Dell EMC Networking OS10 Enterprise Edition Quick Start and Interoperability Guide

An Introduction Guide to OS10 Enterprise Edition

Abstract

Quick start and interoperability guide to assist with the installation, upgrade, and set up of in-band and out-of-band management, authentication, and interoperability between Dell-Dell and Dell-OEM devices.

July 2018

Revisions

Date	Description
July 2018	Initial release

Acknowledgements

This paper was produced by the following members of the Dell EMC Networking Solutions Engineering team:

Author: Victor Teeter

Table of contents

Revisions 2
Acknowledgements 2
Introduction 5
1 Dell EMC Networking OS10EE switches used in this guide 6
1.1 Initial switch settings 6
1.2 Cisco Nexus switches 7
2 OS10EE installation and upgrades 8
2.1 Preparation 8
2.1.1 Acquire operating system image 8
2.1.2 Connect to the switch 9
2.2 Upgrade from current (non-OS10) OS to OS10EE using ONIE 9
2.2.1 Configure USB drive for OS10EE installation 11
2.2.2 Manual install using USB 11
2.3 Upgrade OS10EE to a current version using OS10EE commands 12
2.3.1 Install directly from the TFTP server 14
2.4 Zero-touch deployment 15
2.5 Troubleshooting OS10EE installations 15
3 Management network 17
3.1 OOB management network configuration 17
3.1.1 Configure management IP addresses 19
3.2 In-band management configuration 20
3.3 Serial port management 21
4 Security basics 22
4.1 VTY ACLs 22
4.2 RADIUS, TACACS+, and local authentication 22
4.2.1 Configure authentication methods 23
4.3 Management VRF 25
5 Connecting Dell EMC switches 28
5.1 Port Channels 28
5.2 VLANs 29
5.2.1 Changing the native VLAN 31
5.3 Spanning Tree 31
5.3.1 STP edge ports 33
5.4 VLT 33
6 Connect Dell EMC to third party switches 36

6.1 Port channels 36
6.2 VLANs 38
6.2.1 Changing the native VLAN 40
6.3 Spanning tree protocol 40
6.3.1 STP edge ports 42
A Technical support and resources 43
B Hardware and software versions used in this document 44
C Contact technical support 45

Introduction

The Dell EMC Networking OS10EE Enterprise Edition, or OS10EE, is a network operating system (NOS) that supports multiple architectures and environments. Networking is moving from a monolithic networking model, where the NOS is embedded with the switch, to a customizable solution. The OS10EE design allows for multilayered disaggregation of the network functionality. The contributions to Open Source provides users the freedom and flexibility in selecting networking, monitoring, management, and orchestration applications to meet their needs. OS10EE bundles an industry-hardened networking stack that features standard L2 and L3 protocols over a standard, and well accepted, CLI interface.

This introduction guide provides examples for the installation of OS10EE and the deployment of the most used features of this operating system, such as setting up VLT, port channels, and VLANs. This guide also demonstrates the integration of Dell EMC switches into existing brownfield environments. For more detailed instructions regarding the features and protocols within this guide, readers are directed to the *OS10 Enterprise Edition User Guide Release 10.4.0E (R3)*.

The steps in this document were validated using specified networking switches and operating system(s) which can be leveraged for other Dell EMC Networking switch models using the same networking OS version, or later.

Table 1 Quick Start Guide expectations

This guide is	This guide is not/does not
Supplemental to the *OS10 Enterprise Edition User Guide Release 10.4.0E(R3)*	A complete guide for OS10EE
An introduction for new OS10EE users	An OEM switch configuration guide
A reference for the most used features of OS10EE	A guide for all features of OS10EE
A secondary reference to the Release Notes	Take precedence over Release Notes

Note: Each new version of OS10EE has unique release notes that should be considered the latest information for the release. The information provided takes precedence over any related information in this or other documentation.

1 Dell EMC Networking OS10EE switches used in this guide

The Dell EMC Networking S4148F-ON in Figure 1 is used for most of the OS10EE command examples in this guide. The OS10EE commands are similar to those of other Dell EMC switches that support OS10EE. The port count and naming conventions may be different depending on your particular switch model.

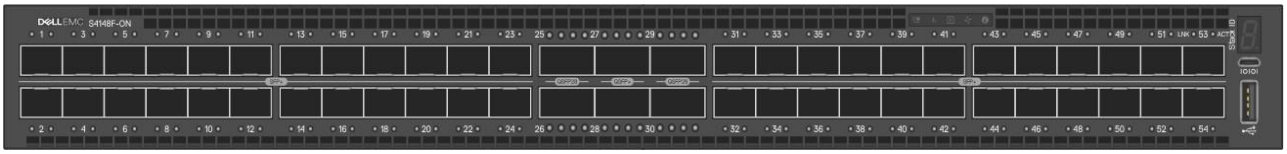

Figure 1 Dell EMC Networking S4148F-ON front view

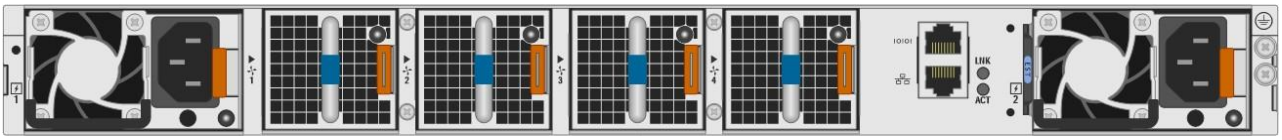

Figure 2 Dell EMC Networking S4148F-ON rear view

The Dell EMC Networking S3048-ON is used in the out-of-band (OOB) examples in this guide. The OS10EE commands are similar to those of other Dell EMC switches that support OS10EE. Port count and naming conventions may be different.

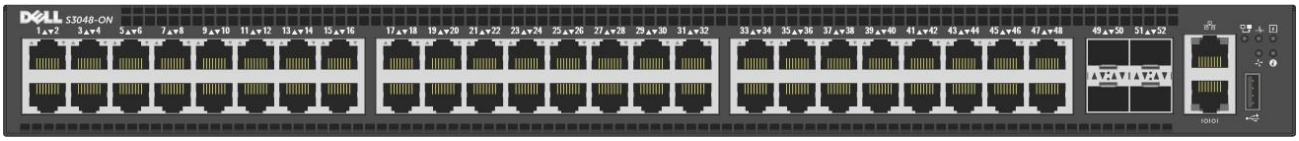

Figure 3 Dell EMC Networking S3048-ON front view

1.1 Initial switch settings

The configuration commands for the examples in this guide assume that the switches start at their factory default settings, with the default login ID (admin) and password (admin). The commands below are used to reset the Dell EMC Networking switches in this guide to factory defaults.

Note: For switches such as the S4148F-ON that support port profiles, resetting to factory defaults also resets the switch to the default port profile. For more information about port profiles, see the *OS10 Enterprise Edition User Guide Release 10.4.0E (R3)*.

To reset OS10EE switches back to the factory default configuration, perform the following steps:

1. Delete the startup-configuration file and reload the switch using the following commands:

```
OS10#delete startup-configuration
    Proceed to delete startup-configuration [yes/no(default)]:yes
OS10#reload

System configuration has been modified. Save? [yes/no]:no
Proceed to reboot the system? [confirm yes/no]:yes
```

   The switch reboots with default configuration settings.

2. To configure the switches, log in using the default username (admin) and password (admin).

1.2 Cisco Nexus switches

Examples provided in this guide show how Cisco Nexus 5600 series, 7000 series, and similar switches, interoperate with Dell EMC switches. The Cisco Nexus N5K-C5672UP switch was used to validate the example commands and common features in this guide.

Use the `write erase` command to reset the Cisco switch to the factory default configuration. Once the reset is complete, the `reload` command is used to restart the switch. After reload, "Power on Auto Provisioning" was not used, the admin password was configured and the Nexus “basic configuration dialog” was not used.

Note: See the Cisco Nexus system documentation for more information.

2 OS10EE installation and upgrades

There are several options for the installation and upgrading of OS10EE. It may be installed manually using the `onie-nos-install <URL>` command while in ONIE, and can be upgraded from the `OS10#` command prompt using the `image install` and `boot system` commands. Several protocols are supported for the transfer of OS10EE files over the network to the switch. These protocols include TFTP, FTP, HTTP, SCP, and SFTP. You can also copy and install the OS from a local file using a USB device, or the IMAGE directory on the switch.

This chapter provides two examples detailing the steps required to:

- Update from any installed (non-OS10EE) OS to OS10EE using ONIE and a USB device
- Update from one version of OS10EE to another using OS10EE commands and a TFTP server

If installed, enter the `show version` command from the `OS10#` command prompt to view the current version of OS10EE on the switch. In the example below, the current OS version is 10.4.0E(R3).

```
OS10# show version
Dell EMC Networking OS10 Enterprise
Copyright (c) 1999-2018 by Dell Inc. All Rights Reserved.
OS Version: 10.4.0E(R3)
Build Version: 10.4.0E(R3.233)
Build Time: 2018-03-30T18:05:41-0700
System Type: S4148F-ON
Architecture: x86_64
Up Time: 22:02:22
```

For details regarding OS10EE installation and updates not covered in this Quick Start Guide, refer to the *Getting Started* chapter of the *OS10 Enterprise Edition User Guide Release 10.4.0E (R3)*. Information on updating or installing using a Zero Touch Deployment through ONIE can be found in the *ONIE User Guide*.

2.1 Preparation

To begin the installation or upgrade process, ensure that the OS10EE image to be installed is acquired and that a proper connection to the switch is present. Network services such as DHCP, TFTP, and FTP, or a USB device, must be ready to accommodate the process as required. This document provides specific steps for each of the examples given, and shows how to use required services for these particular instances.

Note: For installations or upgrades using protocols and services not included in this document, see the *OS10 Enterprise Edition User Guide Release 10.4.0E (R3)*.

2.1.1 Acquire operating system image

The latest OS10EE operating system can be downloaded from either the OS10EE download site (for a trial license), or the Dell Digital Locker (DDL) for a perpetual license beyond the trial period.

1. Sign in to the DDL using your account credentials.
2. Locate the entry for your entitlement ID and order number, then select the product name.
3. From the **Product** page, click the **Available Downloads** tab.
4. Select the OS10EE image to download, then click **Download**.

5. Review the **Dell End User License Agreement** (EULA), and if you agree to the terms provided, click **Yes, I agree.**
6. Select the desired download method for the software files, then click **Download Now**.

Note: Compare checksum values of each downloaded file to ensure integrity.

The new downloaded OS10EE file will be in a **.tar** (archived) format and will need to be unarchived and the contents copied to an accessible location (e.g. USB, IMAGE, TFTP server, etc.) before installing/upgrading. Unarchiving a file may be accomplished using the Linux `tar -xvf file.tar` command or with archiving tools available for Microsoft operating systems such as WinRAR. The file may be transferred to one of the switch's accessible locations using a transport protocol (e.g. TFTP, FTP, etc.). See the OS10EE Release Notes for more information on supported protocols for installation.

2.1.2 Connect to the switch

Use one of the following methods to verify that the system is properly connected before starting installation:

- Connect a serial cable and terminal emulator to the console serial port on the switch. The serial port settings can be found in the *Installation Guide* for your particular switch model. For example, the S4100-ON serial port settings are 115200, 8 data bits, and no parity.
- Connect the management port to the network if you prefer downloading the image over the network. Use the *Installation Guide* for your particular switch model for more information on setting up the management port.

Note: Keep regular backups of switch configurations somewhere off of the switch, and before performing OS updates or changes.

2.2 Upgrade from current (non-OS10) OS to OS10EE using ONIE

This method may be used for upgrading your switch to OS10EE if:

a. The switch is currently running Dell EMC Networking OS9 and the desire is to update to OS10EE
b. The switch is currently running a non-Dell OS, and the desire is to update to OS10EE

This is not the recommended method for updating a switch from one version of OS10EE to another version of OS10EE since it will erase any existing configuration. See the next section for steps in upgrading OS10EE with new versions of OS10EE.

Perform the following steps to uninstall the current OS, then upgrade to OS10EE.

Note: Uninstalling the current OS is recommended, but not required.

1. Reload the switch (if OS9 is currently loaded, use the `reload` command), and press the **ESC** key before the counter reaches zero.

```
Grub 1.99~rc1 (Dell EMC)
Built by root at gbbdev-maa-01 on Sat_Nov_25_12:54:44_UTC_2017
S4000 Boot Flash Label 3.21.2.9 NetBoot Label 3.21.2.9

Press Esc to stop autoboot ... 3..2..1..


Grub 1.99~rc1 (Dell EMC)
Built by root at gbbdev-maa-01 on Sat_Nov_25_12:54:44_UTC_2017
```

```
S4000 Boot Flash Label 3.21.2.9 NetBoot Label 3.21.2.9
+------------------------------------------------------------+
|Dell EMC Networking                                         |
|Dell EMC Networking OS-Boot Line Interface                  |
|DELL EMC DIAG                                               |
|ONIE                                                        |
|                                                            |
|                                                            |
+------------------------------------------------------------+
```

3. Use the down arrow key to highlight ONIE then press the Enter key.
4. An ONIE-enabled device boots up with pre-loaded diagnostics and ONIE software, and displays the following menu:

```
+------------------------------------------------------------+
|*ONIE: Install OS                                           |
| ONIE: Rescue                                               |
| ONIE: Uninstall OS                                         |
| ONIE: Update ONIE                                          |
| ONIE: Embed ONIE                                           |
| ONIE: Diag ONIE                                            |
+------------------------------------------------------------+
```

Only the `ONIE: Uninstall OS` and the `ONIE: Install OS` selections are used in this upgrade example. Table 2 describes the actions for each menu option.

Table 2 GRUB bootloader commands and actions

GNU GRUB menu selection	Actions performed
ONIE: Install OS	• Use for downloading and installing an OS from an URL • Boots to the ONIE prompt • Installs an OS10EE image using the automatic discovery process • Deletes previously installed image and configuration • Starts ONIE with ONIE Discovery Service (factory default boot)
ONIE: Rescue	• Boots to the ONIE prompt • Allows for manual installation of an OS10EE image • Allows for updating ONIE • Useful for running diagnostics manually
ONIE: Uninstall OS	• Does not delete ONIE or diagnostics • Deletes configuration • Erases any installed OS • Restores to factory defaults
ONIE: Update ONIE	• Updates to a new ONIE version • Used for downloading and updating ONIE from an URL • Used for updating ONIE image using the automatic discovery process
ONIE: Embed ONIE	• Formats an empty disk and installs ONIE • Erases any installed OS
ONIE: Diag ONIE	• Runs system diagnostics

5. Select `ONIE: Uninstall OS` to uninstall the operating system currently installed. The uninstallation process takes a few minutes. Once completed, the system automatically reloads and goes into auto-discovery install mode.

Note: During an automatic or manual OS10EE installation, if an error condition occurs that results in an unsuccessful installation, select `Uninstall OS` first to clear the partitions if there is an existing OS on the device. If the problem persists, contact Dell EMC Technical Support.

2.2.1 Configure USB drive for OS10EE installation

Perform the steps in this section to prepare and mount the USB drive on the switch. This process is required for both automatic and manual installations using USB.

1. Extract the .tar file and copy the contents to a FAT32 formatted USB flash drive.
2. Plug the USB flash drive into the USB port on the switch.
3. From the `ONIE:/ #` command prompt, enter the following commands:

Note: To get to the `ONIE:/#` command prompt from the ONIE menu, select `ONIE: Install OS`, then press the **Ctrl-C** key sequence to abort.

```
ONIE:/ # onie-discovery-stop  (this optional command stops the scrolling)
ONIE:/ # mkdir /mnt/usb
ONIE:/ # cd /mnt
ONIE:/mnt # fdisk -l    (this command shows the device USB is using)
```

4. All of the switches storage devices and partitions are displayed. Use the device or partition that is formatted FAT32 (example: /dev/sdb1) in the next command.

```
ONIE:/mnt # mount -t vfat /dev/sdb1  /mnt/usb
ONIE:/mnt # mount -a
```

The USB is now available for installing OS10EE onto the switch.

2.2.2 Manual install using USB

A USB device may be used to manually install or upgrade OS10EE. Run the following commands to complete this installation:

Note: The USB must be prepared and mounted using the instructions in section 2.2.1 above before performing the steps in this section. To get to the `ONIE:/#` command prompt from the ONIE menu, select `ONIE: Install OS`, then press the **Ctrl-C** key sequence to abort.

1. For convenience, use the output of the following command to copy/paste the .bin filename into the install command below.

```
ONIE:/ # ls /mnt/usb
```

2. Change to the usb directory.

```
ONIE:/ # cd /mnt/usb
```

3. Manually install using the `onie-nos-install` command. If installing version 10.4.0E(R3), the command is:

ONIE:/mnt/usb # onie-nos-install PKGS_OS10-Enterprise-10.4.0E.R3.233-installer-x86_64.bin

The OS10EE update takes approximately 10 minutes to complete and boots to the `OS10 login:` prompt when done. Several messages display during the installation process.

4. After the installation is complete, log in to OS10EE and run the `show version` command to verify that the update was successful.

```
OS10# show version
  Dell EMC Networking OS10 Enterprise
  Copyright (c) 1999-2018 by Dell Inc. All Rights Reserved.
  OS Version: 10.4.0E(R3)
  Build Version: 10.4.0E(R3.233)
  Build Time: 2018-03-30T18:05:41-0700
  System Type: S4148F-ON
  Architecture: x86_64
  Up Time: 00:02:14
```

2.3 Upgrade OS10EE to a current version using OS10EE commands

Using OS10EE commands is the recommended way to upgrade from one OS10EE version to another OS10EE version. New versions of OS10EE can contain important updates, fixes or new features. In the example below, OS10EE version 10.4.0E (R3) is upgraded to version 10.4.0E (R3P1).

Perform the steps below to upgrade from one version of OS10EE to another.

Note: It is a best practice to keep regular backups of the switch configuration, and to back it up before making changes or updating the operating system

1. Run the `show boot` command to see the OS10EE versions installed in the Active and Standby partitions.

```
OS10# show boot
Current system image information:
==================================
Type      Boot Type      Active             Standby            Next-Boot
------------------------------------------------------------------------------------------------
Node-id 1 Flash Boot     [A] 10.4.0E(R3)    [B] 10.4.0E(R3)    [A] active
```

The remaining steps transfer a new OS to the switch, install to (overwrite) the Standby partition with the new OS, then activated it.

2. Place the new OS10EE *.bin* file on an accessible TFTP server (e.g. 100.67.2.76) on the network.
3. Use the `image download` command to download the image to the switch from the TFTP server.

```
OS10# image download tftp://100.67.2.76/PKGS_OS10-Enterprise-
10.4.0E.R3P1.237-installer-x86_64.bin
```

Note: If the file does not appear to be transferring to the switch, check the TFTP server log. This issue is commonly caused by an incorrect management gateway on the switch, or firewall settings on the network or locally on the server.

4. While the file is transferring, view the download status using the `show image status` command. The file has completed transferring to the switch when `"Completed: No error"` is seen in the **State Detail** field.

```
OS10# show image status
```

```
Image Upgrade State:     idle
================================================
File Transfer State:     idle
------------------------------------------------------------
  State Detail:          Completed: No error
  Task Start:            2018-05-30T22:55:00Z
  Task End:              2018-05-30T23:06:38Z
  Transfer Progress:     100 %
  Transfer Bytes:        453762947 bytes
  File Size:             453762947 bytes
  Transfer Rate:         650 kbps

Installation State:      idle
------------------------------------------------------------
  State Detail:          No install information available
  Task Start:            0000-00-00T00:00:00Z
  Task End:              0000-00-00T00:00:00Z
```

5. Use the `dir image` command to see the file on the switch.

```
OS10# dir image
Directory contents for folder: image
Date (modified)  Size        Name
-------------------  -----------   ------------------------------------------------------------
2018-05-30T23:06   453762947   PKGS_OS10-Enterprise-10.4.0E.R3P1.237-installer-
x86_64.bin
```

6. Install the 10.4.0E(R3P1) software image to the *standby partition* using the `image install <file-path>` command.

```
OS10# image install image://PKGS_OS10-Enterprise-10.4.0E.R3P1.237-
installer-x86_64.bin
```

7. Enter the `show image status` command to view the status of the current software installation.

```
OS10# show image status
Image Upgrade State:     idle
================================================
File Transfer State:     idle
------------------------------------------------------------
  State Detail:          Completed: No error
  Task Start:            2018-05-30T22:55:00Z
  Task End:              2018-05-30T23:06:38Z
  Transfer Progress:     100 %
  Transfer Bytes:        453762947 bytes
  File Size:             453762947 bytes

  Transfer Rate:         650 kbps

Installation State:      idle
------------------------------------------------------------
  State Detail:          Completed: Success
  Task Start:            2018-05-30T23:29:08Z
```

```
Task End:              2018-05-30T23:38:09Z
```

8. Enter the `show boot` command again to verify that the new OS (R3P1) has been installed in the Standby partition.

Note: Notice that the **Standby [B]** partition is still not active.

```
OS10# show boot
Current system image information:
===================================
Type      Boot Type      Active            Standby            Next-Boot
-------------------------------------------------------------------------------------------
Node-id 1 Flash Boot     [A] 10.4.0E(R3)   [B] 10.4.0E(R3P1)  [A] active
```

9. Use the `boot system standby` command to change the next boot partition to the **Standby** partition.

```
OS10# boot system standby
```

10. Run the `show boot` command again to verify that the Next-Boot is in the **[B] standby** partition.

```
OS10# show boot
Current system image information:
===================================
Type      Boot Type      Active            Standby            Next-Boot
-------------------------------------------------------------------------------------------
Node-id 1 Flash Boot     [A] 10.4.0E(R3)   [B] 10.4.0E(R3P1)  [B] standby
```

11. Run the `reload` command to reboot the switch to the new OS.

```
OS10# reload
```

12. Use the `show version` command to verify that the new version has been installed.

```
OS10# show version
Dell EMC Networking OS10 Enterprise
Copyright (c) 1999-2018 by Dell Inc. All Rights Reserved.
OS Version: 10.4.0E(R3P1)
Build Version: 10.4.0E(R3P1.237)
Build Time: 2018-04-26T10:19:35-0700
System Type: S4148F-ON
Architecture: x86_64
Up Time: 00:02:34
```

2.3.1 Install directly from the TFTP server

An alternative installation method to the one above is available that allows for fewer steps but does not provide verfication during file transfer. Replace steps 3 through 6 above with the one command below to install the OS driectly from the TFTP server.

```
OS10# image install tftp://100.67.2.76/PKGS_OS10-Enterprise-10.4.0E.R3P1
.237-installer-x86_64.bin
```

Return to step 7 in the previous section to continue the process.

2.4 Zero-touch deployment

Automatic (zero-touch) installs of OS10EE images are supported on Dell ONIE-enabled devices. This is a good way to install OS10EE to many new switches at once. After a device successfully boots to `ONIE: Install OS`, auto-discovery obtains the hostname, domain name, Management interface IP address, as well as the IP address of the DNS name server(s) on your network from the DHCP server and DHCP options. The ONIE auto-discovery process locates the stored software image, starts installation, and then reboots the device with the new software image.

Note: If multiple OS's are to be installed at a site, it is recommended to do all of one OS then move to the next, since there can only be one software image available for a zero-touch installation at any given time.

If a USB drive is inserted during this time (using the process in section 2.2.1 above), auto-discovery searches the USB storage supporting FAT32 or EXT2 file systems. It also searches for SCP, FTP, or TFTP servers using the default DNS name, *onie-server,* for the server. DHCP options are not used to provide the IP address of any of these file servers. The auto discovery method repeats until a successful software image installation occurs and reboots the switch.

Steps for an HTTP zero touch installation are as follows:

13. Install a Linux web server (e.g. Apache) that a switch can access once it has obtained its IP address from a DHCP server.
14. Copy the OS10EE .bin installer file to the path shared by the web server (e.g. /var/www/html), and rename it "onie-installer" (or other qualified filename as described in the *ONIE User Guide*).
15. Create a DNS entry to resolve "onie-server" to the Linux web server address.
16. Test web access to the OS10EE installer file by entering **http://onie-server/onie-installer** into the web browser's URL field on a system in the same IP subnet. The directory will open showing the installer file. Click on the file to download a local copy. The test passes when the file successfully downloads.
17. Perform the following with each switch to be installed with OS10EE:
    a. With ONIE installed on the switch (no OS), connect the OOB port to the network containing the web server.
    b. Power up the switch. The switch automatically starts the auto-discovery and zero-touch installation.
    c. Once the switch installs OS10EE, it reboots to the `OS10 login:` prompt. Installation is complete.

For more information on using ONIE for Zero Touch installations, including installations on large networks and those requiring additional network security, see the *OS10 Enterprise Edition User Guide Release 10.4.0E (R3)*. Zero Touch deployment examples may be found in the *ONIE User Guide*.

2.5 Troubleshooting OS10EE installations

The following table shows problems and possible solutions to issues that may be experienced during OS10EE installations.

Table 3 OS10EE installation troubleshooting recommendations

Problem	Solutions
Errors seen during "image download," though the tar file	The OS10EE install .bin file is corrupted when extracted from its .tar file when WinZip is used with its default settings.

appears to have extracted without error Or, the md5 or sha256 checksums do not match after extracting the .bin files from the tar file	Issue is resolved by disabling the “TAR file smart CR/LF conversion” feature enabled by default in WinZip: For newer WinZip versions go to: 1. **Settings** > **WinZip Options** > **Advanced**. **2.** Uncheck **TAR file smart CR/LF conversion** 3. Click **OK**. Close and reopen WinZip. For other versions go to: 1. **Options** > **Configuration** > **Miscellaneous**. **2.** Uncheck **TAR file smart CR/LF conversion** 3. Click **OK**. Close and reopen WinZip. Alternatively, you may use a different unzip utility such as Linux tar or WinRAR.
After installing OS10EE, the GRUB ONIE boot menu (containing “ONIE: Install OS”) continues to reload upon each reboot of the switch	Even after installing OS10EE or DIAG-OS, if you boot into `ONIE Install mode`, ONIE will assume ownership of the switch. ONIE stays in Install mode until OS10EE or the DIAG-OS is successfully installed again. If you want to boot into ONIE for any reason other than installation, use Rescue mode or Update mode. To gain temporary access to the OS10EE that is installed, you may enter “c” at the grub menu, then type “exit” from the grub command line. This will load the grub OS menu where you can select OS10-A or OS10-B to boot the OS. Upon entering the “reload” command in OS10, or power cycling the switch, the ONIE Install mode will resume.
File does not download from web server	By default, certain files (including those without extensions), are not accessible when using some web servers. Check the web server MIME (Multipurpose Internet Mail Extensions) settings and enable downloading of all files, including those without extensions. Check to make sure your filename has been changed to “onie-installer” and not “onie-updater” or other name. Also make sure it has no filename extension. The ONIE itself may also be updated using zero-touch and uses the name “onie-updater” which will not work for updating the NOS.

3 Management network

A management network allows administrators to remotely access all switches on the network for configuring, managing, and analyzing traffic. This prevents having to be physically present at each switch in order to manage it. There are two prevalent approaches for network management: in-band and out-of-band (OOB). An introduction to both are covered in this chapter.

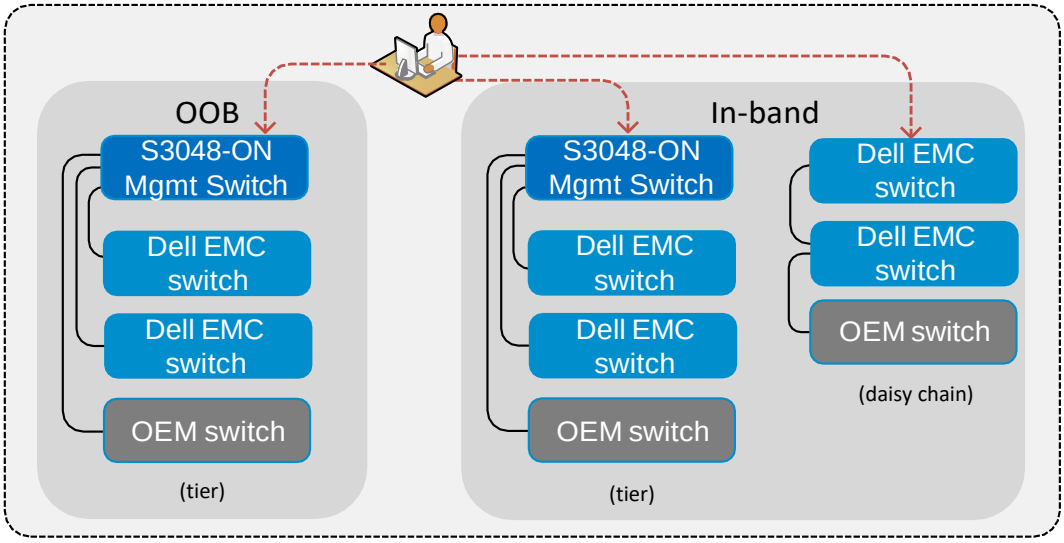

Figure 4 In-band and OOB network management topologies

The method used for management should be carefully considered when designing a network. Switches that use in-band management may become inaccessible if parts of the network are down, but can take advantage of security features such as those provided by access control lists, or ACLs.

A management switch is not required for in-band in order for a management station to achieve one-to-many access of the switches. Administrators can create a tier or daisy-chain network using the management VLAN (requiring two management ports on middle switches).

Note: When a connection is lost, a daisy-chained management network typically blocks administrator access to more switches that on a tiered network.

On any in-band management network, in-band management is lost when a switch goes offline due to misconfigurations, power-cycling, or cable disconnections. In these cases, the administrator can no longer reach affected devices to determine or resolve issues over the network. Until resolved, the switch's serial port must then be used to recover the switch. Extended downtime is often required to access the serial port to restore the switch. SNMP traps, external logging, and other alerts/notifications may also be missed when a switch suddenly goes offline causing further delays in recognition and recovery.

While OOB management typically requires dedicated switching and cabling, it provides an alternate path to circumvent the problems of in-band management. When a switch goes offline due to misconfiguration or a cable disconnect, the OOB management connection remains up. Network administrators are notified immediately through SNMP traps and alerts, and may begin troubleshooting and recovery efforts.

3.1 OOB management network configuration

The OOB management network is a separate network for management traffic only. It is used by administrators to configure, manage, and monitor devices such as switches and servers. Payload traffic

initiated by the network end-users does not traverse the OOB management network. Switches used for management are generally 1GbE. The greatest benefit of using OOB is that you can still access a switch even if part of the network between you and the switch goes down. Figure 5 shows how the Dell EMC Networking S3048-ON switch may be used for this purpose:

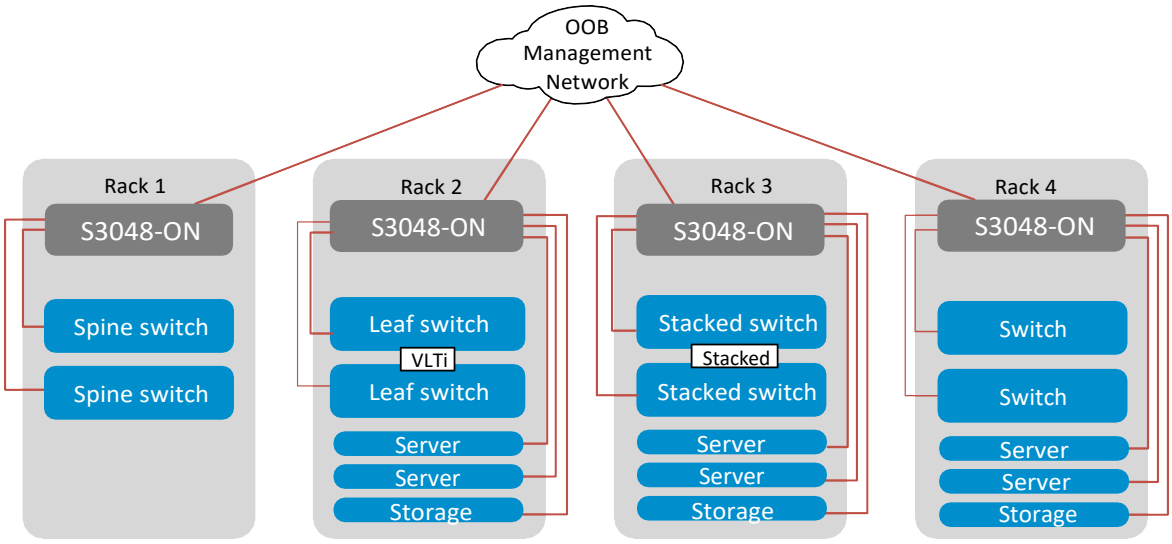

Figure 5 OOB management network example for multiple racks

The figure shows an OOB management network for multiple racks. Each S3048-ON may be used to manage up to 48 devices on the network, typically enough for a single rack of equipment. The switch may then be connected to other adjacent management switches, or upstream to a management core. In Figure 5, the red lines indicate cables connecting all OOB traffic. Note that each device (servers, switches, storage) has a single cable connection attached to the management network. Although a stack of switches is seen as one single switch by other devices on the network, and only one cable connection is required for the entire stack, a second cable is used as a backup in case the stack primary fails.

Note: Figure 5 shows cables used in the management network. In a complete topology picture, each device in the figure would also have in-band cable connections for regular network traffic.

Figure 6 demonstrates how OOB management might look in a single rack. There is one cable from the management switch to each device on the network to be managed. Cables running to Dell EMC switches are connected to the OOB management ports of the switches. Cables running to Dell EMC PowerEdge servers are connected to the iDRAC ports of the servers.

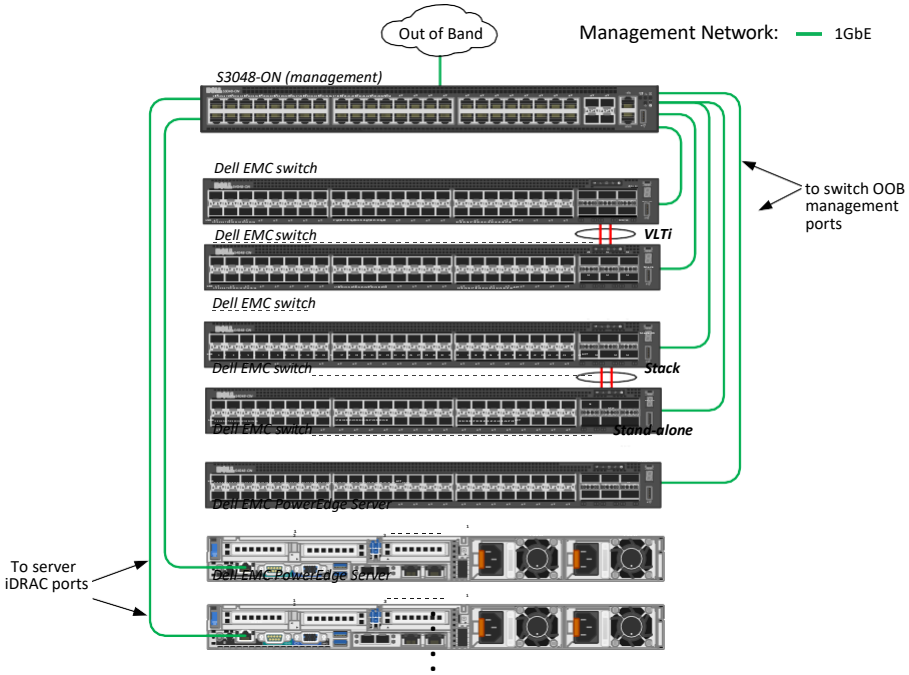

Figure 6 OOB management network for a single rack

3.1.1 Configure management IP addresses

Each switch managed through OOB requires an IP address on its OOB port. The exact command for setting the OOB management port depends on the switch hardware and operating system.

The commands below show how to configure an OOB port in OS10EE. Use the `show interface mgmt` command to find the exact management port assignment for your particular switch. The OOB port for the Dell EMC Networking S4148-ON is **`mgmt 1/1/1.`**

```
OS10#show interface mgmt
Management 1/1/1 is up, line protocol is up…
```

Note: Replace the 192.168.1.10/24 IP address below with an available IP address for your network. Replace the 192.168.0.0/16 IP address and subnet mask to include only IP addresses in your management domain. Substitute the example default gateway (next hop) address of 192.168.1.1 with the one for your network.

```
OS10#configure terminal
OS10(conf)#interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)#no ip address dhcp
OS10(conf-if-ma-1/1/1)#ip address 192.168.1.10/24
OS10(conf-if-ma-1/1/1)#no shutdown
OS10(conf-if-ma-1/1/1)#exit
OS10(config)#management route 192.168.0.0/16 192.168.1.1
```

Note: Dell EMC recommends that you assign static IP addresses to managed switches and on management stations such as OpenManage Network Manager (OMNM).

Cable the OOB port to connect to the management network. Use the `ping` command from a remote switch or management station to test connectivity to the switch. To quickly verify management access, SSH or telnet into the switch from a remote device. SSH is enabled by default on OS10EE. Telnet is disabled by default.

To use telnet, it must first be enabled using the `ip telnet server enable` command from a global configuration prompt.

3.2 In-band management configuration

Similar to OOB, in-band may be used for administrative management (SSH, Telnet, TFTP, etc.) as well as SNMP management, monitoring, and system logging. In-band management can also take advantage of security provided by ACLs. One or more ports on a switch may be enabled for in-band management. A minimum of one port is necessary for the switch itself to be managed through the in-band network. Optionally, additional ports on the switch may also be configured to attach other devices to be managed. For configuring a single port, setting up the in-band management is as simple as providing an IP address to a port on the switch. The IP address should be in a dedicated management subnet. The example below enables port 1/1/12 for in-band management.

```
OS10(config)# interface ethernet 1/1/12
OS10(conf-if-eth1/1/12)# no switchport
OS10(conf-if-eth1/1/12)# ip address 10.1.1.1/24
```

Use the `ping` command from a remote switch or management station to test connectivity to the switch's in-band management port. To quickly verify management access, SSH or telnet into the switch from a remote device. SSH is enabled by default on OS10EE. Telnet is disabled by default. To use telnet it must first be enabled using the `ip telnet server enable` command from a global configuration prompt.

In-band management may also be configured using a VLAN dedicated for management. An IP address is assigned to the VLAN on each switch in order to access the switch. The management VLAN cannot be the default VLAN (i.e. VLAN 1) since an IP address cannot be assigned to it.

```
OS10(config)# interface vlan 11
OS10(conf-if-vl-11)# description management
OS10(conf-if-vl-11)# ip address 10.1.1.1/24
```

Add one or more ports to the VLAN that will participate in in-band management. A minimum of one port is necessary for the switch itself to be managed through the in-band network. Additional ports can be used to attach and manage downstream devices.

```
OS10(conf)# interface range eth 1/1/3-1/1/4
OS10(conf-range-eth1/1/1-1/1/2# switchport access vlan 11
OS10(conf-range-eth1/1/1-1/1/2)# no shutdown
OS10(conf-range-eth1/1/1-1/1/2)# exit
```

If two ports are added to the management VLAN, cable either port to connect to the management VLAN upstream (toward the management station), or directly into the management station. If only one port is configured, cable that port to the management VLAN upstream. Figure 7 shows how the administrator may use SSH or Telnet to access either switch in the figure.

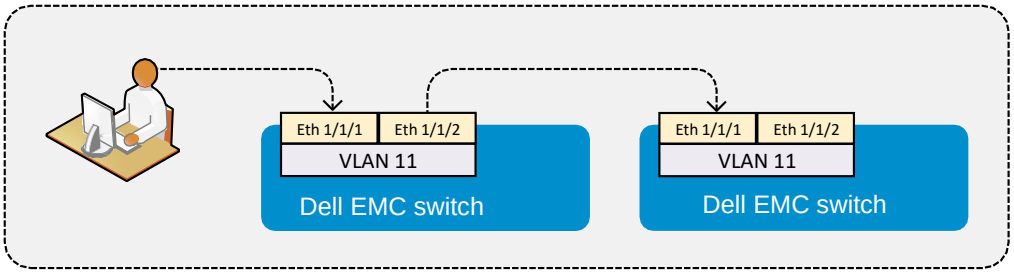

Figure 7 Using a VLAN for In-band management

Use the `ping` command from a remote switch or management station to test connectivity to the switch. You may ping the switch from a remote switch or management station. To verify in-band access, SSH or telnet into the switch from a remote device. SSH is enabled by default on OS10EE. Telnet is disabled by default. To use telnet it must first be enabled using the `ip telnet server enable` command from a global configuration prompt.

If desired, attach another port on the management VLAN to another device downstream that has been configured to use the same management VLAN.

3.3 Serial port management

Using the serial console port is a third method to managing switches on the network. There are a few benefits to using the switch's serial port. It allows administrators to gain access to the switch on the network while the switch is booting, and allows them to view the boot process. It allows access to switches that have not yet been configured and allows administrators to configure them. It also allows access to the command line for continued configuring, alongside the in-band and OOB management. All CLI commands are available through the serial port session. Limitations are that it requires a serial switch on the network in order to achieve one-to-many management access. The serial port is not an Ethernet port and therefore cannot be configured with an IP address or accept SSH, telnet, or SNMP traffic. It also has very limited network security and monitoring capabilities. Once an administrator uses the serial port to initially configure a switch, the serial port is generally considered only as a secondary backup for management purposes.

Note: Serial ports may be used alongside OOB or in-band management.

4 Security basics

To help ensure the security and integrity of data, it is important to control access to switches on the network. Several tools are available to assist network administrators in this area. RADIUS, TACACS+, local authentication, and VTY ACLs are used to authenticate users and control various levels of access to devices.

When accessing the CLI over the in-band or OOB management interfaces, it is a security best practice to use SSH and to leave Telnet disabled. Information (including passwords) is encrypted when sent over SSH, and in plain text when sent over telnet. SSH therefore provides greater data security and integrity over unsecured networks.

4.1 VTY ACLs

Accessing a command line interface (CLI) using telnet or SSH is known as a virtual terminal line (VTY) session. A VTY ACL is used to control what Telnet and SSH users are able to access on the switch. The following steps provide you with control of the Telnet or SSH connections to the switch by applying ACLs on VTY lines:

1. Create IP or IPv6 access lists with permit or deny filters.
2. Enter the VTY mode by using the `line vty` command.
3. Apply the access lists to the VTY line with the `access-class` command.

For example, an ACL may be created and named `deny50`, then assigned to the VTY to disallow the IP address 10.1.1.5 any IP traffic into the switch. Since ACLs have an implicit *deny* statement as the last rule, it is important to also add a *permit* statement to allow all other IP traffic.

```
OS10(config)# ip access-list deny50
OS10(config-ipv4-acl)# deny ip 10.1.1.5 255.255.255.255 any
OS10(config-ipv4-acl)# permit ip 10.1.1.0 255.255.255.0 any
OS10(config-ipv4-acl)# exit
```

Enter the VTY mode by using the `line vty` command while in configuration mode.

```
OS10(config)# line vty
OS10(config-line-vty)# ip access-class deny50
```

View the VTY ACL configuration from within the `line vty` configuration mode.

```
OS10(config-line-vty)# show configuration
!
line vty
 ip access-class deny50
```

To verify the VTY ACL works, SSH or Telnet into the switch using the 10.1.1.5 IP address. The connection will fail. Changing the IP address to 10.1.1.6 or other address on the subnet will regain connectivity. Use other supported ACLs in the OS10EE User Guide to customize the security on your network.

4.2 RADIUS, TACACS+, and local authentication

Accounting, Authentication, and Authorization (AAA) services secure networks against unauthorized access. In addition to local authentication, OS10EE supports Remote Authentication Dial-In Service (RADIUS) and

Terminal Access Controller Access Control System+ (TACACS+) client/server authentication systems. For RADIUS and TACACS+, an OS10EE switch acts as a client and sends authentication requests to a server that contains all user authentication and network service access information.

A RADIUS or TACACS+ server provides accounting, authentication (user credentials verification), and authorization (user privilege-level) services. You can configure the security protocol used for different login methods and users. The server uses a list of authentication methods to define the types of authentication and the sequence in which they apply.

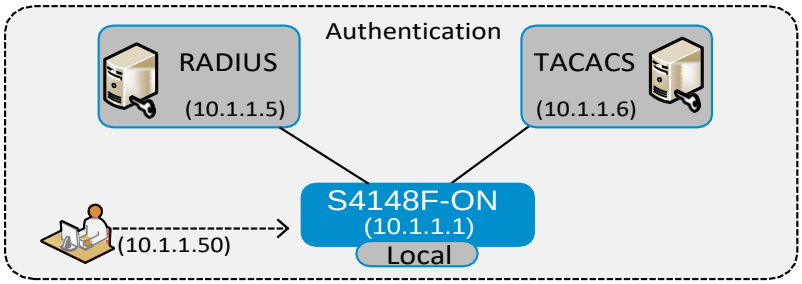

Figure 8 RADIUS, TACACS+, and local authentication methods

4.2.1 Configure authentication methods

The basic rules for user authentication on a Dell EMC network are as follows:

- By default, only Local authentication method is used.
- Local authentication uses the username and password database defined in the local configuration.
- Radius authentication is optional and uses the RADIUS servers configured with the `radius-server host` command as the primary authentication method.
- TACACS+ authentication is optional and uses the TACACS+ servers configured with the `tacacs-server host` command as the primary authentication method.
- The authentication methods in the method list are executed in the order in which they are configured.
- Re-enter the methods as needed to change the order.
- Local authentication must always be in the `aaa authentication` list.
- When a console user logs in with RADIUS or TACACS+ authentication, the privilege-level configured for the user on the RADIUS or TACACS+ server is applied.

Note: You must configure the group name (level) on the RADIUS server using the vendor-specific attribute or the authentication fails.

The *OS10 Enterprise Edition User Guide Release 10.4.0E (R3)* provides good explanations and examples for setting up Radius, TACACS+, and local authentication. The examples below provides steps for setting up RADIUS or TACACS+.

4.2.1.1 RADIUS example

The `aaa authentication` command is used to set the desired authentication. The optional `aaa re-authenticate` command is entered to instantly log out all users whenever authentication requirements change, forcing them to login again using the updated authentication.

```
OS10(config)# aaa authentication radius local
OS10(config)# aaa re-authenticate enable
```

To configure a RADIUS server for authentication, enter the server's IP address or hostname. Provide the key used to authenticate the OS10EE switch on the server. The UDP port number for the server may also be entered if required. The default UDP port (1812) is used in this example.

```
OS10(config)# radius-server host 10.1.1.5 key secretkey
OS10(config)# radius-server retransmit 10
OS10(config)# radius-server timeout 10
```

Use the `show running-configuration | grep radius` command to view the RADIUS configuration.

```
OS10# show running-configuration | grep radius
aaa authentication radius local
radius-server host 10.1.1.5 key secretkey
radius-server retransmit 10
radius-server timeout 10
```

A RADIUS Server is installed on the network and configured using the steps below. There are a number of RADIUS server options out there to choose from such as Windows Network Policy and Access Services, FreeRADIUS, TekRADIUS, and many others. To validate this example, the Windows Network Policy and Access Services was used.

4.2.1.2 Install the RADIUS server

The following steps are performed from a Windows Server 2012 R2 system,

1. Go to the Add Roles and Features wizard, and add Network Policy and Access Services.
2. Click **Next** until you see the **Select server roles** screen.
3. Place a check in the Network Policy and Access Services box.
4. From the pop up box, check **Add Features** then click **Next**.
5. Click **Next** until you see the **Confirm installation selections** option then click **Install**.
6. Hover the cursor over the progress bar until 100% is displayed.
7. Click **Close**.
8. Launch a **Run** session and enter **nps.msc** in the **Open** field, then click **Open**.
9. The **Network Policy Server** opens. The RADIUS server is ready to be configured.

4.2.1.3 Configure the RADIUS server

The steps below are used to quickly validate the RADIUS feature is working on the switch. A RADIUS client is created and a policy assigned.

1. Expand **RADIUS Clients and Servers** on the left of the screen.
2. Right-click **RADIUS Clients** then select **New**.
3. Enter **testswitch** in the **Friendly Name** field and **10.1.1.1** in the **IP address** field.
4. Enter **secretkey** in both **Shared Secret** fields at the bottom, then click **OK**.
5. Expand the **Policies** section on the left of the screen.
6. Right-click **Network Policies** and select **New**.
7. Enter **denyIP** in the **Policy Name** field then click **Next**.
8. On the **Specify Conditions** page, click **Add**. Notice the various conditions that may be applied, including group memberships, date and time restrictions, and others.
9. Scroll down and select **Access Client IP4 Address** then click **Add**.
10. Enter an IP address to be restricted from logging into the network. For example, enter 10.1.1.50, then click **Next**.
11. On the Specify Access Permission page, select **Access denied**, then click **Next**.
12. From the Configure Authentication Methods page, click Next.

13. Click **Next** on the **Configure Constraints** page, and again on the **Configure Settings** page.

The RADIUS server is now configured to not allow network access to IP address 10.1.1.50.

4.2.1.4 Configure TACACS+

Most commands in OS10EE used for configuring RADIUS are also used for configuring TACACS+. The `aaa authentication` command is used to set the desired authentication. The optional `aaa re-authenticate` command is entered to instantly log out all users whenever authentication requirements change, forcing them to login again using the updated authentication.

```
OS10(config)# aaa authentication tacacs local
OS10(config)# aaa re-authenticate enable
```

To configure a TACACS+ server for authentication, enter the server's IP address or host name. You can change the UDP port number on the server and the key used to authenticate the OS10EE switch on the server.

```
OS10(config)# tacacs-server host 10.1.1.6 key secretkey
OS10(config)# tacacs-server timeout 10
```

Use the `show running-configuration | grep radius` command to view the TACACS+ configuration.

```
OS10# show running-configuration | grep tacacs
aaa authentication tacacs local
tacacs-server host 10.1.1.6 key secretkey
tacacs-server timeout 10
```

Note: See the documentation that came with your TACACS+ server for setting up TACACS+ clients.

4.3 Management VRF

Virtual routing and forwarding (VRF) enables partitioning of a physical router into multiple virtual routers. The control and data plane are isolated in each virtual router (VR) so that traffic does not flow across VRs. VRF allows multiple instances of routing tables to co-exist within the same router at the same time. OS10EE supports a management VRF instance and a default VRF instance.

All front panel ports and logical interfaces are part of the default VRF instance. Management ports may be added to the management VRF instance.

Note: Before assigning a management port to the management VRF instance, remove all configured settings on the management port, including the IP address. Removing the IP address disconnects all existing SSH and Telnet sessions on the switch.

Use the serial console port to perform the steps in the example below. These instructions will remove the IP address, configure the management VRF, and then add the IP address back to the management interface.

```
OS10(config)# interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)# show configuration
!
```

```
interface mgmt1/1/1
 no shutdown
 ip address 10.16.208.125/16
 ipv6 address autoconfig
OS10(conf-if-ma-1/1/1)# no ip address
OS10(conf-if-ma-1/1/1)# no ipv6 address autoconfig
OS10(conf-if-ma-1/1/1)# exit
OS10(config)# ip vrf management
OS10(conf-vrf)# interface management
OS10(conf-vrf)# exit
OS10(config)# interface mgmt1/1/1
OS10(conf-if-ma-1/1/1)# no shutdown
OS10(conf-if-ma-1/1/1)# ip address 10.16.208.125/16
OS10(conf-if-ma-1/1/1)# ipv6 address autoconfig
```

Most services listed in Table 4 may be configured and enabled for the management VRF instance. The table shows the services supported in a management VRF instance versus those supported by the default VRF instance.

Table 4 Management VRF services

Service	Management VRF	Default VRF
DHCP client	✓	✓
DNS client	✓	✓
FTP client	✓	✓
HTTP client	✓	✓
ICMP / Ping	✓	✓
NTP client	✓	✓
NTP server	✓	✓
RADIUS server	✓	✓
SCP client	✓	✓
SFTP	✓	✓
SNMP traps	✓	✓
SSH server	✓	✓
Telnet server	✓	✓
TFTP client	✓	✓
Traceroute	✓	✓
VLT backup link	✓	✓
VRRP	✓	✓
sFlow	✓	
Syslog	✓	
DHCP Relay		✓

DHCP server		✓
OSPFV2/OSPFV3/BPG		✓

Refer to the *System management* section of the *OS10 Enterprise Edition User Guide Release 10.4.0E (R3)*, for information on configuring the services in Table 4, for the management VRF. For troubleshooting the management VRF, including ping, traceroute, and logging server features specific for the management VRF, see the *Troubleshoot OS10* section.

5 Connecting Dell EMC switches

There are multiple means of connecting two or more Dell EMC switches to pass network traffic. The desired connection type depends on what is to be achieved. Examples for popular connection types are covered below along with explanations of when each should be used. One or more physical cables are required between each switch. In the figures, blue boxes represent switches and lines between them represent cables. A circle around multiple lines show that the cables may be joined together to form a single logical connection, as depicted in Figure 9.

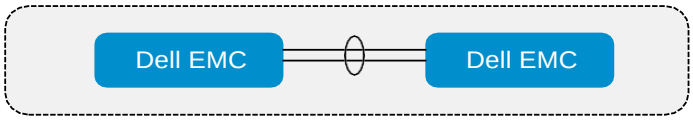

Figure 9 Connecting two Dell EMC Networking switches

All commands below may be entered at the CLI. The management network may be used to attach to each switch via Telnet or SSH, or use the serial cable interface if no management network has been configured. Most examples in this guide start the user in global configuration mode (i.e. `OS10(conf)#` command prompt). To get to this prompt, enter the command `configure terminal` from the `OS10#` prompt.

Data communications between these switches can be achieved using the methods described in this chapter.

5.1 Port Channels

A port channel, also known as a LAG, or link aggregation group, increases bandwidth and provide failover redundancy and load balancing between two switches. Although a port channel can contain a single cable, it is typically created using two or more cables between devices. Use two cables to double bandwidth, three cables to triple bandwidth, or four cables to quadruple bandwidth. Like ports with the same speed are required when combining to form the port channel.

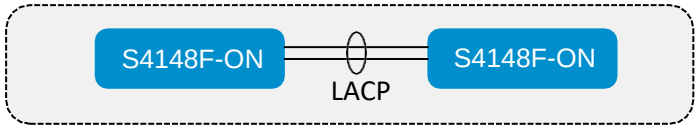

Figure 10 Port channel configured between two OS10EE switches

Two cables used in this example double the bandwidth provided by a single cable. In the commands below, ports 1/1/1 and 1/1/2 from each switch are used to form a port channel. The `port-channel` command is run from the global configuration mode to create the group. The `channel-group` command is then run from the interface configuration mode to assign ports to the group. The preferred `mode active` option is used to create an LACP port channel which allows negotiation with other ports to automate LAG connections. OS10EE supports up to 128 port channels with up to 32 ports (per switch) per channel, though the switch hardware may limit this. In this example, port channel 1 is created and assigned two ports per switch.

Configure a port channel on switch #1	Configure a port channel on switch #2
OS10(conf)#interface port-channel 1 OS10(conf-if-po-1)#exit OS10(conf)#interface range eth 1/1/1-1/1/2 OS10(conf-range-if-eth1/1/1-1/1/2)#channel-group 1 mode active OS10(conf-range-if-eth1/1/1-1/1/2)#exit	OS10(conf)#interface port-channel 1 OS10(conf-if-po-1)#exit OS10(conf)#interface range eth 1/1/1-1/1/2 OS10(conf-range-if-eth1/1/1-1/1/2)#channel-group 1 mode active OS10(conf-range-if-eth1/1/1-1/1/2)#exit

Note: Although the example commands above use the same port range (i.e. 1/1/1-1/1/2), it is not a requirement that the ports be the same across the two switches. It is also not a requirement that they be consecutively numbered ports. For example, switch #2 could use ports 1/1/20 and 1/1/35. For troubleshooting reason however, it is often a best practice to use available ports that are easy to remember.

The `show port-channel summary` command shown below, may be used on each switch to validate the port channel and its member ports are up. The `show lldp neighbors` command may be used on each switch to verify which ports are connected between switches.

```
OS10# show port-channel summary

Flags:  D - Down    I - member up but inactive    P - member up and active
        U - Up (port-channel)
Group Port-Channel          Type      Protocol  Member Ports
1     port-channel1     (U)     Eth       DYNAMIC   1/1/1(P) 1/1/2(P)

OS10# show lldp neighbors
Loc PortID          Rem Host Name      Rem Port Id        Rem Chassis Id
ethernet1/1/1       OS10               ethernet1/1/1      14:18:77:17:f1:b8
ethernet1/1/2       OS10               ethernet1/1/2      14:18:77:17:f1:b8
```

VLAN 1 is the default vlan for all Ethernet ports on the switch, and all interfaces and port channels are assigned to this VLAN by default. Section 5.2 below demonstrates how to create a VLAN and assign interfaces and port channels to the new VLAN.

5.2 VLANs

A virtual LAN (VLAN) is used to partition the switch into two or more logical switches to allow for grouping of end devices into logical groups. Such groups typically consist of devices or users running the same applications. VLANs can also span across several switches to allow ports from these switches to be joined to the same logical network group. Creating one or more VLANs keeps broadcast traffic contained within each logical group of devices.

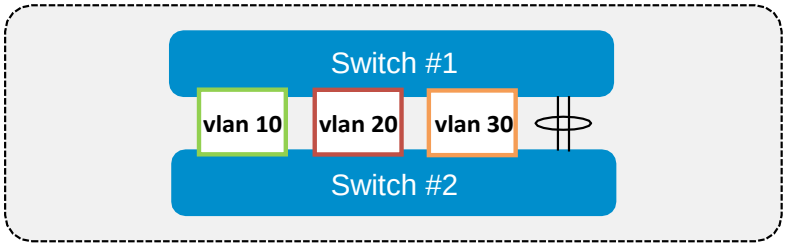

Figure 11 VLANs configured across two S4148F-ON switches

The example below shows the commands to create VLANs 10, 20, and 30, on Switch #1 and Switch #2. The commands are the same on both switches. OS10EE supports VLANS 1 through 4093 (VLAN 4094 is reserved for VLT).

Configure a VLAN on switch #1	Configure a VLAN on switch #2
`OS10(conf)#interface range vlan 10,20,30` `OS10(conf-range-vl-10,20,30)#exit`	`OS10(conf)#interface range vlan 10,20,30` `OS10(conf-range-vl-10,20,30)#exit`

Once a VLAN is created, ports may be assigned to it. End devices connected to these ports can communicate with each other over this common VLAN.

Note: Inter-VLAN routing must be implemented to allow for two or more VLANs to communicate. See the *OS10 Enterprise Edition User Guide Release 10.4.0E (R3)* for more information.

The commands below show how to add ports 1/1/1 through 1/1/8 to VLAN 10 on switch #1, and ports 1/1/1 through 1/1/4 to VLAN 10 on switch #2. A different set of ports is used on each switch to demonstrate they do not need to be the same. A different number of ports are used on each switch to demonstrate that there is no one-to-one correlation (like in a port channel). In this example, one switch has four ports on VLAN 10, while the other switch has eight.

Add interfaces to the VLAN on switch #1	Add interfaces to the VLAN on switch #2

`OS10(conf)#interface range eth 1/1/1-1/1/8`
`OS10(conf-range-eth1/1/1-1/1/8#switchport access vlan 10`
`OS10(conf-range-eth1/1/1-1/1/8)#no shutdown`
`OS10(conf-range-eth1/1/1-1/1/8)#exit`
	`OS10(conf)#interface range eth 1/1/1-1/1/4`
	`OS10(conf-range-eth1/1/1-1/1/4)#switchport access vlan 10`
	`OS10(conf-range-eth1/1/1-1/1/4)#no shutdown`
	`OS10(conf-range-eth1/1/1-1/1/4)#exit`

To allow devices on a VLAN on one switch to communicate with devices on the same VLAN on another switch, a trunk port has to be created between the two switches. Trunk ports are used to pass VLAN traffic from one switch to the next, and across the entire network. For example, traffic from end devices on VLAN 10 on one switch can be passed across a port or port channel interface in trunk mode to communicate with end devices on VLAN 10 on another switch.

An interface in trunk mode forwards all VLAN traffic by default. For more control over where traffic goes on the network, an administrator can restrict a trunk port to only pass traffic of certain VLANs. Use the following commands to create a port channel trunk to only pass VLANs 10 and 20 traffic between the switches.

Create port channel trunk to forward VLAN traffic	Create port channel trunk to forward VLAN traffic
OS10(config)# interface port-channel 1 OS10(conf-if-po-1)# switchport mode trunk OS10(conf-if-po-1)# switchport trunk allowed vlan 10,20 OS10(conf-if-po-1)# interface range ethernet 1/1/15-1/1/16 OS10(conf-range-eth1/1/15-1/1/16)# channel-group 1 mode active OS10(conf-range-eth1/1/15-1/1/16)# exit	OS10(config)# interface port-channel 1 OS10(conf-if-po-1)# switchport mode trunk OS10(conf-if-po-1)# switchport trunk allowed vlan 10,20 OS10(conf-if-po-1)# interface range ethernet 1/1/15-1/1/16 OS10(conf-range-eth1/1/15-1/1/16)# channel-group 1 mode active OS10(conf-range-eth1/1/15-1/1/16)# exit

Use the `show vlan` command on each switch to confirm the port channel trunk and the access ports assigned to each VLAN. Run the `show port-channel summary` to show the member ports of each port channel and the port channel status.

```
OS10# show vlan 10
Codes: * - Default VLAN, M - Management VLAN, R - Remote Port Mirroring VLANs
Q: A - Access (Untagged), T - Tagged
    NUM    Status    Description              Q Ports
    10     up                                 T Po1
                                              A Eth1/1/21-1/1/24
OS10# show port-channel summary
Flags:  D - Down  I - member up but inactive  P - member up and active
        U - Up (port-channel)
Group Port-Channel          Type     Protocol  Member Ports
--------------------------------------------------------------------------
1     port-channel1     (U)     Eth      DYNAMIC   1/1/15(P) 1/1/16(P)
```

5.2.1 Changing the native VLAN

The default VLAN 1 is the native VLAN for OS10EE. Use the commands below to change the native VLAN to a different VLAN. This example creates VLANs 10, 20, and 30, and a trunk port (eth 1/1/40), then makes VLAN 30 the native VLAN.

```
OS10# configure terminal
OS10(config)# interface vlan 10
OS10(conf-if-vl-10)# interface vlan 20
OS10(conf-if-vl-20)# interface vlan 30
OS10(conf-if-vl-30)# interface eth 1/1/40
OS10(conf-if-eth1/1/40)# switchport mode trunk
OS10(conf-if-eth1/1/40)# switchport trunk allowed vlan 10,20
OS10(conf-if-eth1/1/40)# switchport access vlan 30
```

VLAN 30 is now the untagged native VLAN. VLANs 10 and 20 remain tagged.

5.3 Spanning Tree

The Spanning Tree Protocol (STP) in Ethernet networks is used to build a loop-free logical topology to prevent bridge loops which result in broadcast storms. Virtually all topologies should implement spanning tree. When a loop is detected, spanning tree automatically shuts down an interface or port channel, as shown in

Figure 12. There are multiple spanning tree protocols supported in OS10EE including Rapid Spanning Tree Protocol (RSTP), Rapid Per-VLAN Spanning Tree+ (RPVST+), and Multiple Spanning Tree (MST). Each of these protocols are covered in detail in the *OS10 Enterprise Edition User Guide Release 10.4.0E (R3)*.

Configuring the commonly used RPVST+ protocol is demonstrated in the example below. RPVST+ is enabled by default in OS10EE. Port-channels or physical interfaces must be a member of a VLAN to participate in RPVST+. A spanning tree instance is created for a VLAN upon adding the first member port to the VLAN.

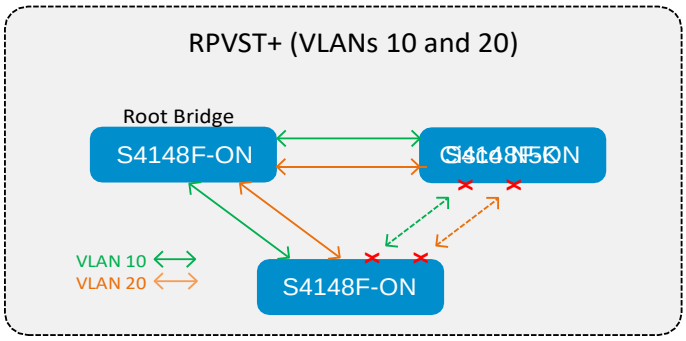

Figure 12 RPVST+ blocking interfaces on multiple VLANs and switches

There are several global and port level configuration commands for spanning tree. Global commands are used to enable/disable spanning tree on the entire switch, whereas port level commands are used to limit or supplement spanning tree features on individual ports.

From global configuration mode, the example commands below set the spanning tree mode on each switch to RPVST+ (default), then sets the priorities for each VLAN on each switch. This “bridge priority” helps determine which switch on the network is more likely to become the root bridge for a VLAN when loops are detected on that particular VLAN. There are 16 bridge priorities ranging from 0 to 61440, in increments of 4096. Lower priority numbers are more likely to become the root bridge. Switches that you do not care about becoming the root can usually be left at the default priority of 32768, or raised as high as the highest setting of 61440.

Configure RPVST+ on desired root bridges	Configure RPVST+ on other switch VLANs

`OS10(conf)#spanning-tree mode rapid-pvst`
`OS10(conf)#spanning-tree vlan 10 priority 0`
`OS10(conf)#spanning-tree vlan 20 priority 0`
	`OS10(conf)#spanning-tree mode rapid-pvst`
	`OS10(conf)#spanning-tree vlan 10 priority 32768`
	`OS10(conf)#spanning-tree vlan 20 priority 32768`

The `show spanning-tree active` and `show spanning-tree brief` commands are used to see the spanning tree configuration and status, including which ports are currently blocking and which ports are forwarding for each VLAN on the switch.

Notice that one of the trunks in Figure 12 is not being used to pass traffic for either VLAN since a single switch on the network was assigned the root bridge role. For RPVST+ demonstration purposes, now give VLAN 10 the lower priority on one switch, and VLAN 20 the lower priority on another switch. Two root bridges are now created, one for each VLAN, as shown in Figure 13. While designing or modifying a network, the topologies need to be carefully designed, with all possible root bridge assignments considered and properly configured.

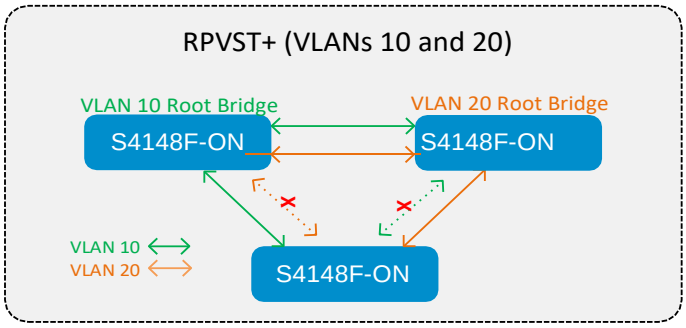

Figure 13 RPVST+ with multiple root bridges

The `show spanning-tree active` and `show spanning-tree brief` commands are used to see the spanning tree configuration and status, including which ports are currently blocking and which ports are forwarding for each VLAN on the switch.

5.3.1 STP edge ports

A port level command often used with spanning tree is the `edge` command. While in interface configuration mode, the `edge` command allows the devices that are plugged in to not participate in spanning tree blocking and learning states, and thereby allows these ports to go immediately into a forwarding state. Configure `edge` only on links connecting to end devices such as servers. `Edge` can cause loops when enabled on interfaces connecting to other network devices. The example commands below apply `edge` to port interface 9 on an OS10EE switch.

Configure a port interface as an edge port

```
OS10(conf)#interface eth 1/1/9
OS10(conf-if-eth1/1/9)#spanning-tree port type edge
OS10(conf-if-eth1/1/9)#exit
```

5.4 VLT

Virtual Link Trunking (VLT) may be used for connecting top-of-rack (ToR) switches or leaf switches in a leaf-spine topology. It offers end devices (such as servers) a redundant, load-balancing connection to the core-network in a loop-free environment. The VLT Interconnect (VLTi) is the physical link (cables and ports) used to form the VLT domain between the pair of switches.

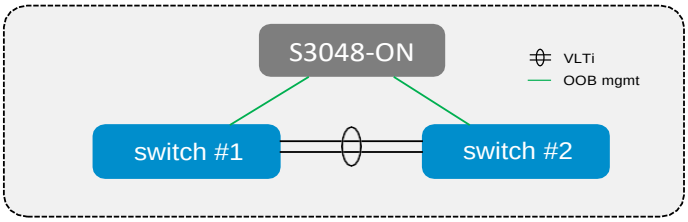

Figure 14 VLT configured on a pair of S4148F-ON switches running OS10EE

The commands below setup a VLTi using ports 25 and 26 on each switch. For backup destination, use the IP address of the management interface of the VLT peer switch.

Configure VLTi on switch #1

```
OS10(conf)#interface mgmt1/1/1
OS10(conf-if-ma-1/1/1)#no shutdown
OS10(conf-if-ma-1/1/1)#ip address
100.67.183.129/24
OS10(conf-if-ma-1/1/1)#exit
OS10(conf)#interface range eth 1/1/25-1/1/26
OS10(conf-range-eth1/1/25-1/1/26)#no
switchport
OS10(conf-range-eth1/1/25-1/1/26)#exit
OS10(conf)#vlt-domain 1
OS10(conf-vlt-1)#backup destination
100.67.183.130
OS10(conf-vlt-1)#discovery-interface ethernet
1/1/25-1/1/26
OS10(conf-vlt-1)#exit
```

Note: Use the `show vlt 1` command to verify VLTi link is up. Use `show vlt 1 backup-link` to verify Peer Heartbeat is up.

Configure VLTi on switch #2

```
OS10(conf)#interface mgmt1/1/1
OS10(conf-if-ma-1/1/1)#no shutdown
OS10(conf-if-ma-1/1/1)#ip address
100.67.183.130/24
OS10(conf-if-ma-1/1/1)#exit
OS10(conf)#interface range eth 1/1/25-1/1/26
OS10(conf-range-eth1/1/25-1/1/26)#no
switchport
OS10(conf-range-eth1/1/25-1/1/26)#exit
OS10(conf)#vlt-domain 1
OS10(conf-vlt-1)#backup destination
100.67.183.129
OS10(conf-vlt-1)#discovery-interface ethernet
1/1/25-1/1/26
OS10(conf-vlt-1)#exit
```

Note: Use the `show vlt 1` command to verify VLTi link is up. Use `show vlt 1 backup-link` to verify Peer Heartbeat is up.

To take advantage of VLT, a minimum of one port from each switch must be paired into a VLT port channel for each device being attached, so they can connect to both switches. Figure 15 shows two such devices.

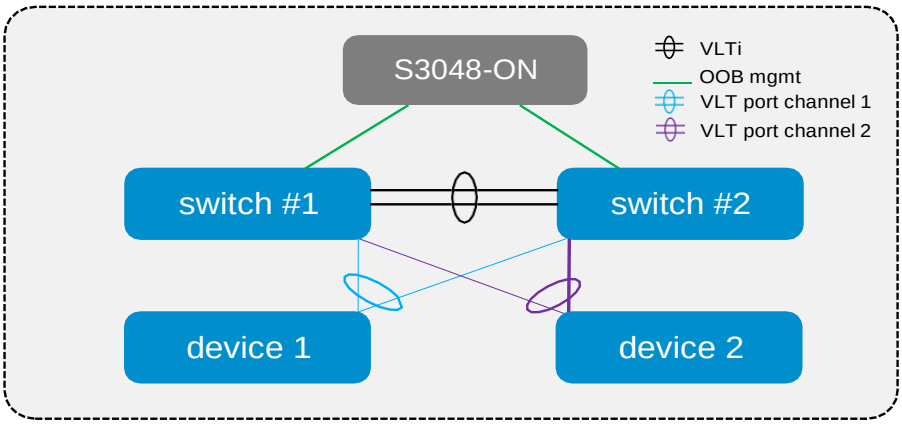

Figure 15 Connecting devices to the VLT domain

The commands below allow for the two devices to be attached, each connecting to its own VLT port channel. Additional VLT port channels would allow for attaching more devices.

Configure ports to attach end devices (switch #1)	Configure ports to attach end-device (switch #2)
OS10(conf)#interface range eth 1/1/1-1/1/2 OS10(conf-range-eth1/1/1-1/1/2)#switchport access vlan 10 OS10(conf-range-eth1/1/1-1/1/2)#no shutdown OS10(conf-range-eth1/1/1-1/1/2)#exit OS10(conf)#interface port-channel 1 OS10(conf-if-po-1)#description "Device 1" OS10(conf-if-po-1)#switchport access vlan 10 OS10(conf-if-po-1)#vlt-port-channel 1 OS10(conf-if-po-1)#spanning-tree port type edge OS10(conf-if-po-1)#interface port-channel 2 OS10(conf-if-po-2)#description "Device 2" OS10(conf-if-po-2)#switchport access vlan 10 OS10(conf-if-po-2)#vlt-port-channel 2 OS10(conf-if-po-2)#spanning-tree port type edge	OS10(conf)#interface range eth 1/1/1-1/1/2 OS10(conf-range-eth1/1/1-1/1/2)#switchport access vlan 10 OS10(conf-range-eth1/1/1-1/1/2)#no shutdown OS10(conf-range-eth1/1/1-1/1/2)#exit OS10(conf)#interface port-channel 1 OS10(conf-if-po-1)#description "Device 1" OS10(conf-if-po-1)#switchport access vlan 10 OS10(conf-if-po-1)#vlt-port-channel 1 OS10(conf-if-po-1)#spanning-tree port type edge OS10(conf-if-po-1)#interface port-channel 2 OS10(conf-if-po-2)#description "Device 2" OS10(conf-if-po-2)#switchport access vlan 10 OS10(conf-if-po-2)#vlt-port-channel 2 OS10(conf-if-po-2)#spanning-tree port type edge

6 Connect Dell EMC to third party switches

Dell EMC switches can connect to most other Ethernet switches in the industry, and are commonly connected to the Cisco Nexus switch. Examples of the most popular protocols used between the switches are covered below along with explanations of when each should be used. One or more physical cables are required between each switch. In the figures, the rectangular boxes represent switches and lines between them represent cables. A circle around multiple lines show that one or more cables may be joined together to form a single LAG, as shown in Figure 16.

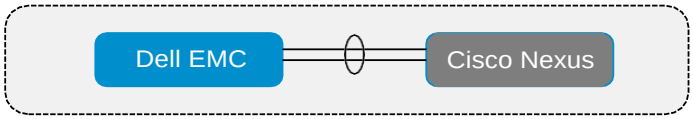

Figure 16 Dell EMC switch connecting to a Cisco Nexus switch

Commands in the sections that follow are entered at the CLI of each switch. The management network may be used to attach to each switch via Telnet or SSH, or use the serial cable interface if no management network has been configured. Most examples in this guide start the user at the `OS10(conf)#` prompt for Dell EMC switches and at the `switch(config)#` prompt for Cisco Nexus switches. To get to these prompts, enter the command `configure terminal` from the global command prompt.

Data communications between these switches can be achieved using the methods described in this chapter.

6.1 Port channels

A port channel, also known as a LAG, or link aggregation, increases bandwidth and provides failover redundancy between two switches. The port channel is created using two or more cables between the devices. Use two cables to double bandwidth, three cables to triple bandwidth, or four cables to quadruple bandwidth. Like ports with the same speed are a best practice when combining to form the port channel.

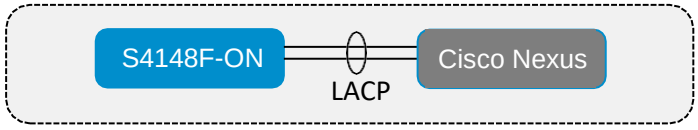

Figure 17 Port channel configured between an OS10EE switch and an OEM switch

Two cables are used in this example which doubles the bandwidth supplied by a single cable. In the commands below, ports 1/1/15 and 1/1/16 from the Dell EMC switch and ports 1/17 and 1/18 from a Cisco Nexus are used to form a port channel. The `interface port-channel` command is run from the global configuration mode to create the group. The `channel-group` command is then run from the interface configuration mode to assign ports to the group. The preferred `mode active` option is used to create an LACP port channel which allows negotiations with other ports to automate LAG connections. OS10EE supports up to 128 port channels with up to 32 ports (per switch) per channel. In this example, port channel 1 is created and assigned two ports per switch.

Configure a port channel on the Dell EMC Switch

```
OS10(conf)#interface port-channel 1
OS10(conf-if-po-1)# switchport mode trunk
OS10(conf-if-po-1)#exit
OS10(conf)#interface range eth 1/1/15-1/1/16
OS10(conf-range-if-eth1/1/15-1/1/16)#channel-group
1 mode active
OS10(conf- range-if-eth1/1/15-1/1/16)#exit
```

Configure a port channel on the Cisco Nexus

```
switch(config)#feature lacp
switch(config)#interface port-channel 1
switch(config-if)#switchport
switch(config-if)#switchport mode trunk
switch(config-if)#interface ethernet 1/17-18
switch(config-if-range)#channel-group 1 mode active
switch(config-if-range)#exit
```

Note: The port ranges are different for each switch in the example above to show that it is not a requirement that the ports be the same across the two switches. It is also not a requirement that they be consecutively numbered ports. It is often preferred to use the same ports and consecutive ports just to make them easier to remember.

The `show port-channel summary` command may be used on each switch to validate the port channel and its member ports are up. The `show lldp neighbors` command may be used on each switch to verify which ports are connected between switches.

Validate port channels for each switch

```
OS10# show port-channel summary

Flags:  D - Down    I - member up but inactive    P - member up and active
        U - Up (port-channel)
Group Port-Channel          Type     Protocol  Member Ports
1    port-channel1    (U)    Eth      DYNAMIC   1/1/15(P) 1/1/16(P)

switch# show port-channel summary
Flags:  D - Down         P - Up in port-channel (members)
        I - Individual   H - Hot-standby (LACP only)
        s - Suspended    r - Module-removed
        S - Switched     R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
Group Port-       Type     Protocol  Member Ports
      Channel
1     Po1(SU)     Eth      LACP      Eth1/17(P)    Eth1/18(P)
```

Verify port connections between switches

```
OS10# show lldp neighbors
Loc PortID          Rem Host Name        Rem Port Id                    Rem Chassis Id
ethernet1/1/15      switch               Eth1/17                        00:2a:6a:f7:80:58
ethernet1/1/16      switch               Eth1/18                        00:2a:6a:f7:80:59

switch# show lldp neighbors
Capability codes:
  I Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf      Hold-time  Capability  Port ID
OS10                Eth1/17         120        PBR         ethernet1/1/15
OS10                Eth1/18         120        PBR         ethernet1/1/16
Total entries displayed: 2
```

VLAN 1 is the default vlan for all Ethernet ports on the switch, and all ports are assigned to this VLAN by default. Other VLANs must be created by the administrator, who can then assign ports to the new VLANs.

Section 6.2 below demonstrates how to create a VLAN and assign interfaces and port channels to the new VLAN.

6.2 VLANs

A virtual LAN (VLAN) is used to partition the switch into two or more logical switches to allow for grouping of end devices into logical groups. Such groups typically consist of devices or users running the same applications. VLANs can also span across several switches to allow ports from these switches to be joined to the same logical network group. Creating one or more VLANs keeps broadcast traffic contained within each logical group of devices.

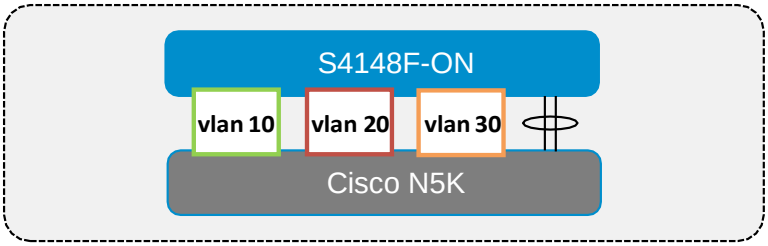

Figure 18 VLANs configured across an OS10EE switch and a Cisco Nexus

The commands below create VLANs 10, 20, and 30 on both switches. OS10EE supports VLANS 1 through 4093 (VLAN 4094 is reserved for VLT). VLANs supported on other switches and operating systems may vary.

Configure VLANs on the Dell EMC Switch	Configure VLANs on the Cisco Nexus
`OS10(conf)#interface range vlan 10,20,30` `OS10(conf-range-vl-10,20,30)#exit`	`switch(config)#vlan configuration 10,20,30` `switch(config-vlan-config)#exit`

Once a VLAN is created, ports may be assigned to it. End devices connected to these ports can communicate with each other over this common VLAN.

Note: Inter-VLAN routing must be implemented to allow for two or more VLANs to communicate. See the *OS10 Enterprise Edition User Guide Release 10.4.0E (R3)* and the User Guide for the third party switch, for more information on configuring inter-VLAN routing.

Use the following commands to add ports 21 through 24 on each switch to VLAN 10. Use the same command structure to add other ports to other VLANs as needed.

Assign access ports to a VLAN on the Dell EMC switch	Assign access ports to the VLAN on the Cisco Nexus switch

`OS10(config)# interface range ethernet 1/1/21-1/1/24`
`OS10(conf-range-eth1/1/21-1/1/24)# switchport access vlan 10`
`OS10(conf-range-eth1/1/21-1/1/24)# exit`
	`switch(config)# interface ethernet 1/21-24`
	`switch(config-if-range)# switchport`
	`switch(config-if-range)# switchport access vlan 10`
	`switch(config-if-range)# exit`

To allow devices on a VLAN on one switch to communicate with devices on the same VLAN on another switch, a trunk port, like the one created in section 6.1 above, has to be created between the two switches. The trunk port passes VLAN traffic from one switch to the next, and across the entire network. For example, traffic from end devices on VLAN 10 on one switch can be passed across a port channel trunk to communicate with devices on VLAN 10 on another switch.

For more control over where traffic goes on the network, a trunk may be restricted to only pass traffic of certain VLANs. Use the following commands to create a port channel trunk to only pass VLAN 10 and 20 traffic between two switches.

Exchange VLAN traffic with neighbor switch	Exchange VLAN traffic with neighbor switch
OS10(config)# interface port-channel 1 OS10(conf-if-po-1)# switchport mode trunk OS10(conf-if-po-1)# switchport trunk allowed vlan 10,20 OS10(conf-if-po-1)# interface range ethernet 1/1/15-1/1/16 OS10(conf-range-eth1/1/15-1/1/16)# channel-group 1 mode active OS10(conf-range-eth1/1/15-1/1/16)# exit	switch(config)#feature lacp switch(config)#interface port-channel 1 switch(config-if)#switchport switch(config-if)#switchport mode trunk switch(config-if)#switchport trunk allowed vlan 10,20 switch(config-if)#interface ethernet 1/17-18 switch(config-if-range)#channel-group 1 mode active switch(config-if-range)#exit

The `show vlan` command may be used on each switch to confirm the trunked port channel and the access ports assigned to each VLAN. The `show port-channel summary` command may be ran to show the member ports of each port channel and the port channel status.

From the Dell EMC switch

```
OS10# show vlan 10

Codes: * - Default VLAN, M - Management VLAN, R - Remote Port Mirroring VLANs
Q: A - Access (Untagged), T - Tagged
    NUM    Status    Description                    Q Ports
    10     up                                       T Po1
                                                    A Eth1/1/21-1/1/24


OS10# show port-channel summary

Flags:  D - Down    I - member up but inactive    P - member up and active
        U - Up (port-channel)
Group Port-Channel          Type     Protocol  Member Ports
-------------------------------------------------------------------------
1     port-channel1    (U)    Eth      DYNAMIC   1/1/15(P) 1/1/16(P)
```

From the Cisco Nexus switch

```
switch# show vlan id 10

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
10   VLAN0010                          active    Po1, Eth1/17, Eth1/18, Eth1/21
                                                 Eth1/22, Eth1/23, Eth1/24
```

```
switch# show port-channel summary
Flags:  D - Down         P - Up in port-channel (members)
        I - Individual   H - Hot-standby (LACP only)
        s - Suspended    r - Module-removed
        S - Switched     R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------
1     Po1(SU)     Eth      LACP      Eth1/17(P)    Eth1/18(P)
```

6.2.1 Changing the native VLAN

The default VLAN 1 is the native VLAN for OS10EE. The commands below demonstrate how to change the native VLAN to a different VLAN. This example creates VLANs 10, 20, and 30, and a trunk port (eth 1/1/40), then makes VLAN 30 the native VLAN.

```
OS10# configure terminal
OS10(config)# interface vlan 10
OS10(conf-if-vl-10)# interface vlan 20
OS10(conf-if-vl-20)# interface vlan 30
OS10(conf-if-vl-30)# interface eth 1/1/40
OS10(conf-if-eth1/1/40)# switchport mode trunk
OS10(conf-if-eth1/1/40)# switchport trunk allowed vlan 10,20
OS10(conf-if-eth1/1/40)# switchport access vlan 30
```

VLAN 30 is now the untagged native VLAN. VLANs 10 and 20 remain tagged.

6.3 Spanning tree protocol

Spanning Tree Protocol (STP) in Ethernet networks is used to build a loop-free logical topology to prevent bridge loops which result in broadcast storms. When a loop is detected, STP automatically shuts down an interface or port channel, as shown in Figure 19. Virtually all topologies should implement spanning tree as a precaution. There are multiple spanning tree protocols supported in OS10EE including Rapid Spanning Tree Protocol (RSTP), Rapid Per-VLAN Spanning Tree+ (RPVST+), and Multiple Spanning Tree (MST). These protocols are covered in detail in the *OS10 Enterprise Edition User Guide Release 10.4.0E (R3)*.

Configuring the RPVST+ protocol is demonstrated in the example below. The commonly used RPVST+ is enabled by default in OS10EE, and is also supported on the Cisco Nexus 5000. Port-channels or physical interfaces must be a member of a VLAN to participate in RPVST+. A spanning tree instance is created for a VLAN upon adding the first member port to the VLAN.

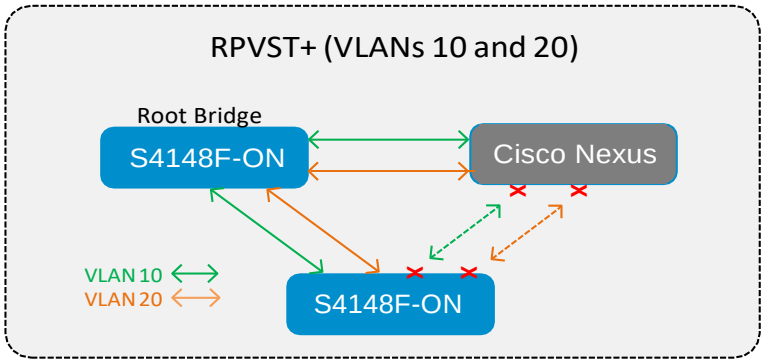

Figure 19 RPVST+ blocking interfaces on multiple VLANs between Dell and OEM switches

There are several global and port level configuration commands for spanning tree. Global commands are used to enable/disable spanning tree on the entire switch, whereas port level commands are used to limit or supplement spanning tree features on individual ports.

From global configuration mode, the example commands below set the spanning tree mode on each switch to RPVST+ (default), then sets the priorities for each VLAN on each switch. This “bridge priority” helps determine which switch on the network is more likely to become the root bridge for a VLAN when loops are detected on that particular VLAN. There are 16 bridge priorities ranging from 0 to 61440, in increments of 4096. Lower priority numbers are more likely to become the root bridge. Switches that you do not care about becoming root can usually be left at the default priority of 32768, or raised as high as the highest setting of 61440.

Configure RPVST+ and set the priority for the desired root bridges for each VLAN	Configure RPVST+ and set the priority for the desired non-root bridges for each VLAN

On the first Dell EMC switch (desired root bridge)
`OS10(conf)#spanning-tree mode rapid-pvst`
`OS10(conf)#spanning-tree vlan 10 priority 4096`
`OS10(conf)#spanning-tree vlan 20 priority 4096`
	On the second Dell EMC switch
	`OS10(conf)#spanning-tree mode rapid-pvst`
	`OS10(conf)#spanning-tree vlan 10 priority 20480`
	`OS10(conf)#spanning-tree vlan 20 priority 20480`
	
	On the Cisco Nexus switch
	`switch(conf)#spanning-tree mode rapid-pvst`
	`switch(conf)#spanning-tree vlan 10 priority 20480`
	`switch(conf)#spanning-tree vlan 20 priority 20480`

Notice that one of the trunks in Figure 19 above is not being used to pass traffic for either VLAN since a single switch on the network was assigned the root bridge role. For RPVST+ demonstration purposes, now give VLAN 10 the lower priority on one switch, and VLAN 20 the lower priority on another switch. Two root bridges are now created, one for each VLAN, as shown in Figure 20. While designing or modifying a network, the topologies need to be carefully designed, with all possible root bridge assignments considered and properly configured.

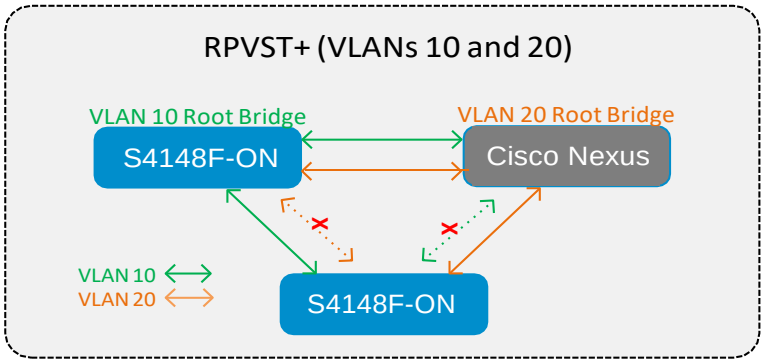

Figure 20 RPVST+ using all port channel trunks

The `show spanning-tree active` and `show spanning-tree brief` commands are used to see the spanning tree configuration and status, including which ports are currently blocking and which ports are forwarding for each VLAN on the switch.

6.3.1 STP edge ports

A port level command often used with spanning tree is the `spanning-tree port type edge` command. While in interface configuration mode, apply this command to allow devices that are plugged in to not participate in spanning tree blocking and learning states, and thereby allows these ports to immediately enter into the forwarding state. Configure edge ports only on links connecting to end (or "edge") devices on the network, such as a server. `Edge` can cause loops when enabled on interfaces connecting to other network devices. The example commands below apply `edge` to port interface 9 on an OS10EE switch, and again on a Cisco Nexus switch.

Configure port interfaces as edge ports

On the Dell EMC switch

```
OS10(conf)#interface eth 1/1/9
OS10(conf-if-eth1/1/9)#spanning-tree port type edge
OS10(conf-if-eth1/1/9)#exit
```

On the Cisco Nexus switch

```
switch(conf)#interface ethernet 1/9
switch(conf-if)#spanning-tree port type edge
switch(conf-if)#exit
```

A Technical support and resources

Dell Support is focused on meeting your needs with proven services and support.

Dell TechCenter is an online technical community where IT professionals have access to numerous resources for Dell EMC software, hardware, and services.

Other referenced or recommended Dell EMC publications:

- Dell Digital Locker (for the latest OS10EE version) https://www.dell.com/support/software/us/en/4?~ck=mn.
- OS10EE Enterprise Edition Spec Sheet http://i.dell.com/sites/doccontent/shared-content/data-sheets/en/Documents/dell_networking_os10_spec_sheet.pdf
- ONIE Manually Loading DNOS on a Switch http://en.community.dell.com/techcenter/networking/m/networking_files/20442832
- Dell EMC Networking S4148-ON User Guides http://www.dell.com/support/home/us/en/04/product-support/product/networking-s4148f-on/manuals
- Dell EMC Networking Z9100-ON User Guides http://www.dell.com/support/home/us/en/19/product-support/product/networking-z9100/manuals
- ONIE User Guide https://opencomputeproject.github.io/onie/user-guide/index.html
- Dell EMC Networking Whitepapers http://en.community.dell.com/techcenter/networking/p/guides
- Leaf-Spine Deployment and Best Practices Guide http://en.community.dell.com/techcenter/networking/m/networking_files/20444291
- Dell EMC Networking L3 Design for Leaf-Spine with OS10 http://en.community.dell.com/techcenter/networking/m/networking_files/20487411

B Hardware and software versions used in this document

The examples in this document were validated using the following software versions:

Hardware/software	Versions
Dell EMC Networking S3048-ON	DNOS 10.4.0E (R3) DNOS 10.4.0E (R3P1) DNOS 10.4.0E (R3P2)
Dell EMC Networking S4148-ON	
Dell EMC R630 BIOS	2.4.3, 2.7.1
Dell EMC R630 iDRAC	2.41.40.40, 2.52.52.52
Intel NIC (for XC630)	17.5.10,18.0.17
Microsoft Windows 2012 Server	R2 Standard

C Contact technical support

Technical support contact information

Web: http://www.dell.com/support

Telephone: USA: 1-800-945-3355

We encourage readers of this publication to provide feedback on the quality and usefulness of this deployment guide by sending an email to Dell_Networking_Solutions@Dell.com.