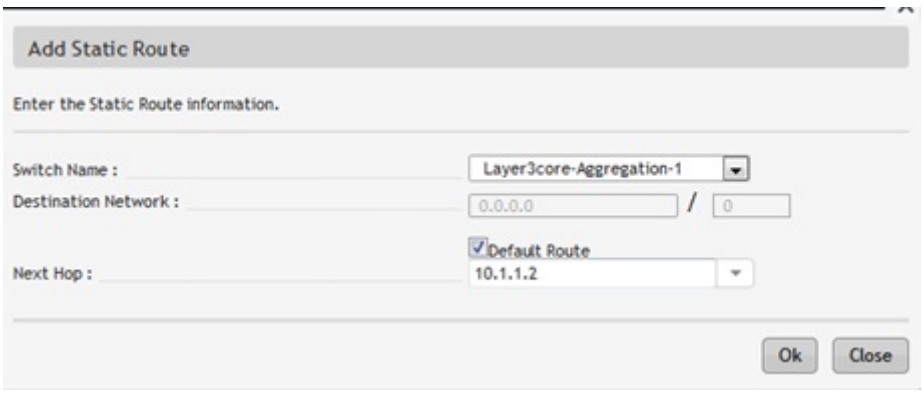
NOTE: When the Open Shortest Path First (OSPF) is selected for both uplinks and interlinks, one of uplinks or interlinks must be in area 0.

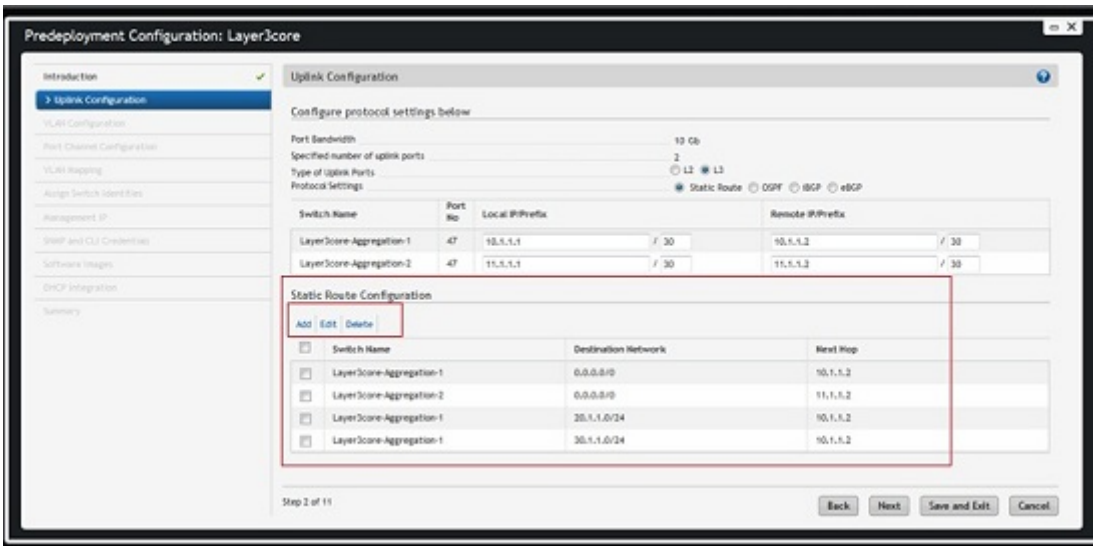
To configure the uplink protocol for the edge port uplinks to the WAN for a Layer 3 distributed core fabric:

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 **Type of Uplink Ports** area, select one of the following options:
   a. **static routes —** When you select the **static routes** option, AFM displays the **Adds Static Route** window. You can configure up to 10 static routes for each aggregation device. When you check the of **Default Route** option , AFM automatically populates the destination network field to **0.0.0.0/0**. For static routes, enter the destination network and the next hop.

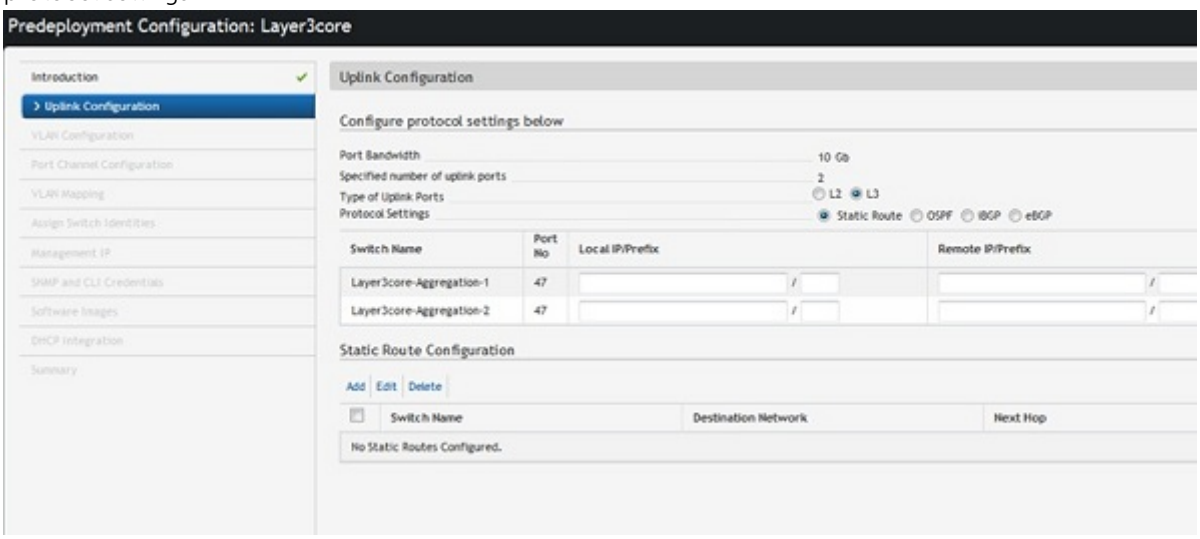






b. **L2** —Configures Layer 2 uplinks for a Layer 2 fabric. By default, this option is disabled on a Layer 3 Distributed Core fabric.

c. **L3** — Configures uplinks for a Layer 2 VLT or Layer 3 Distributed Core fabric. When you select the **L3** option, the **Uplink Configuration** screen displays additional options to configure the Layer 3 protocol settings.



5. 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 **Bandwidth and Port Count** screen.

   AFM automatically populates the range of IP addresses that 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**.
6. Click **Next** to go the **Downlink Configuration** screen.

Pre-deployment – Step 1d : Downlink Configuration (Layer 3)

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 Gb, 10 Gb, or 40 Gb (a read-only field). For more information about downlinks, see Distributed Core Terminology.

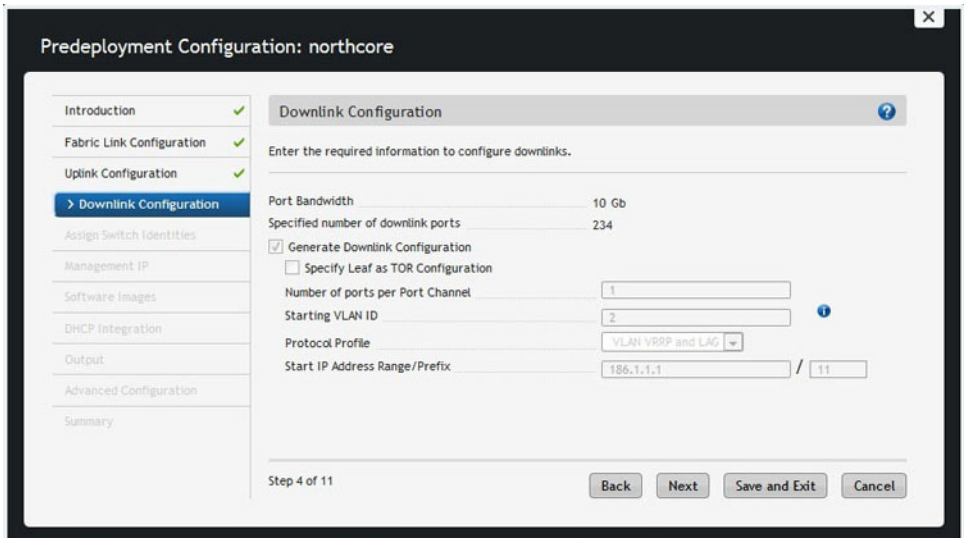


Figure 66. Downlink Configuration for Layer 3 Distributed Core Fabric

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. To have the leaves act as a ToR, select the **Specify Leaf as ToR** option.
5. Manually configure the downlinks, or to automatically generate the downlink configuration, check 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 **Assign Switch Identities** screen.

Protocol Configuration — Layer 3 with Resiliency (Routed VLT) : Step 1

To configure the pre-deployment protocol configuration for a Layer 3 with Resiliency (Routed VLT) , complete the following tasks:

NOTE: The Layer 2 VLT, Layer 3 Distributed Core, and Layer 3 with Resiliency (Routed VLT) fabrics use the same pre-deployment configuration screens from step 2 through step 7. Before you begin, review the pre-deployment workflow at Using the Pre-deployment Configuration Wizard.

1. Pre-deployment – Step 1a: Fabric Link Configuration
2. Pre-deployment – Step 1b: Uplink Configuration
3. Pre-deployment – Step 1c: VLAN Configuration
4. Pre-deployment – Step 1d: Port Channel Configuration
5. Pre-deployment – Step 1e: VLAN Mapping

Pre-deployment – Step 1a: Fabric link Configuration

Before you begin, review the Using the Pre-deployment Configuration Wizard and Pre-deployment Wizard: Introduction sections.

To configure the links that connect the leaves and spines for a Layer 3 distributed core fabric or the links that connect the core, access, and aggregation switches for a Layer 3 with Resiliency (Routed VLT) fabric using the OSPF routing protocol, use the **Fabric link Configuration** screen. The **Port Bandwidth** (a read-only field) is automatically determined by the selected fabric type and fabric oversubscription ratio. 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**.

Important: The area ID for the interconnect link must **not** be the same as the area ID for the uplink.

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 1b: Uplink Configuration

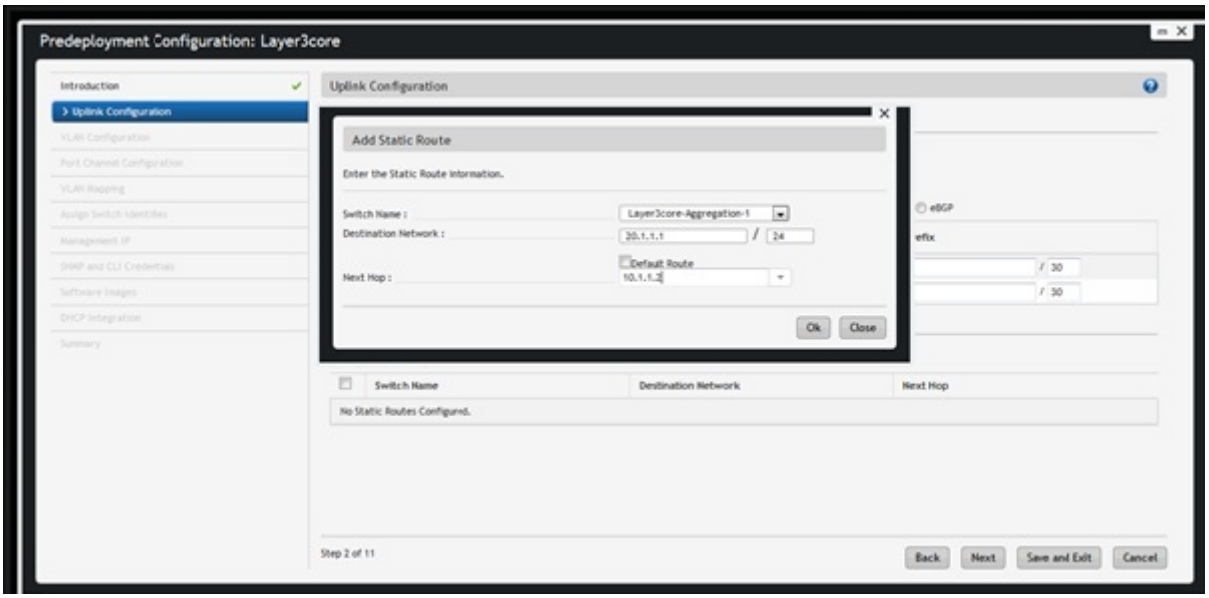
The **Uplink Configuration** screen for a Layer 3 and Layer 3 with Resiliency (Routed VLT) fabric displays the port bandwidth and the number of specified ports (read-only fields) entered on the **Bandwidth and Port Count** screen. To configure the uplink protocol for the edge port uplinks to the WAN,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

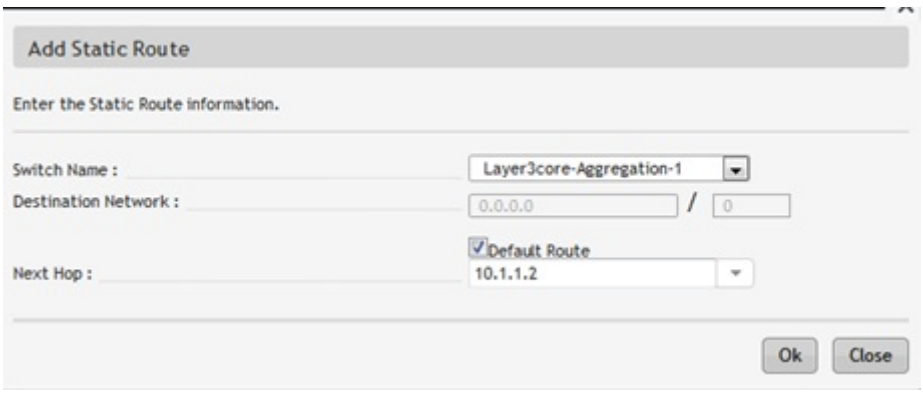
NOTE: When the Open Shortest Path First (OSPF) is selected for both uplinks and interlinks, one of uplinks or interlinks must be in area 0.

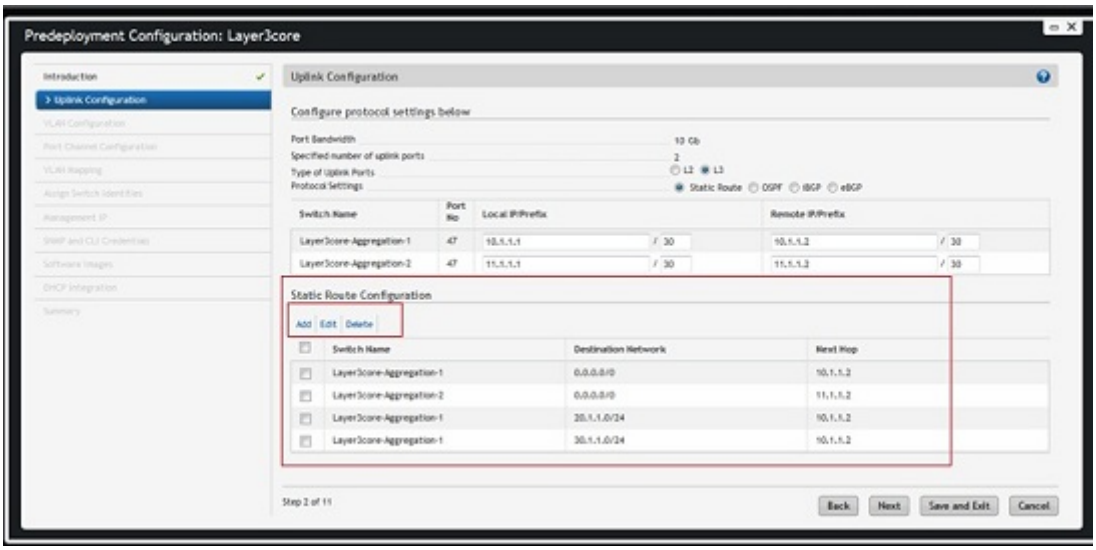
To configure the uplink protocol for the edge port uplinks to the WAN for a Layer 3 distributed core fabric:

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 **Type of Uplink Ports** area, select one of the following options:
   a. **static routes —** When you select the **static routes** option, AFM displays the **Adds Static Route** window. You can configure up to 10 static routes for each aggregation device. When you check the of **Default Route** option , AFM automatically populates the destination network field to **0.0.0.0/0**. For static routes, enter the destination network and the next hop.

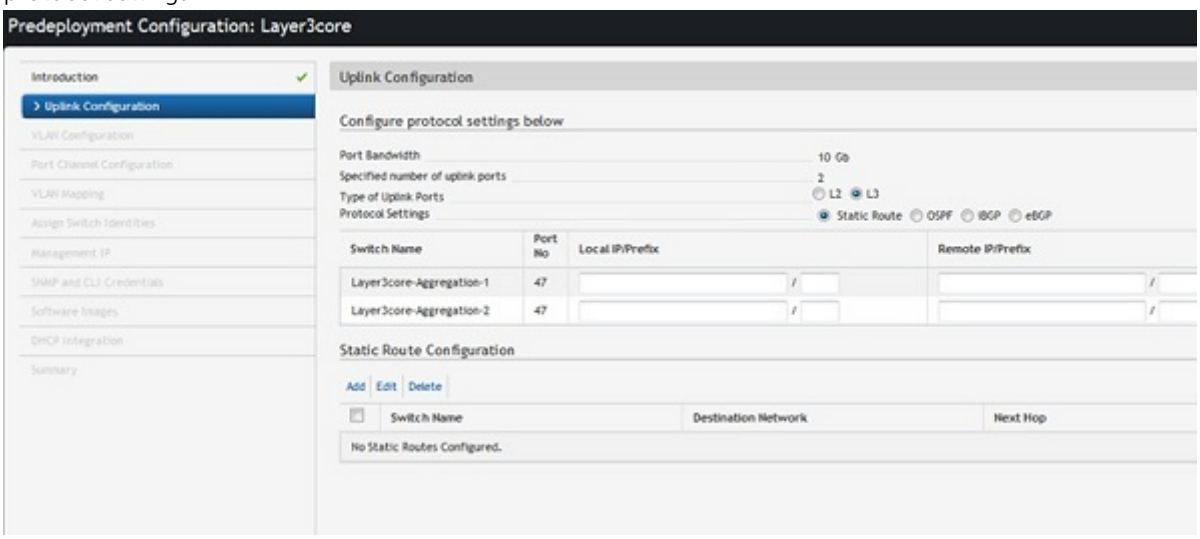






b. **L2** —Configures Layer 2 uplinks for a Layer 2 fabric. By default, this option is disabled on a Layer 3 Distributed Core fabric.

c. **L3** — Configures uplinks for a Layer 2 VLT or Layer 3 Distributed Core fabric. When you select the **L3** option, the **Uplink Configuration** screen displays additional options to configure the Layer 3 protocol settings.



5. 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 **Bandwidth and Port Count** screen.

   AFM automatically populates the range of IP addresses that 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**.

6. Click **Next** to go the **Downlink Configuration** screen.

Pre-deployment – Step 1c: VLT VLAN Configuration for Layer 3 with Resiliency Fabric (Routed VLT)

Use this screen to configure the VLT VLAN configuration for a Layer 3 with Resiliency (Routed VLT) fabric.

This section contains the following topics:

- VLT VLAN Layer 3 with Resiliency (Routed VLT)
- Advanced VLAN IP Configuration

Table 27. VLT VLAN Configuration Options for Layer 3 with Resiliency (Routed VLT) Fabirc

VLAN Option	Description
Add VLAN	Creates a VLAN row.
Add VLAN Range	Automates VLAN creation and automatically populates IP addresses. Enter the following VLAN information: • **Starting VLAN ID** — Enter the Starting VLAN ID. Range: **2** to **4094** • **Number of VLANs** — Enter the Number of VLANs. • **VLAN Increment**. If you do not specify an increment, the VLAN is incremented by 1. • **Start Subnet IP Address/Prefix:** — IP range to automatically populate VLAN IP addresses. IP addresses include primary, secondary peer VLAN, and VRRP IP. NOTE: You must check the **VLAN and VRRP Configuration** option to view this option.
VLAN and VRRP Configuration (for a Layer 3 fabric for Resiliency (Routed VLT)	Configures IP address with VRRP protocol. When the **VLAN and VRRP Configuration** option is selected the following fields are displayed. • Primary IP • Secondary IP • Virtual IP
Autofill VLAN IP (For Enable Layer 3 Protocol in Access Switches option only)	Enter the starting subnet IP address/prefix for the range of selected VLANS. The IP addresses are automatically populated.

Delete VLAN	Removes selected VLAN row.
Edit VLAN	Edit VLAN ID, primary IP address, and secondary IP address.
VLAN ID	Enter the VLAN ID. Range: **2** 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 address Prefix range: from **8** to **29** **Default** Secondary IP: <Blank> **Default** Prefix: **24**

VLT VLAN Configuration for Layer 3 with Resiliency (Routed VLT)

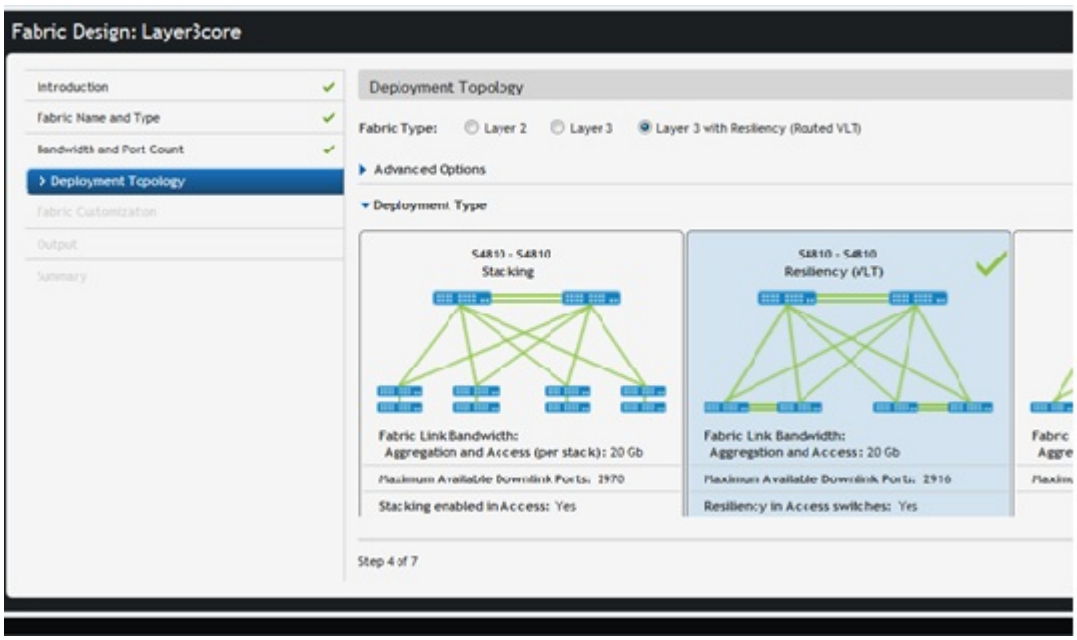


Figure 67. Layer 3 with Resiliency (Routed VLT) Deployment Topology

The following screen shot displays a VLT VLAN Configuration screen without selecting the **Enable Layer 3 protocol in Access Switches** option. By default the VLT VLAN screen for Layer 3 with Resiliency (Routed VLT) requires that you enter the primary and secondary IP address for the VLAN ID as show in the following screen shot.

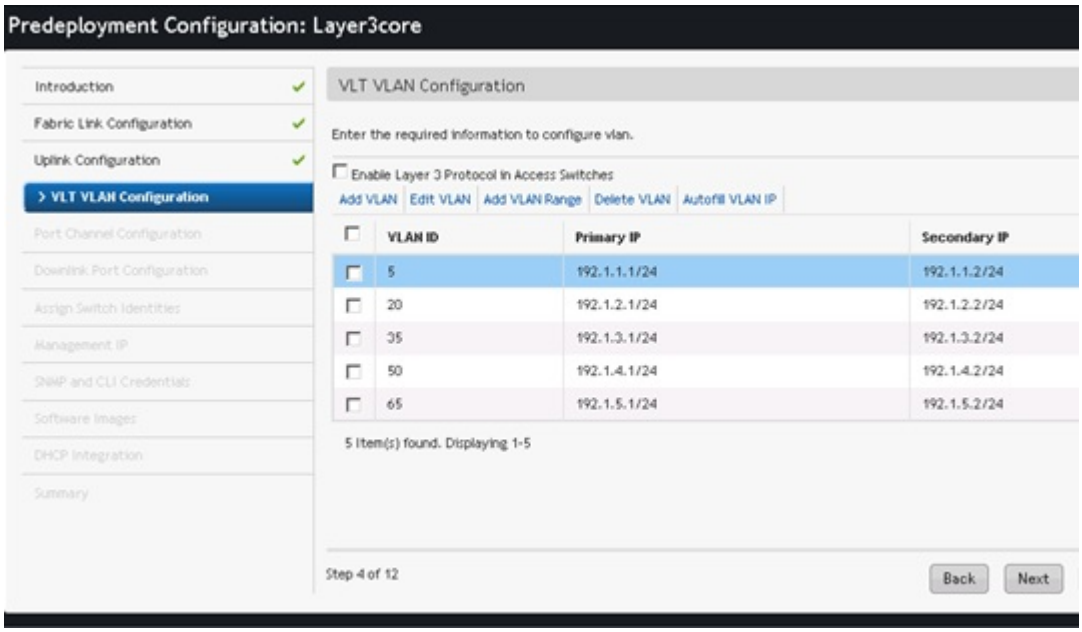


Figure 68. VLT VLAN Configuration Without Using the Enable Layer 3 Protocol in Access Switches Option

The following screen shot displays a VLT VLAN Configuration screen using the **Enable Layer 3 protocol in Access Switches** option. To have the topology for a Layer 3 with Resiliency (Routed VLT) support both access and aggregation devices, select the **Enable Layer 3 protocol in Access Switches** option. When you use this option, provide the network IP address range using the **Add VLAN Range** link. The IP addresses are assigned to all the access and aggregation switches.

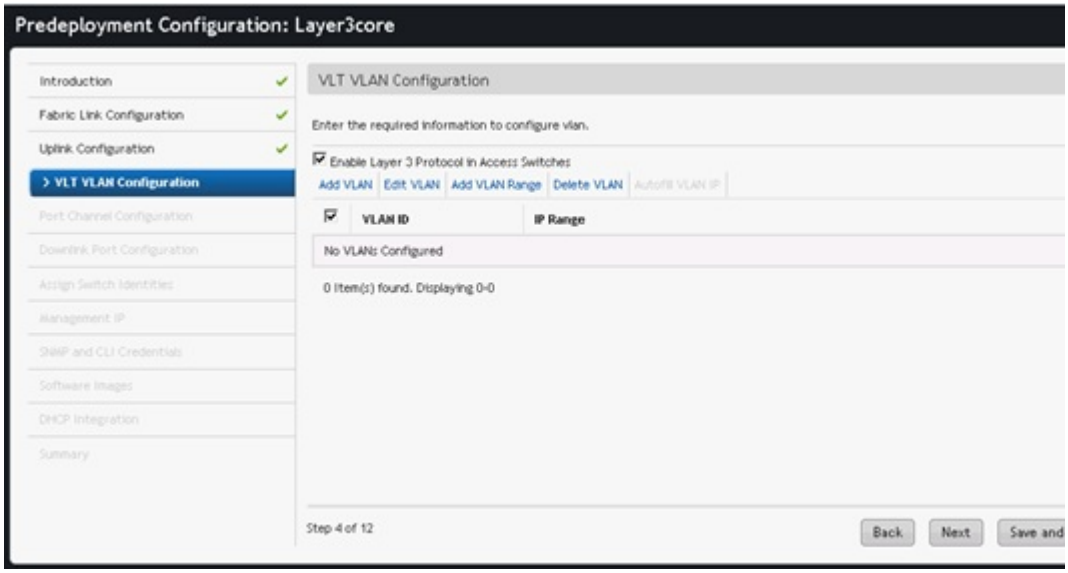


Figure 69. Layer 3 with Resiliency Using the Enable Layer 3 Protocol in Access Switches Option

The following screen shot displays the results after checking the **Enable Layer Protocol in Access Switches** option and adding VLANs for a Layer 3 with Resiliency (Routed VLT) fabric.

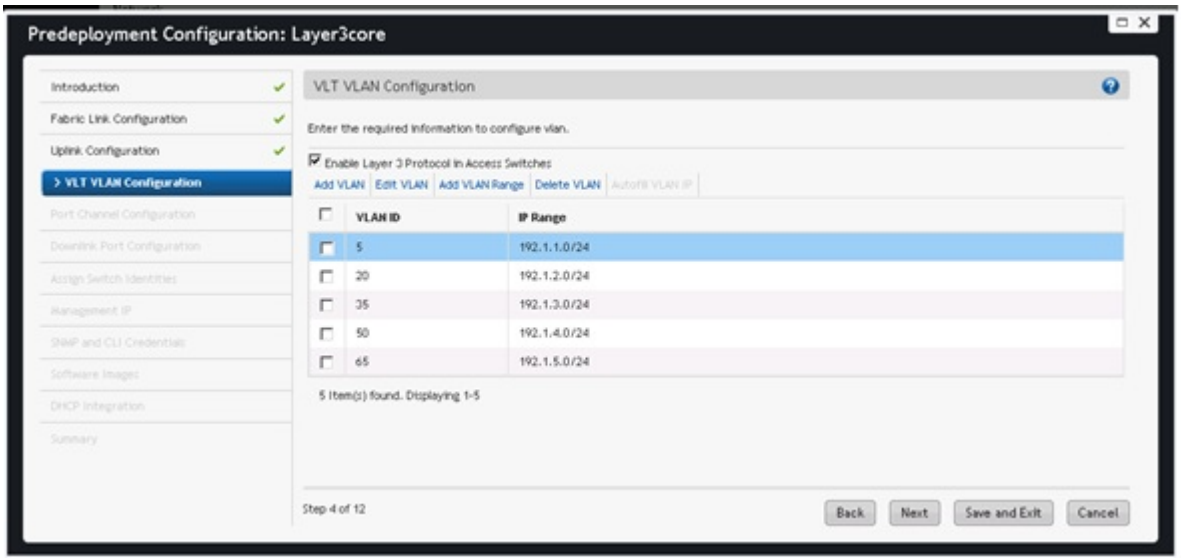


Figure 70. Adding VLANs and Enabling the Layer Protocol in Access Switches Option

To configure a VLT VLAN for a Layer 3 with Resiliency (Routed VLT) topology:

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. Check the **Enable Layer 3 Protocol in Access Switches** option.

5. Click the **Add VLAN** link.

   The **Add VLAN Window** is displayed.

6. Click the **Add VLAN Range** link and then specify the VLAN range to assign the IP addresses to the switches for the Layer 3 with Resiliency (Routed VLT) fabric.
7. Click the **Next** button to view the **Port Channel Configuration** screen.

Advanced VLAN IP Configuration

After completing the pre-deployment process, you can later modify the VLT VLAN configuration for Layer 3 with Resiliency (Routed VLT) topology using the **Advanced VLAN IP Configuration** option at the **Network** > *Fabric* > *Switch* > **Configure and Deploy** screen.

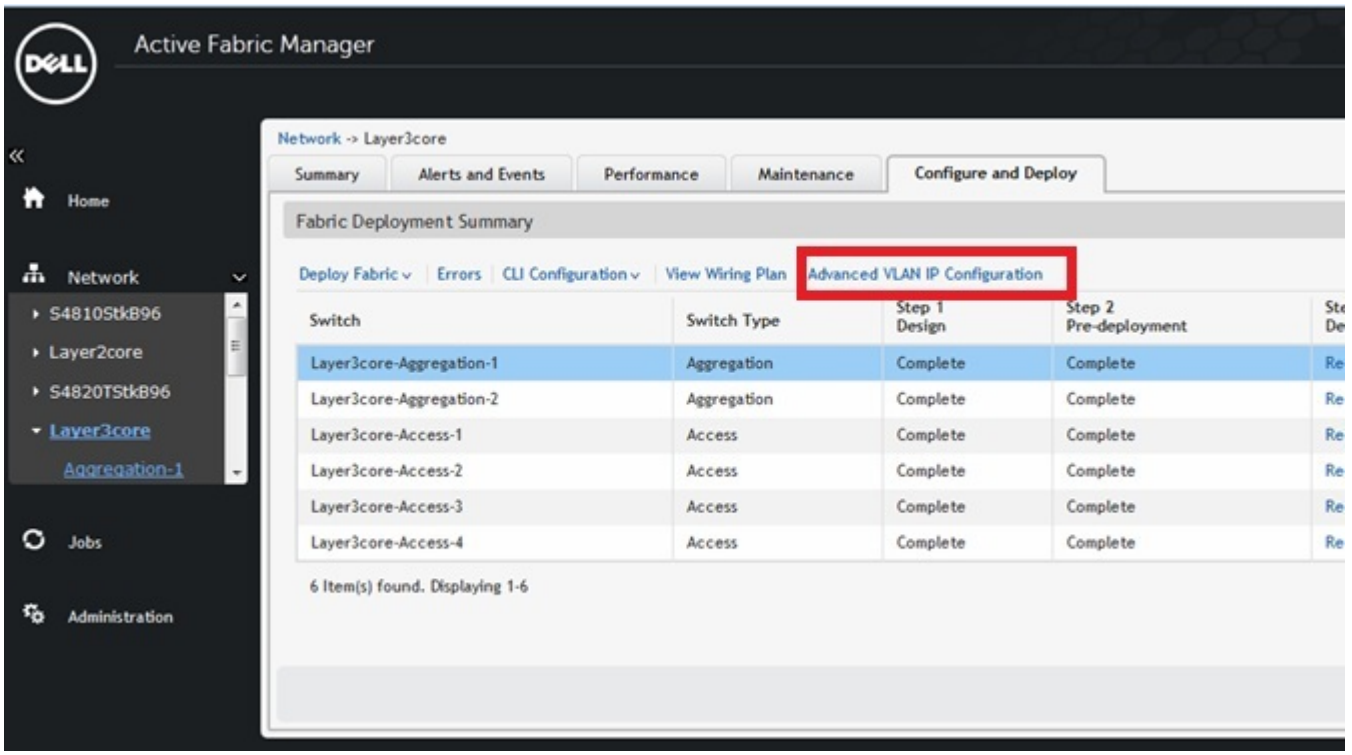


Figure 71. Advanced VLAN IP Configuration Option

Pre-deployment – Step 1d: Port Channel Configuration (Layer 3 — Routed VLT)

Use this screen to optionally add, edit, delete, and automatically populate the port channel configuration for Layer 3 with Resiliency (Routed VLT) fabric. Once you add a port channel configuration you can copy it.

Table 28. Port Channel Configuration Options

Field Name	Description
Add	Enter port channel information and enable LACP.
Auto Populate	Enter port channel information to automatically assign port channels to switches in the fabric and enable LACP. • Number of Ports per Port Channel

	• Start Port Channel ID • Number of Port Channel • Port Channel Increment • Enable LACP (optional)
Copy Switch Port Channel Configuration	Copies over switch port channel configuration from another switch. You first create a port channel configuration and then you can copy over to another switch.
Delete	Deletes a selected port channel configuration.
Edit	Enter the port channel configuration.

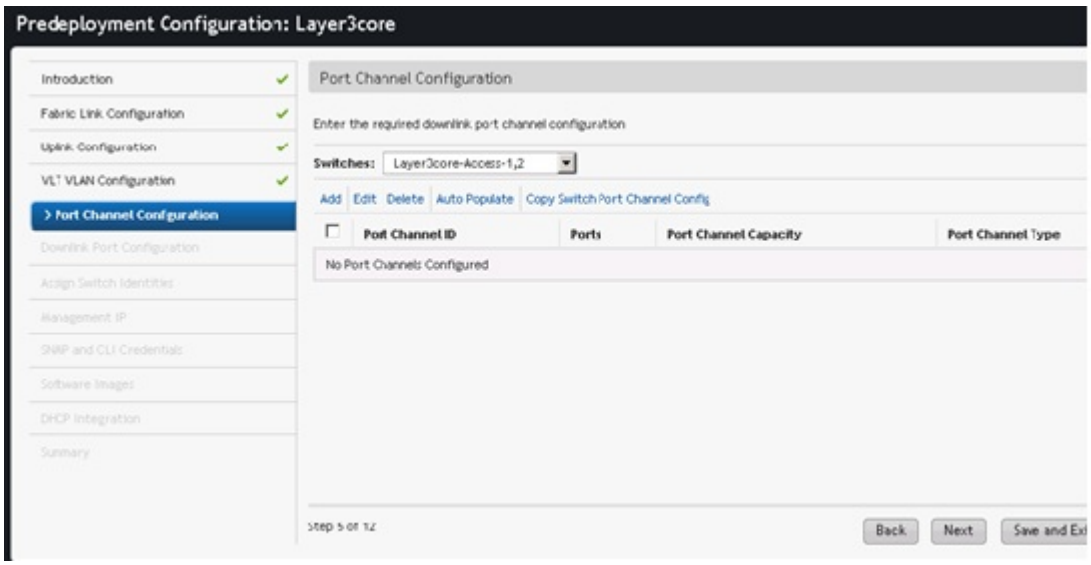


Figure 73. Port Channel Configuration Screen

To create port channels to increase bandwidth and redundancy:

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 **Port Channel Configuration** screen.
4. From the **Switch** pull-down menu, select a switch to apply the port channel configuration.
5. Click the **Add** link to manually add a port channel or the **Auto populate** link to automatically populate the port channels. For more port channel configuration options, refer to the Port Channel Options table above for more information.
6. Click **Next** to go to the **Downlink Port Configuration** screen.

Pre-deployment – Step 1e: VLAN Mapping (Layer 3– Routed VLT)

To add VLANs and associate ports on the different access switches to which VLAN for a Layer 3 with Resiliency (Routed VLT) fabric, use the **VLAN Mapping** 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.

Table 29. VLAN Mapping 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>

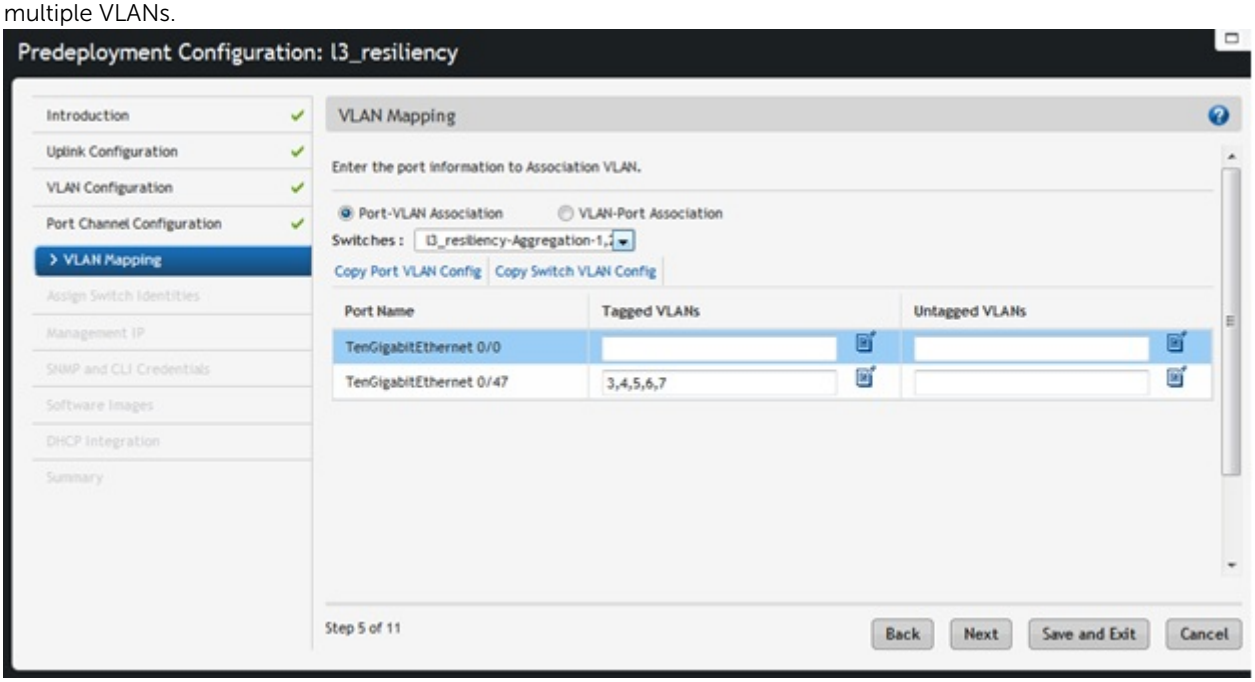
Table 30. VLAN Mapping Options

Option	Description
Auto-fill Tagged Port	For selected VLANs, sequential tagging is applied to the available ports and the number of ports specified on a VLAN.
Auto-fill Untagged Port	For selected VLANs, untagging is applied. Based on available ports, only one port per VLAN is associated. **Note**: **The number of Port/VLAN Port** option is disable on the **Autofill Tagged/Untagged Port** screen.
Copy Switch VLAN Config	Copies the VLAN association from the current switch to other switch (es) in the fabric.
Copy VLAN Port Config	Copies the VLAN association from a selected port to other port (s) within a switch.
Port-VLAN Association	Maps the physical port to the VLAN ID. For example, maps 1 port to multiple VLANs.
VLAN-Port Association	Maps the VLAN ID to physical port interfaces. For example, maps 1 VLAN to multiple ports.

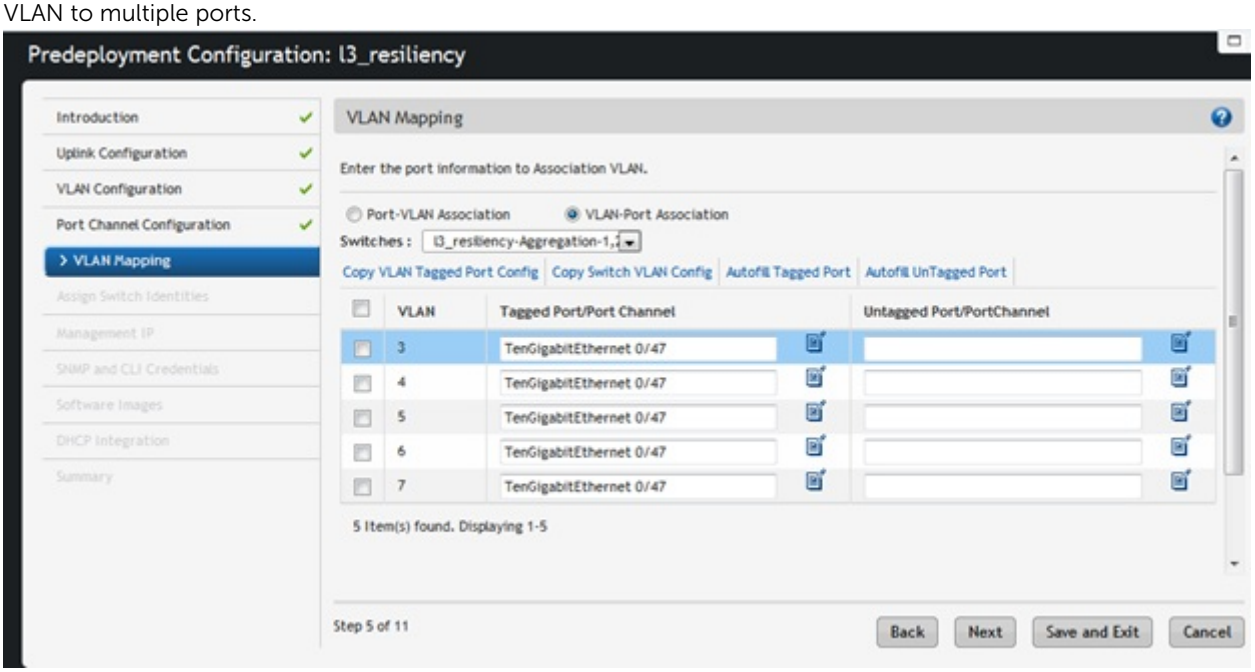
To configure downlink ports on the switches:

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 Layer 3 with Resiliency (Routed VLT) **VLAN Mapping** screen.
4. Select one of the following options:
   - **Port-VLAN Association** — Maps the physical port to the VLAN ID. For example, maps 1 port to multiple VLANs.



   - **VLAN-Port Association** — Maps the VLAN ID to physical port interfaces. For example, maps 1 VLAN to multiple ports.



5. From the **Switches** pull-down menu, select a switch or a set of switches.

6. In the **Tagged VLANs**, click on the icon next and enter one or more VLANs to be associated with the port.
7. When you are finished, click the **Next** button to go to the **Assign Network Identities** screen.

Pre-deployment – Step 1e: VLAN Mapping (Layer 2 VLT)

To add VLANs and associate ports on the different switches for a Layer 2 fabric, 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.

Table 31. VLAN Mapping 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. NOTE: VLANs previously associated with storage facing ports are part of the selection list.
Untagged VLANs	Select a VLAN to associate with the port. Validation Criteria: Tagged VLAN field should be empty. Default: <Blank> NOTE: VLANs previously associated with storage facing ports are part of the selection list.

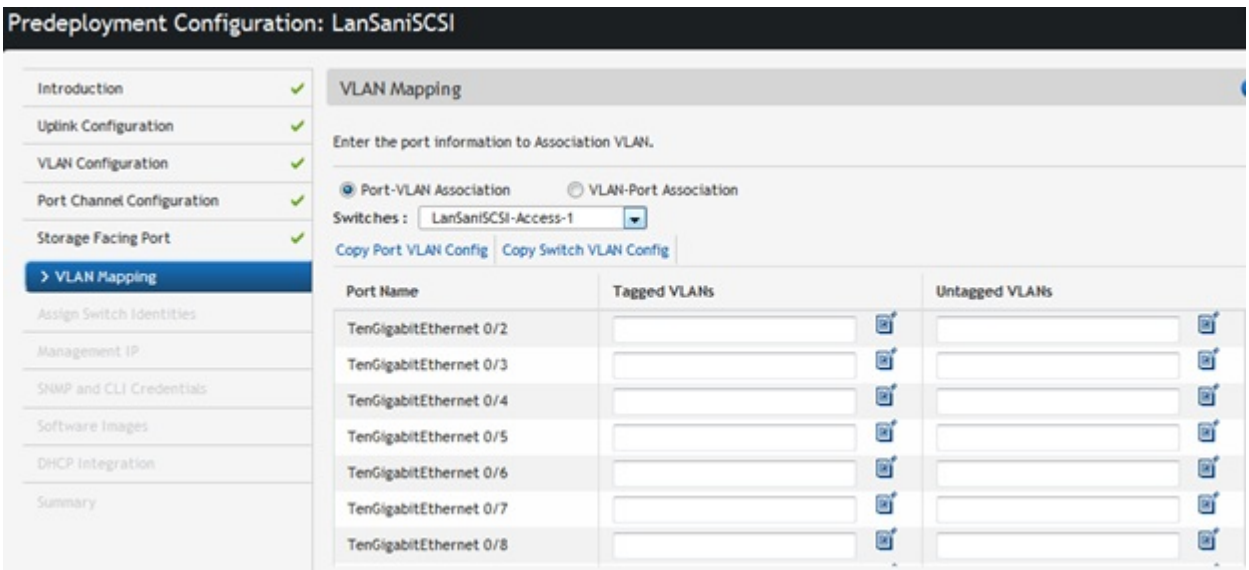
Table 32. Layer 2 VLAN Mapping Options

Option	Description
Auto-fill Tagged Port	For selected VLANs, sequential tagging is applied to the available ports and the number of ports specified on a VLAN.
Auto-fill Untagged Port	For selected VLANs, untagging is applied. Based on available ports, only one port per VLAN is associated. **Note**: **The number of Port/VLAN Port** option is disable on the **Autofill Tagged/Untagged Port** screen.

Copy Switch VLAN Config	Copies the VLAN association from the current switch to other switch (es) in the fabric.
Copy VLAN Port Config	Copies the VLAN association from a selected port to other port (s) within a switch.
Port-VLAN Association	Maps the physical port to the VLAN ID. For example, maps 1 port to multiple VLANs.
VLAN-Port Association	Maps the VLAN ID to physical port interfaces. For example, maps 1 VLAN to multiple ports.
Copy VLAN Tagged Port Config	Copies the VLAN tagged port configuration from a selected port to other port (s) within a switch.

To configure the downlinks on the access switches and uplinks on the aggregation 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 **VLAN Mapping** screen.



4. From the **Switche**s pull-down menu, select an access or aggregation switch.
5. In the **Tagged VLANs** field, click on the icon to the right and then enter one or more VLANs to be associated with the port.
6. When you are finished, click the **Next** button to go to the **Assign Network Identities** screen.

Pre-deployment – Step 2: Assign Switch Identities

To assign the system MAC addresses to the switches in the fabric, use the **Assign Switch Identities** screen.

Important: Make sure you associate the switches with the correct system MAC address; otherwise, your wiring plan will be wrong.

The following is a sample CVS file.

Table 33. Sample CSV Format

serial_number	purchase_order	mfg_part_number	mac_address	server_tag
HADL134J20193	163	759-0096-02 REV.F	00:01:E8:8B: 15:77	9RGZTS2

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.

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 **Choose MAC** icon in each row to associate the switch name with the MAC address, (optional) serial number, and (optional) service tags using the CSV file or manually enter this information. If you are using a CSV file, the **Select MAC Address Selection** screen is displayed.
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 3: 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 management IP 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.

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 4: SNMP and CLI Credentials

Use this screen to configure SNMP and CLI credentials at the fabric level. Configure SNMP so that the AFM 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. The write community string is populated from the AFM global setting, which is configure during installation. To provision the fabric, enter the FTOS CLI user's credentials 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 SNMP and CLI credentials:

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 **SNMP and CLI Credentials** screen.
4. Navigate to the **SNMP Configuration** area.
5. In the **Read Community String** field, enter the read community string. For example, "public".
6. In the **Write Community String** field, enter the write community string. For example, "private".
7. Navigate to the **CLI Credentials** area.
8. In the **Protocol** pull-down menu, select one of the following options: Telnet or SSHv2.
9. In the **User Name** field, enter the user name.
10. In the **Password** field, enter the password.
11. In the **Confirm Password** field, confirm the password. The privilege level is a read-only field and is set at **15**.
12. In the **Enable Password** field, enter a password for the privilege level.
13. In the **Confirm Enable Password** field, confirm the enabled password for the privilege level.
14. Click **Next**.

Pre-Deployment – Step 5: 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 from this site.

To change the address of the TFTP or FTP site, navigate to the **Administration > Settings** > **TFTP/FTP** 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 6: 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

To automatically integrate the file into the AFM local DHCP server, use the default setting **Local (AFM provisioned to be a DHCP server)**. AFM automatically generates a switch configuration file and transfers it to the local DHCP server on AFM.

To manually integrate the DHCP configuration into the external DHCP server, select the **Remote (External DHCP server)** option.

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, S6000, 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, AFM generates a port MAC address from the pre-deployment configuration, not a chassis MAC address.

To integrate the DHCP 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 **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.
6. Click **Next** to go to the **Summary** screen.

Pre-Deployment – Step 7: 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 the **Finished** button to commit 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 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 DHCP Integration.

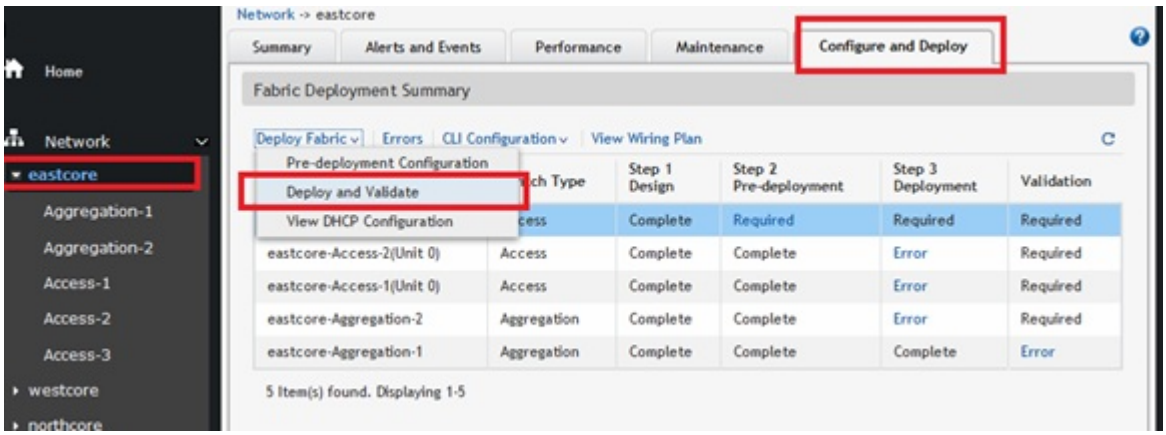
Deploying and Validating the Fabric

This section contains the following topics:

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

Deploying the Fabric

To deploy the fabric, use the **Network >** *Fabric Name*> **Configure and Deploy** > **Deploy Fabric** > **Deploy and Validate** screen. When you deploy a fabric, make sure that the fabric design matches the deployed fabric. AFM prompts you to fix any errors when you deploy the fabric.



Attention:
During initial deployment, the BMP process wait time to install the software onto the switches in the fabric is the following:

- 10 minutes for a non-stack fabric
- 20 minutes for stack fabric.

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 34. 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 DHCP Integration. For information about how to view the DHCP configuration file for a fabric, see Viewing the DHCP Configuration File.
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 switches that you want to deploy in the **Switch Name** 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. Select the **Apply configuration changes to the switch** option or the **Overwrite entire configuration on the switch** option.

When you deploy a switch, the following options are available:

- **Apply configuration changes to the switch**– Apply new configuration changes from the AFM Server to the switch.
- **Overwrite entire configuration on the switch** – Overwrites the entire current configuration on the switch instead of applying only the changes to the current switch configuration.
  - If the **Reset to factory defaults** option is selected, AFM resets the switch to the factory default mode (BMP mode). AFM deploys the new configuration which overwrites the entire current configuration onto the switch.
  - If the **Reset to factory defaults** option is not selected, AFM deploys the new configuration which overwrites the entire current configuration onto the switch.

11. 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. 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.

Advanced Configuration

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

- View the Auto-Generated Configuration
- Associate the Templates to Fabric Switches

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

View the Auto-generated Configuration

To view the AFM auto-generated configuration:

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy > Deploy Fabric > > Advanced Configuration > View Auto-Generated Configuration** screen.
2. From the **Deploy Fabric** pull-down menu, select the **Deploy and Validate** option.
3. On the **Deploy** tab, click the **Advanced Configuration** link.
4. Click on **View Auto-Generated Configuration** link and wait for the configuration to be displayed

Associating Templates

You can associate one or more existing configuration templates to the fabric (entire fabric), all spines, all leaves, all aggregation switches, all core switches, all access switches or a set of switches. When a template is associated to an entire fabric or all spines, all leaves, all core switches, all aggregation switches, and all core switches, 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 **Deploy Fabric** pull-down, select the **Deploy and Validate** option.
3. On the **Deploy** tab, click the **Advanced Configuration** link.
4. Click the **Associate Templates to Fabric Switches** link.
   The **Associate Templates** screen displays:
5. Click the **Add Association** link.
6. In the **Template Name** pull-down menu, select the template that you want to use.
7. (Optionally) In the **Comments** field, enter your comments.
8. In the **Select Association** area, select one the following options:
   a. **All** — Associates the template to all the switches in the fabric
   b. **Aggregation** — Associates the template to all the aggregation switches.
   c. **Access** — Associates the template to all the access switches.
   d. **Core** — Associates the template to all the core switches.
   e. **Spines** — Associates template to all the spine switches.
   f. **Leafs** — Associates template to all the leaf switches.
   g. **Custom** — Associates template with specific switches. In the **Available Switches**, select the switches that you want to associate the template with.
9. 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 **Deploy Fabric** pull-down, select the **Deploy and Validate** option.
3. On the **Deploy** tab, select the A**dvanced Configuration** link and then click the A**dd Switch Specific Custom Configuration** link.

   The Switch Specific Custom Configuration screen displays.

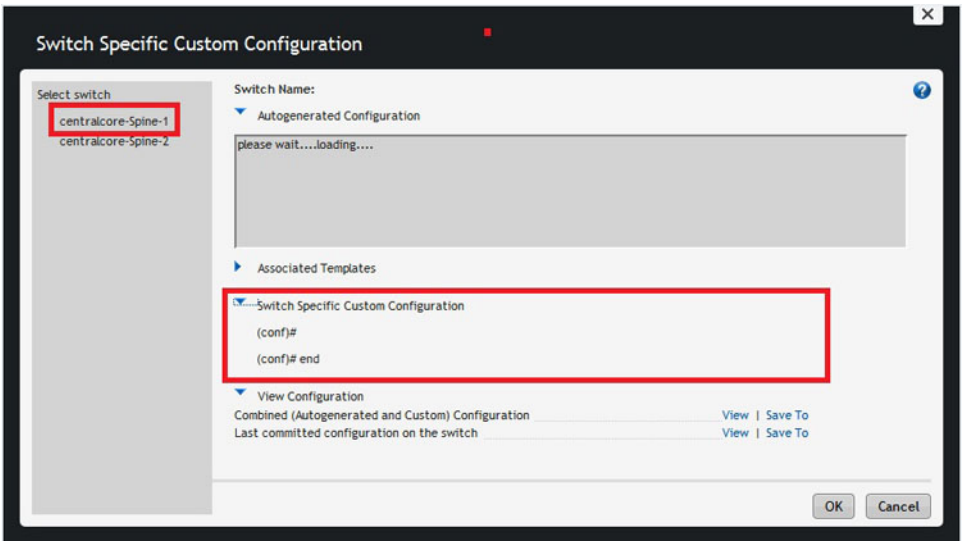


Figure 74. Switch Specific Custom Configuration

   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

To preview the combined configuration:

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, click the **Advanced Configuration** link.

4. Click the **Preview Combined Configuration** screen.
   The **Combined Configuration** screen displays.

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
- Delete Templates
- Copy 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 aggregation switches in the fabric
- All the access switches in the fabric
- All the core switches
- All the switches in the fabric
- All the leafs in the fabric
- All the spines in the fabric

To add templates:

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

To edit 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.

To delete templates:

1. Navigate to the **Network** > **Configure and Deploy** screen.
2. From the **CLI Configuration**, select the **Managing Templates** pull-down menu.
3. Select the template and then click the **Delete Link** option.
4. Click **Yes.**

Copying Templates

You can copy an existing template, modify it, and then apply it to fabric or switch. 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.

To copy 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.

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 aggregation switches in the fabric
- All the access switches in the fabric
- All the core switches
- All the switches in the fabric
- All the leafs in the fabric
- All the spines in the fabric

To add templates:

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

To edit 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.

To delete templates:

1. Navigate to the **Network** > **Configure and Deploy** screen.
2. From the **CLI Configuration**, select the **Managing Templates** pull-down menu.
3. Select the template and then click the **Delete Link** option.
4. Click **Yes.**.

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.

To copy 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 the spines, all the leaves, all the aggregation, all the access, all core switches or a set of switches. When a template is associated to an entire fabric, all spines, or all leaves, or all aggregation, access, or core switches, 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

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:

   - **All** — Associates the template to all the switches in the fabric.
   - **Aggregation** — Associates the template to all the aggregation switches.
   - **Access** — Associates the template to all the access switches.
   - **Core** — Associates the template to all the core switches.
   - **Custom** — Associates the template with specific switches. In the **Available Switches**, select the switches to associate to the template.

- **Leafs** — Associates the template to all the leaf switches.
- **Spines** — Associates the template to all the spine switches.

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 **Deploy Fabric** pull-down, select the **Deploy and Validate** option.
3. On the **Deploy** tab, select the A**dvanced Configuration** link and then click the A**dd Switch Specific Custom Configuration** link.

   The Switch Specific Custom Configuration screen displays.

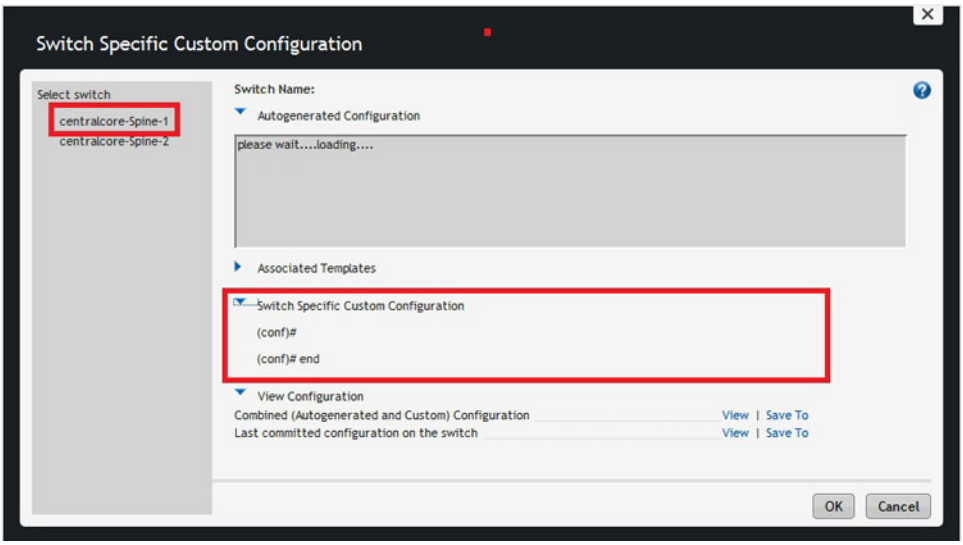


Figure 75. Switch Specific Custom Configuration

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.

10

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.

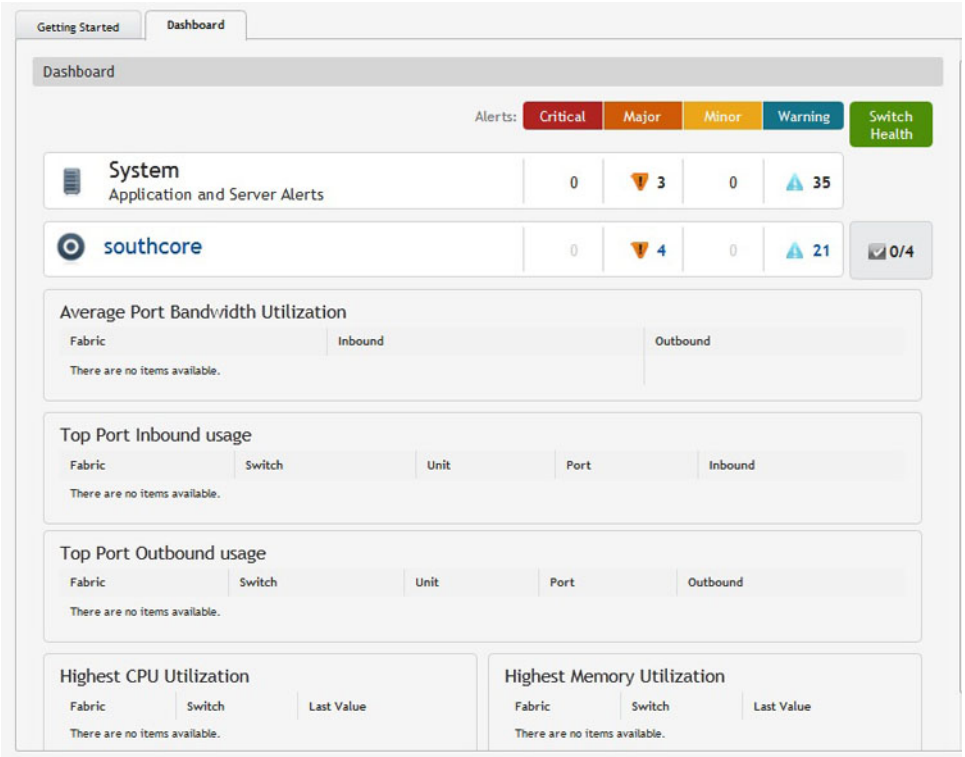


Figure 76. Dashboard

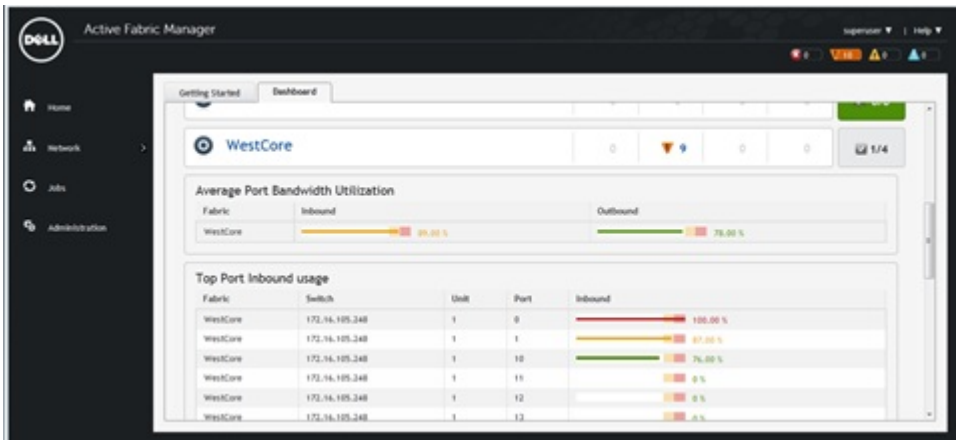


Figure 77. Dashboard with Color Codes

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 35. 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 36. 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 37. 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

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.

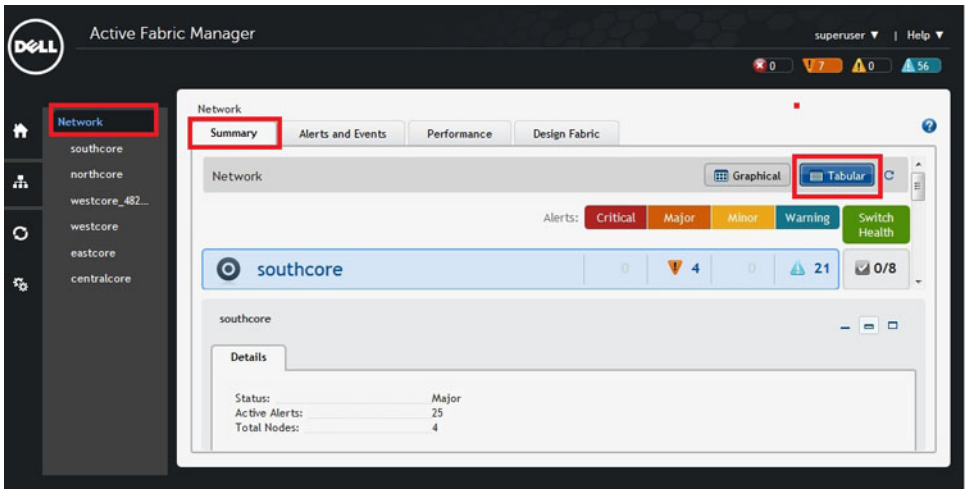
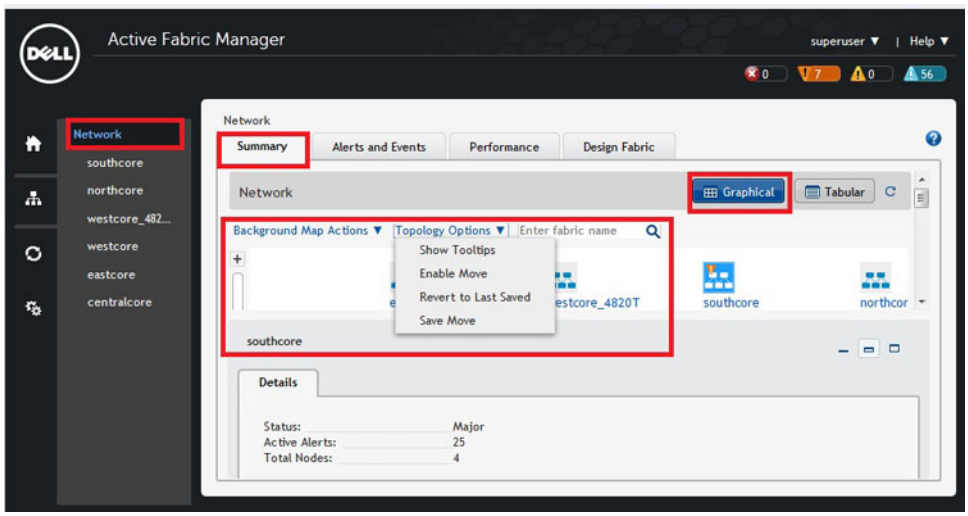


Figure 78. Network Summary Tabular View

Network Topology Graphical View

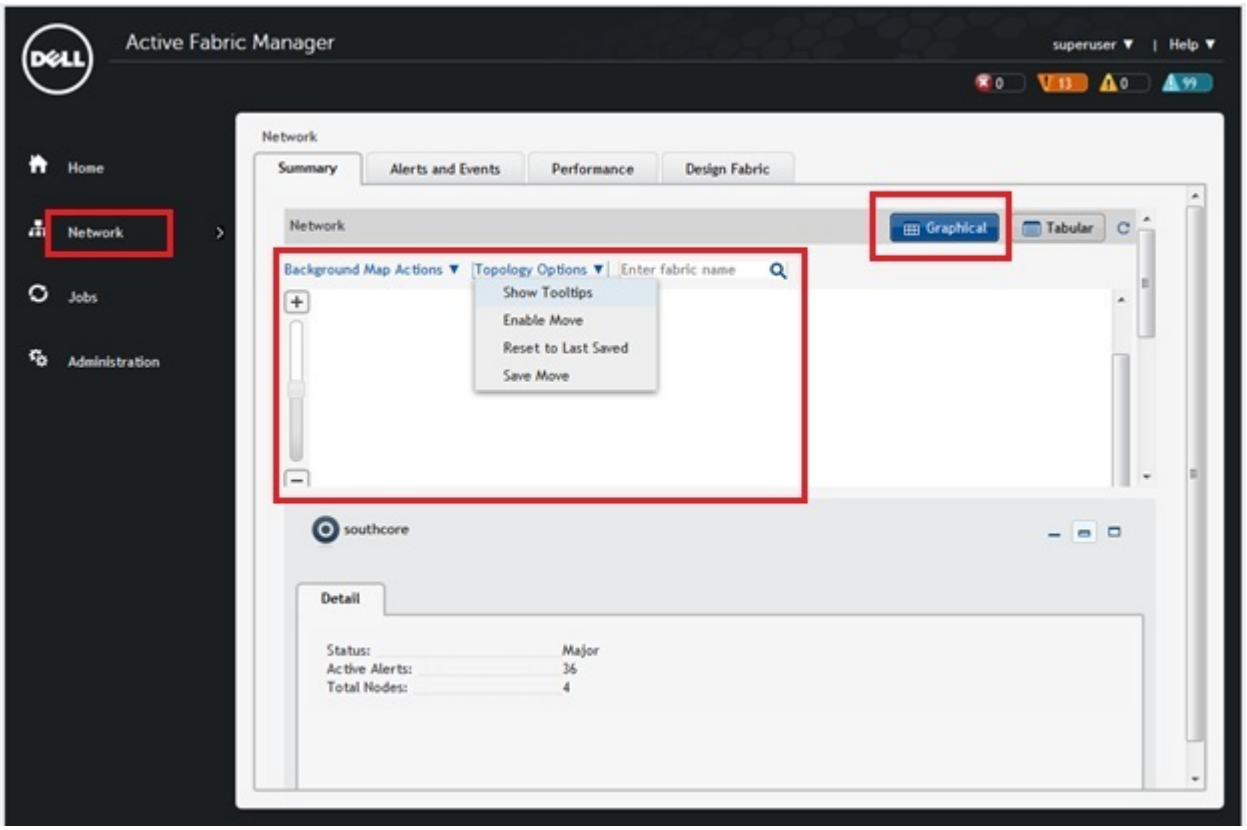


The network topology contains fabric icons. Each fabric icon has the following functions:

- **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

With the fabric tabular view, you can view the switches in the fabric and check alarms. Export your results using the **Export** link.

- You can also manage or unmanage a switch using the **Manage/Unmanage Switch**
- You can display additional performance statistics about a fabric using the **Launch Active Link** option by navigating to the **Network > Fabric level > Tabular** screen. From the **Action** pull-down menu, select the switch row and then click the **Launch Active Link** option.

For information about how to configure the Active Link, navigate to the **Administrative > Settings > Active link Settings** screen. For additional information about the fabric, select the following tabs:

- **Detail**
- **Links**
- **Hardware**
- **VLANS**
- **Port Channels**

Displaying the Fabric in a Graphical 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 or the aggregation switches associated with the access switches by clicking a aggregation switch. 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.
- **Launch Active Link** — Displays additional performance statistics about a fabric in graphical view by navigating to the following screens:
  - **Network >Fabric level > Graphical** screen. Then right click the switch icon and select the **Active Link** option.
  - **Network >Fabric level > Graphical** screen. From the **Action** pull-down menu, select the **Active Link** option.

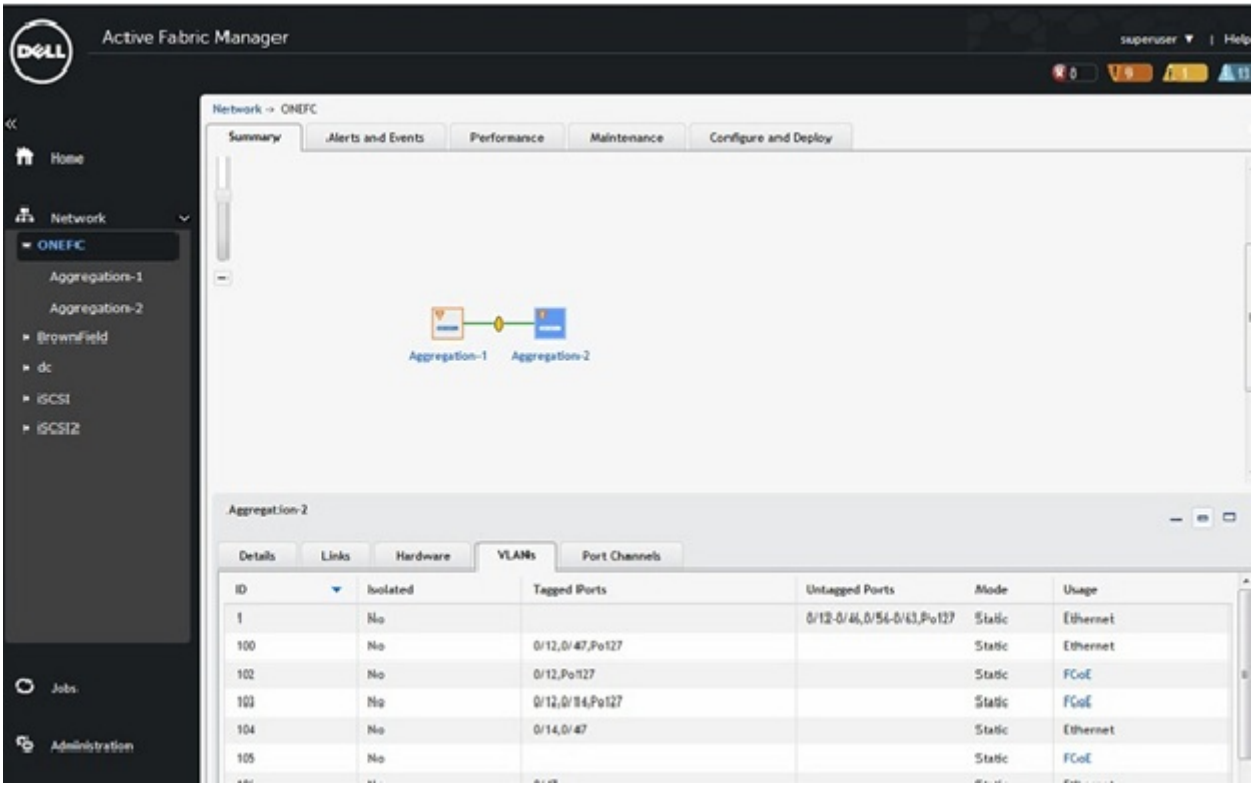


Figure 79. Fabric Summary Screen in Graphical View

For information about how to configure the Active Link, navigate to the Administrative > Settings > Active Link Settings screen.

- **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, aggregation and access, or aggregation, access, and core.
- **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.

Switch Summary

To view the following switch summary information from a graphical view, 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. You can also view this information in a tabular view by selecting the **Tabular** button.

- Click on a port to display information about the state of the port
- Click on the **Port Legends** arrow to display the port legends.
- Click on the **Launch Active Link** from the graphical or tabular view to display additional statistics about a switch through the AFM using a OMNM server. For information about how to configure a element management service, navigate to the Administrative > Settings > Active Link Settings screen.
- Status

- Active Alerts
- Speed
- Manage State

11

Troubleshooting

This section contains the following topics:

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 the AFMwhen you deploy the switch, use the following table:

Table 38. 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

Use the following table to troubleshoot 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

Use the following table to troubleshoot 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. Validation reports any inconsistencies between the design and the discovered fabric. The mismatches are reported by AFM as errors and the corresponding alarms that are generated.

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

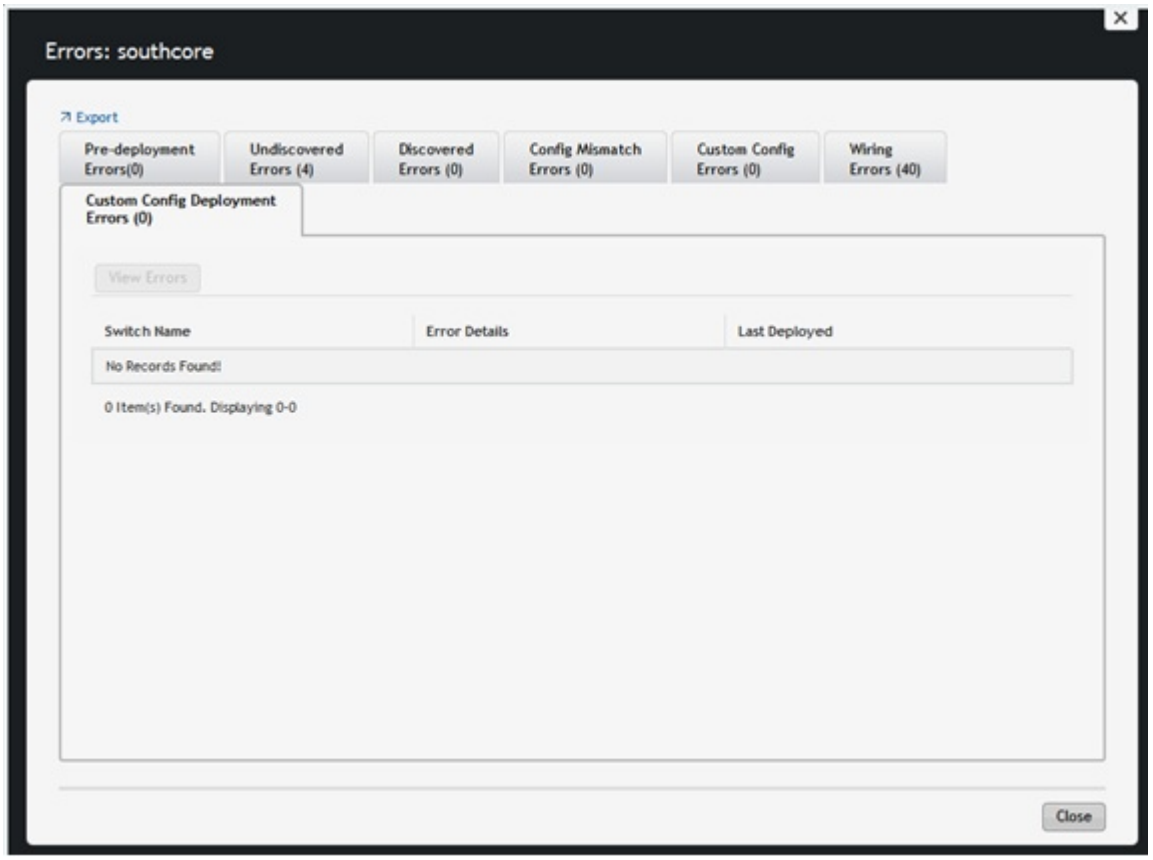


Table 39. Configuration Errors

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 40. 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 41. 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 42. 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 43. 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.

Use the following table to diagnose AFM deployment tasks that have failed.

Table 44. AFM Deployment Tasks

AFM Deployment Task	Error Status	Recommended Action
Verify switch eligibility	Eligibility check for deployment: Failed	VLT switch deployment needs management ip for all its peers
Ping verification	Ping verification: Failed	Verify DHCP offer is received in the device console; Power cycle if needed
Telnet/SSH connectivity verification	Telnet/SSH session verification: Failed	Verify Telnet/SSH connection; Verify DHCP offer is received in the device console; Power cycle if needed

Reset to factory defaults	Reset to factory defaults task: Failed	Verify Telnet/SSH connectivity and deploy again
Minimal configuration upload to switch	Minimal config upload: Failed	Verify Telnet/SSH connectivity and deploy again
	Minimal config upload on Unit-1: Failed	Verify Telnet/SSH connectivity and deploy again
Reload of switch	Reboot of switch: Failed	Verify Telnet/SSH connectivity and deploy again
Boot image error	Boot image was not loaded from flash	Change the boot image path to flash by executing the CLI command through console session.
Stack unit cleanup	Stack unit renumbering task: Failed	Verify Telnet/SSH/SNMP connectivity
Upgrade standby	Upgrade standby: Failed	Standby MAC not found or reported card problem, verify standby switch
Full configuration file transfer	Full config file transfer to TFTP/FTP server: Failed	Verify the TFTP/FTP connectivity. Verify FTP credentials
TFTP/FTP connectivity	TFTP/FTP connection issue between switch and TFTP server	Verify TFTP/FTP connectivity between the switch and TFTP server
Full configuration upload to switch	Full config upload: Failed	Verify TFTP/FTP and Telnet/SSH connectivity and deploy again.Or Verify optional modules have been installed per fabric design. Verify whether AFM supported software version is used.
Smart script transfer failed	Smart script transfer: Failed	Verify Telnet/SSH connectivity and deploy again
Wiring validation	Unable to validate Wiring	Verify SNMP connectivity
	Wiring Errors Exists	Review error details in Errors screen
Merge configuration changes	Apply configuration changes: Failed	Verify Telnet/SSH connectivity and deploy again
Custom configuration upload	Custom configuration upload: Failed	Verify Telnet/SSH connectivity and deploy again
Backup running configuration	Backup config: Failed	Verify Telnet/SSH connectivity and deploy again

TFTP/FTP Error

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

Table 45. 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 or access downlink connections to the ToR:

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

12

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.

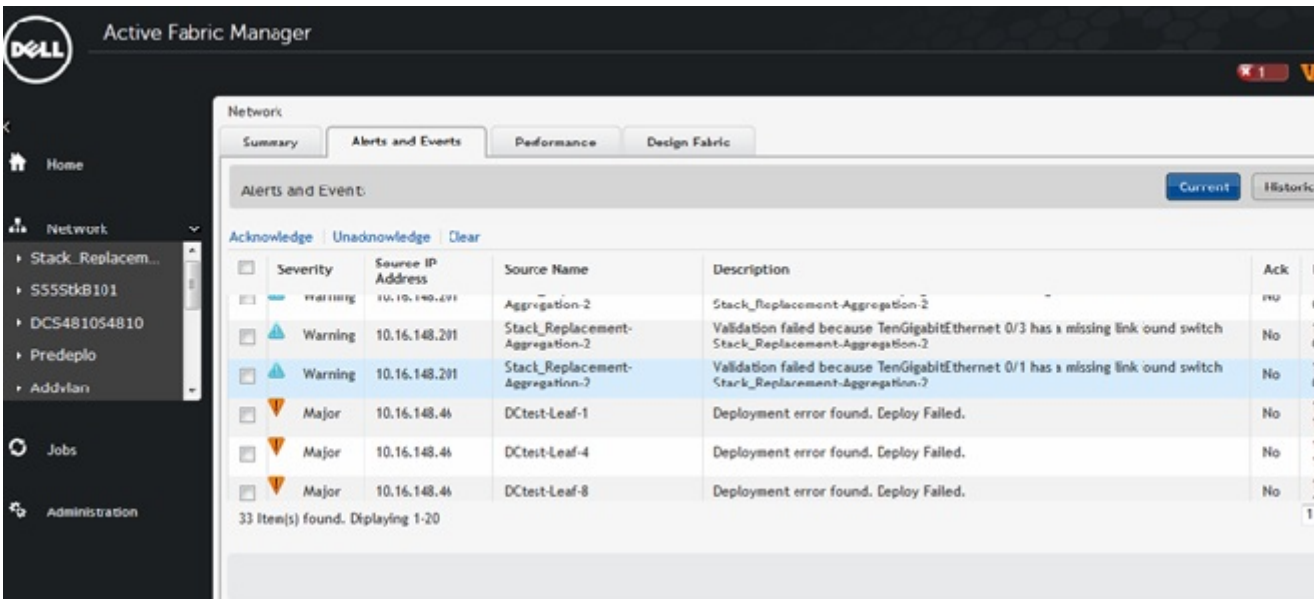


Figure 80. Network Alerts

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

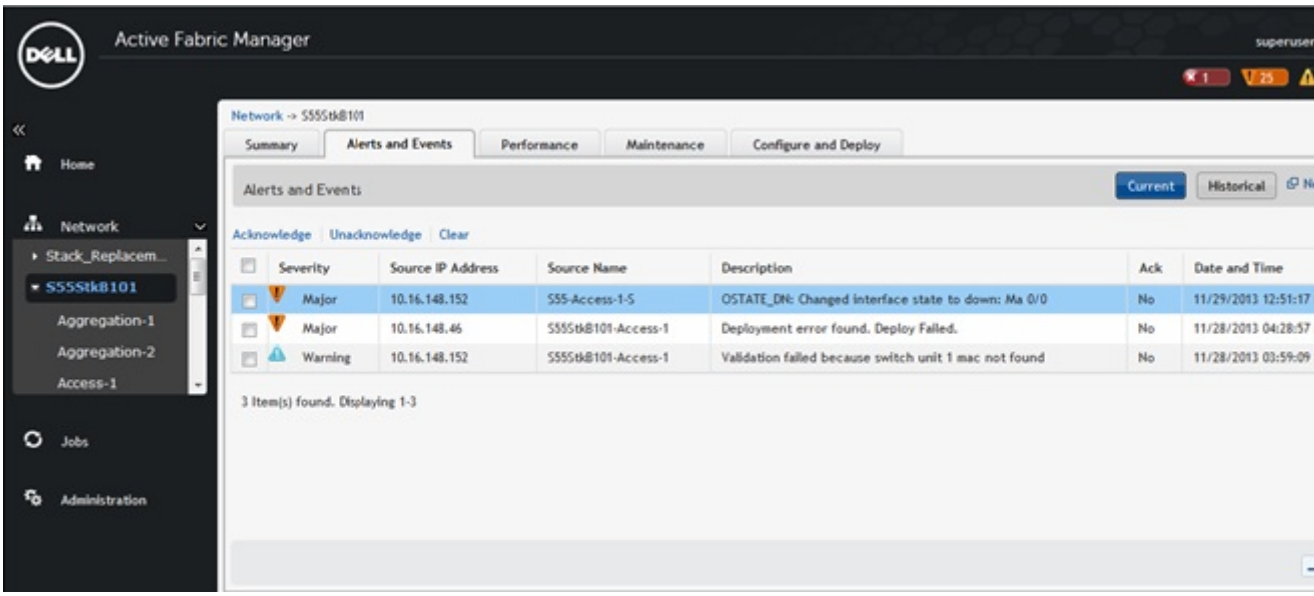


Figure 81. Fabric Alerts

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

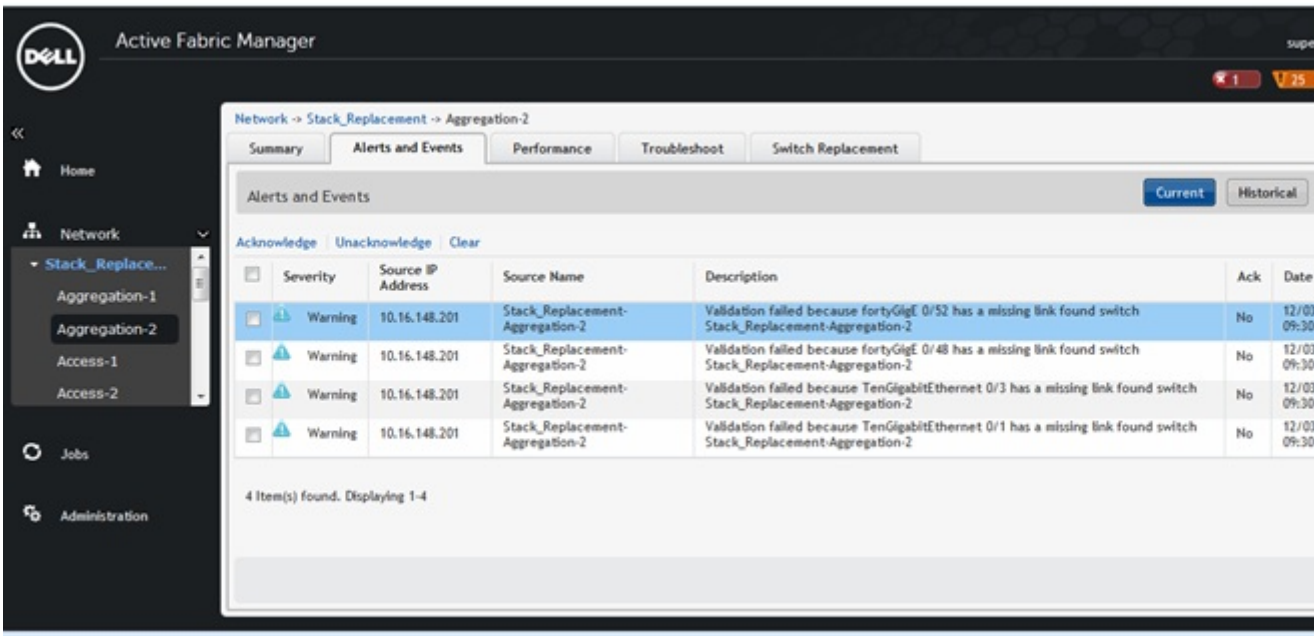


Figure 82. Switch Alerts

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.

13

Performance Management

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

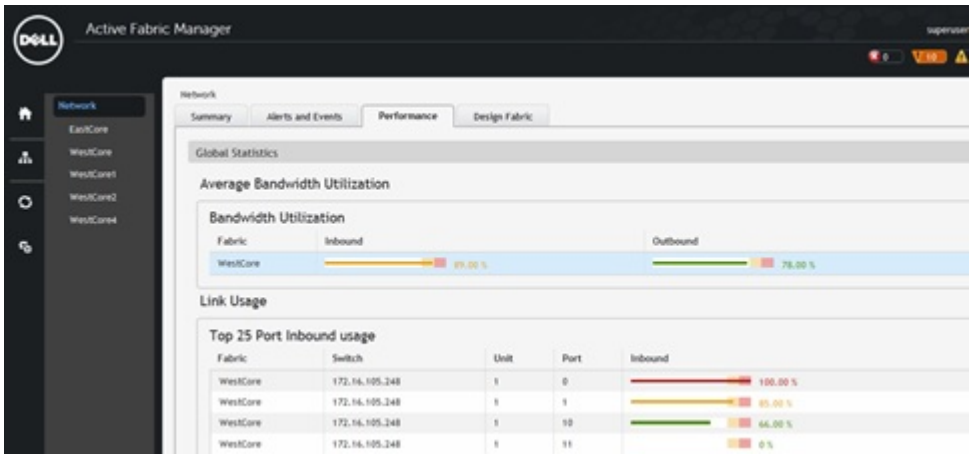
This section contains the following topics:

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

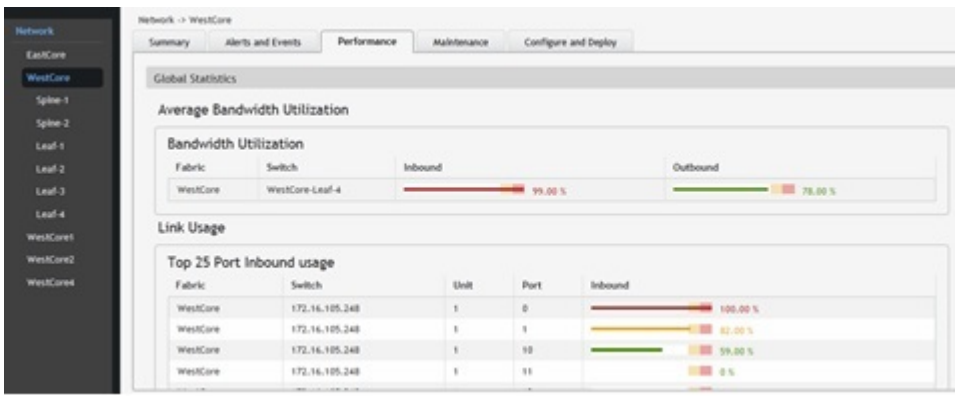
For information about the color codes for the historical data, see Dashboard.



Fabric Performance Management

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

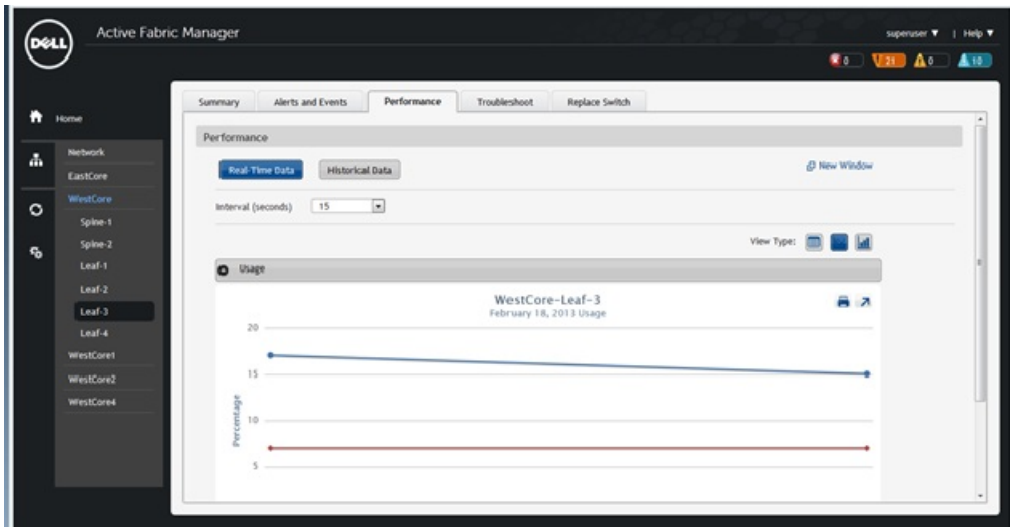
- Bandwidth utilization
- Top 25 port inbound usage
- Top 25 port outbound usage
- Top 10 highest CPU utilization
- Top 10 high memory utilization



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.

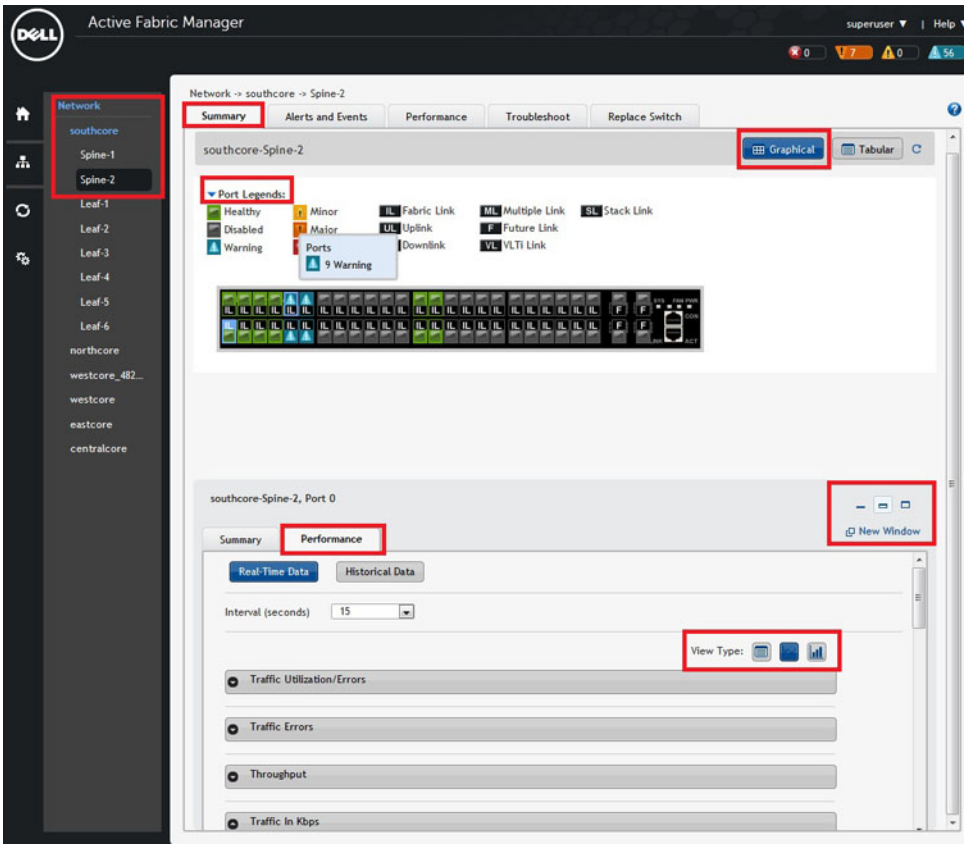


Figure 83. Displaying Summary of Port Performance

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.

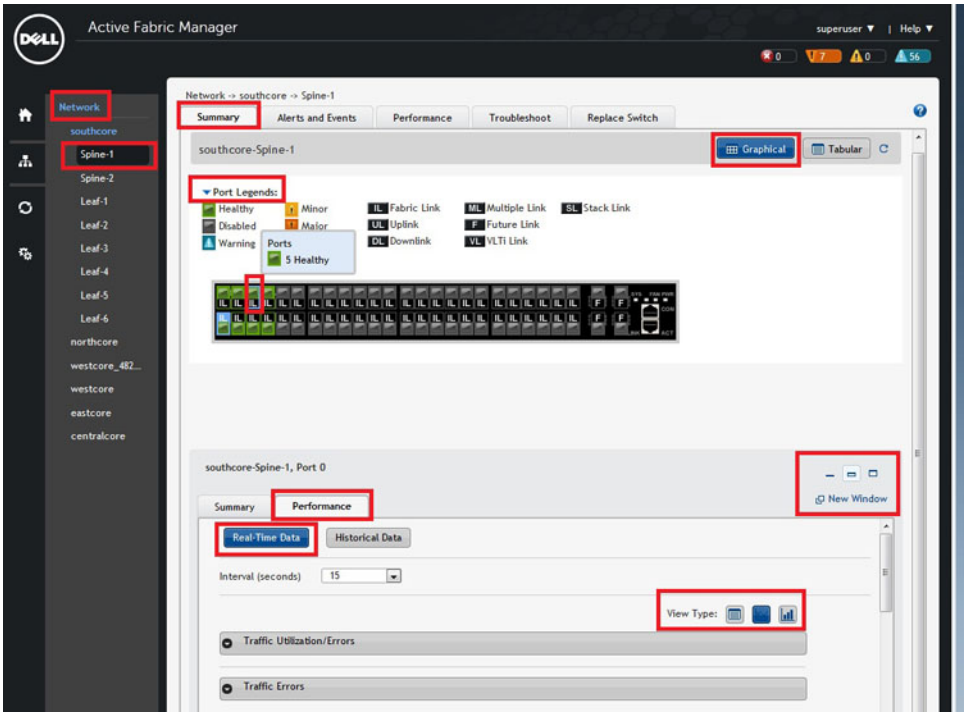


Figure 84. Display Detailed Port Performance

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:

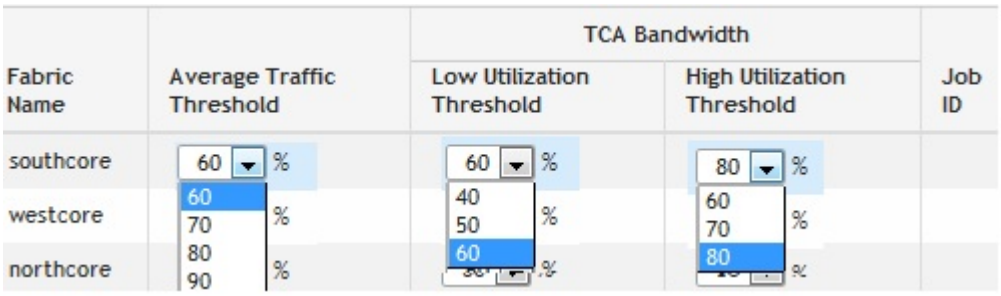
1. Navigate to the **Jobs > Data Collection** screen.
2. Click the **Schedule Data Collection** link.
   The **Edit Data Collection** window displays.
3. Check the fabrics to enable data collection.
4. From the **Polling Rate** pull-down menu, select the polling rate.
   a. **15 Minutes (default)**
   b. **30 Minutes**
   c. **45 minutes**
   d. **1 Hour**

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

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.

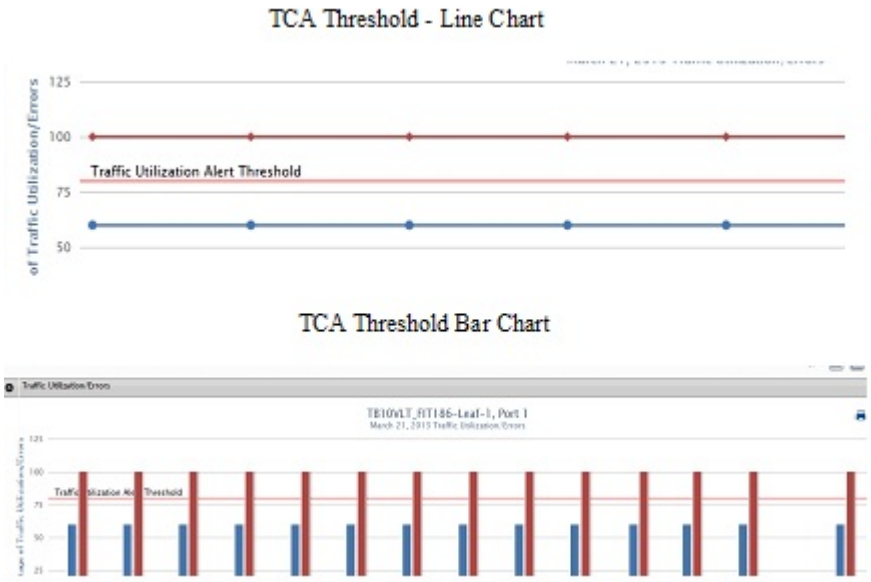


Figure 85. Example: TCA Exceeds the Threshold

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 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**.

14

Maintenance

This section contains the following topics:

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:

Attention: With an IOA blade switch, you can only restore the startup 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 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.

Viewing and Editing the Switch Backup Configuration

Use the **View/Edit** option to edit the running or startup configuration on the deployed devices. The edited configuration becomes available when you restore the switch backup configuration.

To view and edit the switch backup configuration:

1. Navigate to the **Network** > *Fabric Name* > **Maintenance** screen.
2. Click the **Backup Switch** option in the upper right of the screen and then click the **View/Edit** option.

   The **View and Edit Switch Backup Screen Configuration** displays.

   The following options are available:
   - **Edit** — Edit the running or startup configuration on the deployed devices.
   - **View Difference** — View difference between the running and startup configuration on the deployed devices.
   - **View** — View the running or startup configuration on the deployed devices.

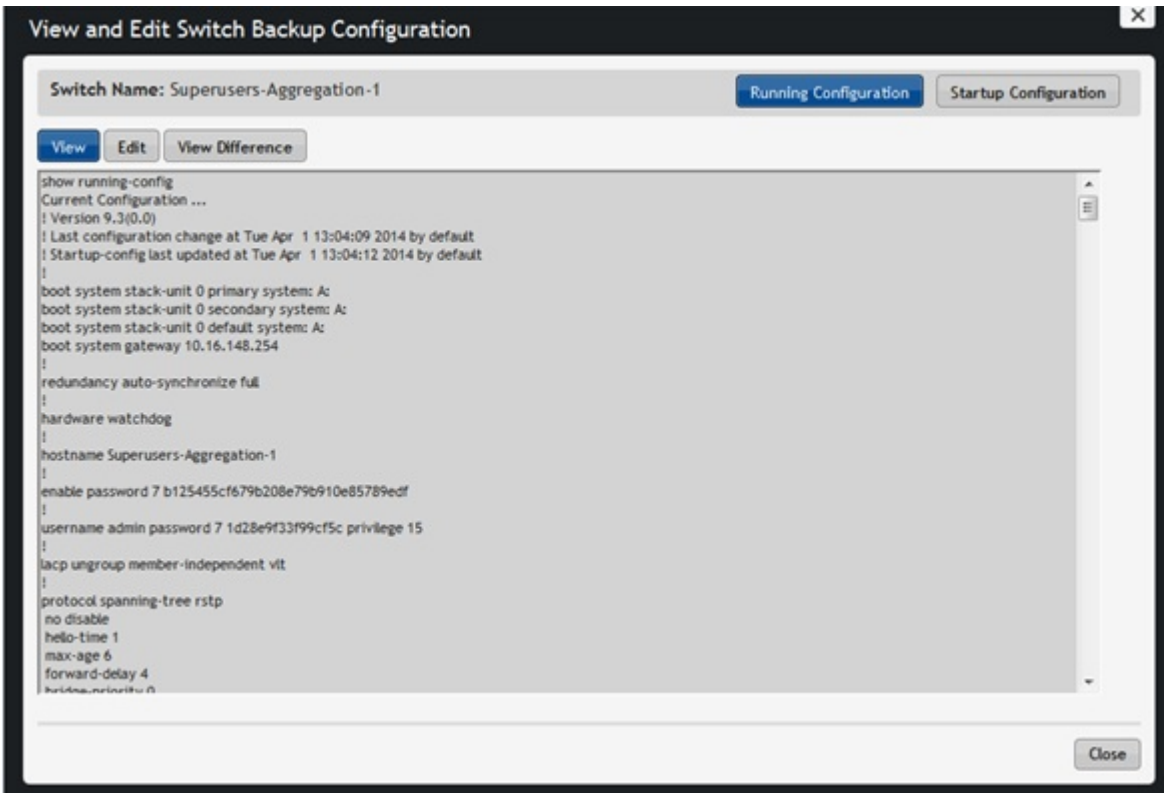


Figure 86. View and Edit Switch Backup Screen Configuration Screen

3. Click the **Close** button to exit from this screen.

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 an IOA Blade Switch

This section describes how to replace an IOA blade switch. For information about how to replace non-IOA blade switches, see Replacing a Switch.

To replace an IOA Blade switch in a M1000e chassis:

1. Remove the faulty IOA blade switch from the M1000e chassis.
2. Replace the faulty IOA blade switch with the new IOA blade switch in the **same** slot of the M1000e chassis.
3. Rediscover the chassis using the **Network** > **Design Fabric** > **Discover Status** screen.

NOTE: During the rediscover process, AFM sets the previously configured IP address on the replacement IOA blade switch.

4. Deploy the successfully discovered replacement IOA blade switch with the **Overwrite entire configuration on the switch deploy** option.

Replacing a Switch

To replace a switch in the fabric:

1. Decommission Switch
2. Replace Switch
3. Deploy Switch

   You must replace the switch with same type of switch.

Attention: If you are replacing an IOA blade switch, see Replacing an IOA Blade Switch.

Step 1: Decommission a Switch

Key Considerations

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" and the AFM stops managing this switch.
- The new switch should use the factory default setting.
- If the old switch is used, reset it to the factory default setting.
- AFM generates information for Return Material Authorization (RMA), which you submit to iSupport.

NOTE:
You must replace the switch with the same type of switch. See Replacing a Switch.

To decommission a switch:

1. Navigate to the **Network** > *Fabric Name* > *Switch Name*.
2. Click the **Switch Replacement** tab.

   The **Switch Replacement Summary** screen displays.
3. Click the **Decommission Switch** link.

   The **Decommission Switch** screen is displayed.
4. Review and follow the instructions on the **Decommission** screen.
5. 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 representative to arrange switch replacement at the iSupport Portal at http://www.force10networks.com/support/.
6. Once a replacement switch is available, click the **Replace Switch** link.

Step 2: Replacing a Switch

Pre-requisites

Before you replace a switch, gather the following useful information:

- Obtain the system MAC address, service tag and serial number for the new switch to be used for replacement, provided from Dell.
- Location of the switch, including the rack and row number from your network administrator or operator.
- Remote Trivial File Transfer Protocol (TFTP) / File Transfer Protocol (FTP) address from your network administrator or operation.
- Last deployed FTOS Software Image for switch being replaced should be on the TFTP/FTP site. The software images on the TFTP/FTP site is used by the switch to install the appropriate FTOS software image and configuration file.
- Dynamic Host Configuration Protocol (DHCP) server configuration will need update. If remote DHCP server is used then you need to manually update the same based on configuration provided by AFM. If local DHCP server is used, AFM will update the DHCP server automatically. After you power cycle the switches, the switches communicate with the DHCP server to obtain an 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 bare metal provisioning (BMP).

NOTE: The replacing a switch feature is not supported when you discover an existing fabric. For information about discovering existing fabrics, see Discovering an Existing Fabric. For information about how to replace a switch, see Replacing a Switch.

Attention: If you are replace an IOA blade switch, see Replacing an IOA Blade Switch.

To replace a switch:

1. Navigate to the **Network** > *Fabric Name* > *Switch Name* screen.
2. Click the **Switch Replacement** tab and then click the **Replace Switch** link.
3. Review the introduction and instructions on the **Switch Cabling** screen.
4. 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.
5. Click the **Next** button.

   The **MAC Replacement** screen displays.
6. In the **MAC Replacement** screen, enter the following information for the replacement switch:
   a. The new serial number in the **New Serial Number** field.
   b. The new service tag in the **New Service Tag** field.
   c. The new system MAC address for the replacement switch in the **New MAC address** field.
7. Click the **Next** button.

   The **DHCP** screen is displayed.
8. Save the replacement switch DHCP configuration file.
9. Review the **Summary** screen and then click the **Finish** button.
10. Before you deploy the switch:
    a. If you are using a remote DHCP server, integrate the new DHCP file, which contains the system MAC address of the replacement switch and then restart the DHCP service.
    b. Rack your hardware according to the wiring plan.
11. Click the on the **Deploy Switch** link.

Step 3: Deploy Switch

To deploy a replacement switch:

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

   Note: If you make changes to the 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 Server

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**

     If the location is a remote server, enter the URL location of the RPM file on the remote server.

     1. From the **Protocol Type** pull-down menu, select the protocol type: **https**, **ftp**, or **sftp**
     2. Specify the path of the RPM packaging file using the following formats:

        Important: The RPM file name must start with AFM and must end with ".noarch.rpm"; for example, **AFM2.5.0.79.noarch.rpm**

        - **https**://*ipaddress*/*path_to_rpm.file*
        - **ftp**://*ipaddress*/*path_to_rpm.file*
        - **sftp**://*ipaddress*/*path_to_rpm.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.
   - **AFM Upload/Download** — The update is copied to the standby partition on the server but will not be applied. This option does not cause a restart. You must manually triggered the update from the AFM server server update page.
   - **Apply Installation and Restart Server**— The update is copied to the standby partition on the server. The update is applied and the restart 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.

15

Jobs

This section contains the following topics:

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.

   - **2 Tier distributed core filtering options** — All, Spine, and Leaves
   - **2 Tier VLT options** — All, Aggregation and Access
   - **3 tier filtering options** — All, Core, Aggregation and Access
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.
   - **2 Tier distributed core filtering options** — All, Spine, and Leaves
   - **2 Tier VLT options** — All, Aggregation and Access
   - **3 tier filtering options** — All, Core, Aggregation and Access
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.

- **2 Tier distributed core filtering options** — All, Spine, and Leaves
- **2 Tier VLT options** — All, Aggregation and Access
- **3 tier filtering options** — All, Core, Aggregation and Access

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.
      - **2 Tier distributed core filtering options** — All, Spine, and Leaves
      - **2 Tier VLT options** — All, Aggregation and Access
      - **3 tier filtering options** — All, Core, Aggregation and Access

   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 pull-down menu select one of the following options:
   - **2 Tier distributed core filtering options** — All, Spine, and Leaves
   - **2 Tier VLT options** — All, Aggregation and Access
   - **3 tier filtering options** — All, Core, Aggregation and Access
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:
      - **2 Tier distributed core filtering options** — All, Spine, and Leaves
      - **2 Tier VLT options** — All, Aggregation and Access
      - **3 tier filtering options** — All, Core, Aggregation and Access

   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 the **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.

16

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.

Active Link Settings

To display additional performance statistics through the AFM using a Dell OpenManage Network Manager (OMNM) server, use the **Active Link Settings** option. OMNM monitors and manages Dell network devices. It automates common network management operations and provides advanced network element discovery, remote configuration management, and system health monitoring to proactively alert network administrators to potential network problems. OMNM provides SOAP based web services to allow 3rd parties to integrate with it.

AFM provides integration with the Dell OMNM web application as view only. When the **Active Link** is started, it displays another browser to view AFM performance statistics. For information about how to install and configure OMNM, see **http://www.dell.com/support/Manuals/us/en/555/Product/dell-**

openmanage-network-manager. Refer to the release notes or *AFM Installation Guide* for the supported versions of OMNM.

Important: Install the Dell OMNM software onto a different server other than the AFM. To activate the performance statics, login directly as write permission into Dell OMNM web service.

Important: By default, the web service is turned off in the OMNM server.

To use the OMNM web service:

1. On the OMNM server go to the server installation directory.
2. Navigate to the **installed.properties** file at **C:\ProgramFiles\Dell\OpenManage\Network Manager\owareapps\installprops\lib**
3. Turn off the Application Server and Synergy Network Management server.
4. Add the following three lines in the **installed.properties** file:

```
com.dorado.core.ws.disable=false
com.dorado.core.ws.legacy.soap.enabled=true
oware.webservices.authrequired=false
```

5. Turn on the **Resource Monitoring** option to enable performance monitoring.
6. Start the Application server and Synergy Network Management server.

Before you configure the Active Link, gather the following OMNM server information:

- OMNM server IP address
- communication protocol (HTTP or HTTPS)
- user name and password

The AFM provides the Active Link server and Active Link webs service status at the following screens:

1. **Administration-> Settings > Active Link Settings**
2. **Network** > **Alerts and Events** screen in the **Description** column
3. **Network** > *Fabric* > **Details**
4. **Network** > *Switch* > **Summary**

The **Active Link** feature is disabled when:

- The AFM cannot connect to Active Link server.
- The AFM cannot connect to Active Link web service.
- The selected switch is un-manage by AFM.
- The Active Link server is not configured.

The topology view refreshes every **60** seconds (default). The refresh rate interval can be changed from the **Administration > Settings** > **Client Settings** > **GUI Polling** screen. The link status is refreshed every **60** seconds (default).

You start the Active Link at the following levels:

- AFM UI provides Active Link server status and Active Link WEB Service status at:

  a. **Administration > Settings >Active Link Settings** screen.

b. **Network** > *Fabric* > **Details** screen.

c. **Network** > *Switch* > **Summary** screen.

By default, the topology view and link status refreshes every 60 seconds. To change the interval, navigate to the **Administration > Settings** screen.

The Active link is available at the following screens.

- Navigate to the **Network** > *Fabric* > **Graphical** view. Under the **Action** menu list, select the **Launch Active Link** option.
- Navigate to the **Network** > *Fabric* > **Graphical** view. Right click the switch icon and then select the **Launch Active Link** link.
- Navigate to the **Network** > *Fabric* > **Tabular** view. Under the **Action** menu list, select the switch row and then select the **Launch Active Link** link. The Active Link displays the selected switch view and display performance charts.
- Navigate to the **Network** >*Switch* > **Graphic** view. Click the **Launch Active Link** link. The Active Link displays the selected switch view and performance charts.
- Navigate to the **Network** >*Switch* > **Tabular** view. Click the **Launch Active Link** link. The Active Link displays the selected switch view and performance charts.

To configure active link settings: :

1. Navigate to the **Administration > Settings** screen.
2. Navigate to the **Active Link Settings** area and click the **Edit** link.
3. In the **Active Link** area, check the **Integrate to Dell OpenManage Network Manager (OMNM)** option to display additional performance statistics.
4. In the **Active Link System IP Address** field, specify the Active Link server IP address of the element management system. In the **Communication Protocol** area, select one of the following protocols.
   - **Use HTTP protocol to connect through AFM Server**.
   - **Use HTTPS protocol to connect through AFM Server**.
5. In the **User Name**, specify the Active Link user name.
6. In the **Password** field, specify the Active Link user password.
7. Click the **OK** button.

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** or

   SSHv2.
4. In the **User Name** field, enter the user name.

5. In the **Password** field, enter the password.
6. In the **Confirm Password** field, confirm the password. The privilege level is a read-only field and is set at 15.
7. In the **Enable Password** field, enter a password for the privilege level.
8. In the **Confirm Enable Password** field, confirm the enabled password for the privilege level.
9. 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 used 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:

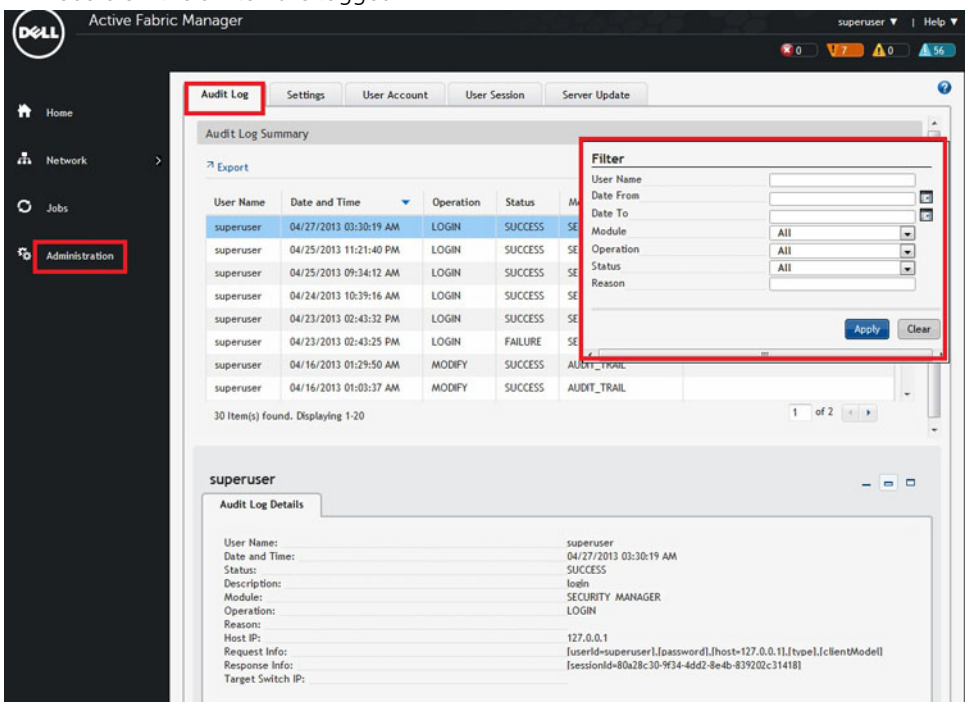
- **Username**
- **Session Login Time**
- **Client IP Address**
- **Current Session**

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.