

Dell EMC Networking Surveillance Networking Quick Reference Guide

Supplement to the Dell EMC Surveillance Reference Architecture and Implementation
Guide

Dell EMC Networking Infrastructure Solutions
March 2018

Revisions

Date	Description	Authors
March 2018	Initial release	Colin King, Gerald Myres

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND. Copyright © 2018 Dell Inc. All rights reserved. Dell and the Dell EMC logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of contents

Revisions.....	2
1 Introduction.....	5
2 Objective.....	6
3 Surveillance networks summary.....	7
3.1 Topologies	7
3.1.1 Dedicated full mesh network	7
3.1.2 Distributed ring network.....	8
3.1.3 Converged full mesh network	9
3.1.4 Small scale traditional network for SMB.....	9
4 Networking switch models.....	11
4.1 Dell EMC Networking S4048 Series.....	11
4.2 Dell EMC Networking X4012.....	11
4.3 Dell EMC Networking S3100 Series.....	11
4.4 Dell EMC Networking N3000 Series.....	12
4.5 Dell EMC Networking N2000 Series.....	12
4.6 Dell EMC Networking N1500 Series.....	13
4.7 Dell EMC Networking N1100 Series.....	13
4.8 Dell EMC Networking X1000 Series.....	13
5 Surveillance networking features	14
5.1 802.1X authentication	14
5.1.1 Dell EMC Networking OS 6	14
5.1.2 Dell EMC Networking OS 9	15
5.1.3 Dell EMC Networking OS 3	15
5.2 Quality of Service (QoS).....	16
5.2.1 Differentiated Services (DiffServ)	16
5.2.2 Single priority example	16
5.2.3 Multiple priority example.....	21
5.2.4 Multiple priority with WRED	22
5.2.5 Multiple priority with strict queuing.....	26
5.3 Multicast features.....	27
5.3.1 L2 Multicast features	27
5.3.2 L3 Multicast features	28

5.4	Automatic port configuration	29
5.4.1	Device identification with Link Layer Discovery Protocol (LLDP)	30
6	Power over Ethernet.....	33
6.1	PoE features	33
6.1.1	PoE, PoE+, PoE 60W	33
6.1.2	Dell EMC Networking OS6 PoE features	33
6.1.3	Dell EMC Networking OS9 PoE features	34
6.1.4	Dell EMC Networking OS3 PoE features	34
6.2	PoE budget planning methodology.....	35
6.2.1	PoE budget example	35
7	Networking features for topologies.....	39
7.1	Virtual Link Trunking	39
7.2	Force10 Resilient Ring Protocol	40
7.3	Virtual Routing and Forwarding	40
7.4	VLAN routing for X-Series switches	41
A	Validated hardware and components.....	42
B	Technical support and resources	43
B.1	Related resources.....	43
B.2	Feedback	43

1 Introduction

Surveillance solutions that enable organizations to monitor their assets and protect individuals consist of many components. Cameras, security software, and storage are the common pieces associated with a complete solution. In addition, the network that connects all of these components is a key element in a robust and stable surveillance system.

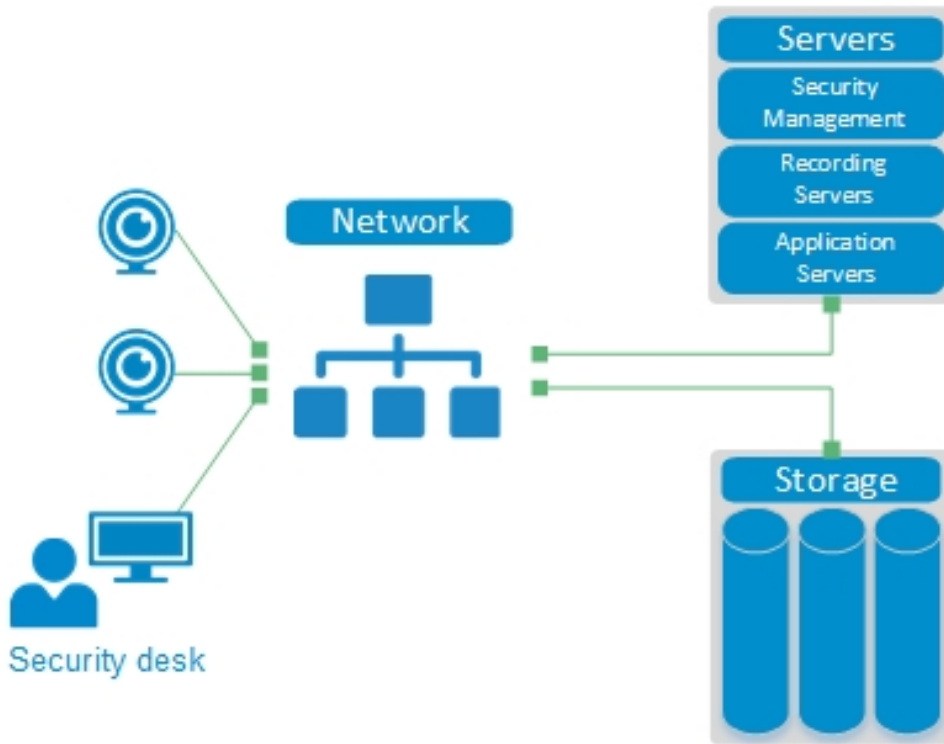


Figure 1 Surveillance solution key components

2 Objective

This supplemental document contains information common to most surveillance networks. It discusses networking features and topologies used in many access networks to support surveillance cameras, video, and management traffic. The configuration and sizing examples enable the reader to apply standard networking methods to various deployment types.

Table 1 Supplemental configuration guide definition

Is	Is not
<ul style="list-style-type: none">• Configuration examples to apply to many types of network deployments• Sizing guide for Power over Ethernet on an example network• Networking feature information for access networks	<ul style="list-style-type: none">• Step by step instructions for a specific deployment• Sizing guide rules for Power over Ethernet to apply for every type of deployment scenario• Data center design practices• Instructions for surveillance management and appliance deployment• Instructions for storage design and deployment

3 Surveillance networks summary

Surveillance solutions may contain many of the same common components. However, the network topologies can significantly change based on the organization’s security requirements and other application traffic on the network. This section provides information on several types of network topologies common within industries deploying surveillance solutions.

3.1 Topologies

The following topologies show the most common deployments for both converged and dedicated security networks.

3.1.1 Dedicated full mesh network

Networks dedicated to only transporting surveillance traffic have several benefits over converged networks that also transport application, internet, and phone traffic. Surveillance traffic on dedicated networks does not have to deal with traffic competing for bandwidth. User generated traffic due to file transfers, applications, or video streaming can initiate intermittent traffic spikes and cause congestion.

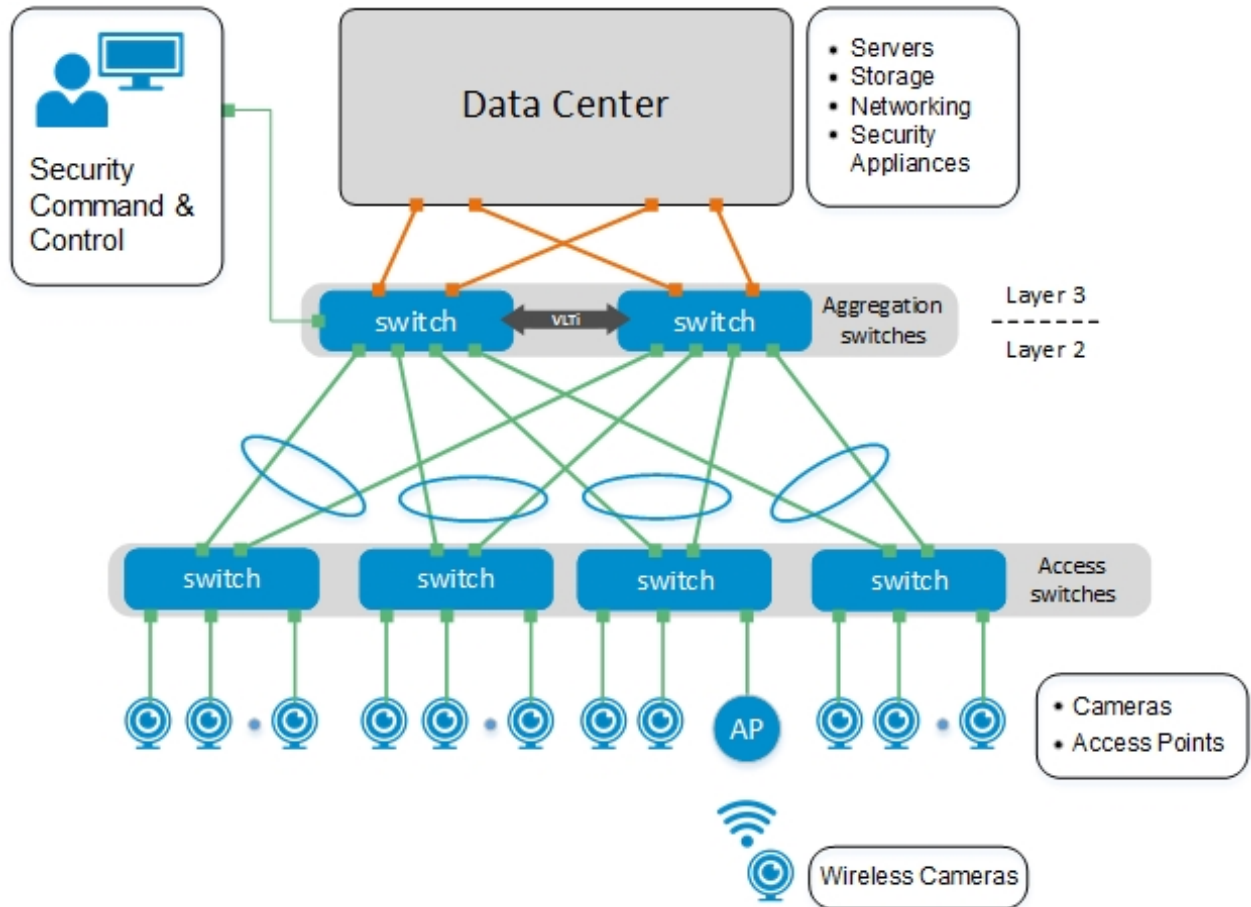


Figure 2 Dedicated full mesh network

Dedicated full mesh networks feature full use of available bandwidth while providing redundancy. Dell EMC Networking uses Virtual Link Trunking (VLT) to provide load-balancing in a loop-free topology.

Configuration examples for VLT can be found in the [Leaf-Spine Deployment and Best Practices Guide](#) and the [Dell EMC Surveillance Implementation Guide](#).

3.1.2 Distributed ring network

A distributed ring network can connect multiple buildings or sites. Each access network can connect to a single data center at the main site where security appliances and storage are centrally located.

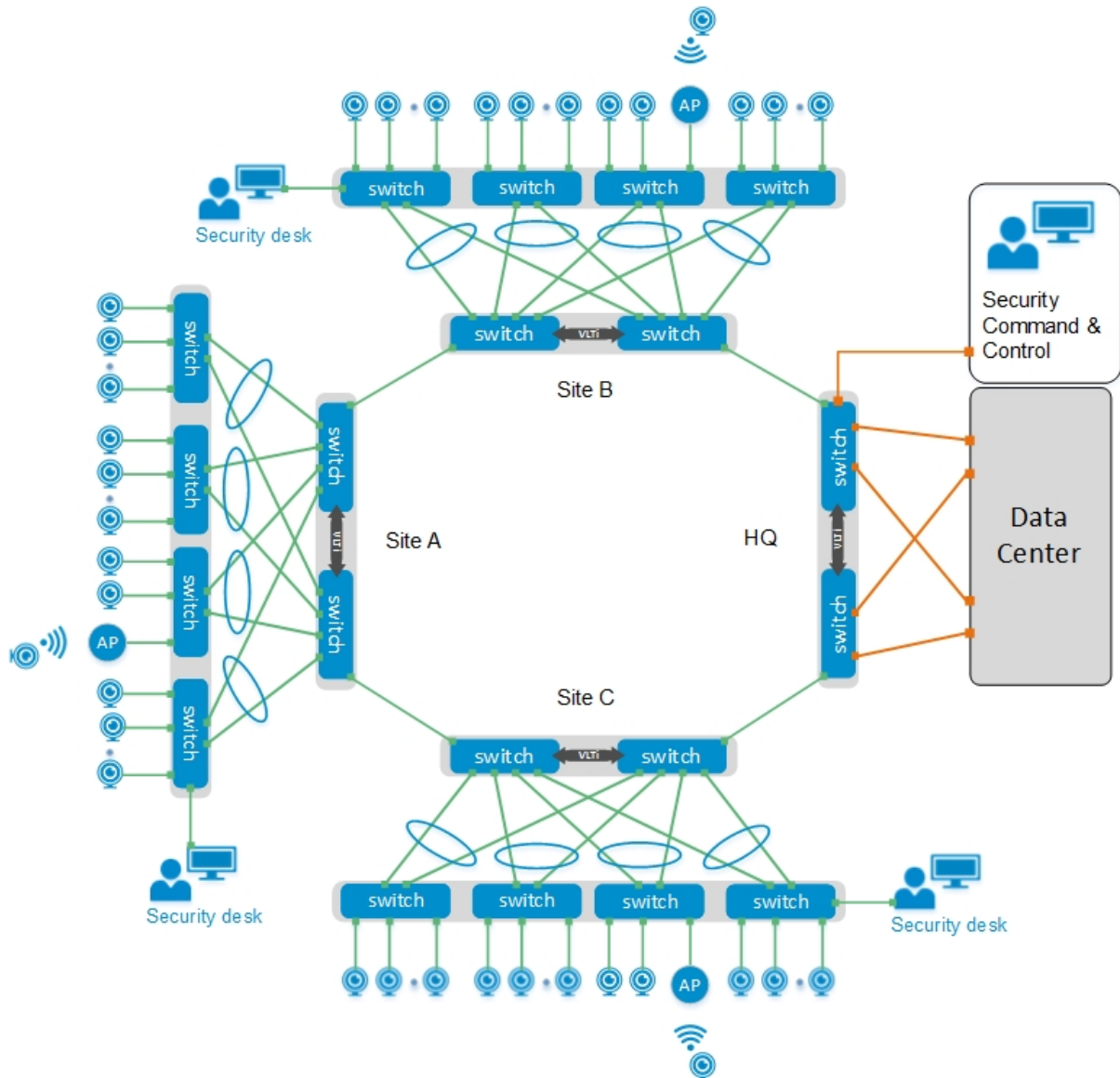


Figure 3 Distributed ring network

Distributed ring networks use Force10 Resilient Ring Protocol (FRRP) to create ring topologies with fast convergence without the use of Spanning Tree Protocol (STP). Configuration examples for FRRP can be found in the [Dell EMC Surveillance Implementation Guide](#).

3.1.3 Converged full mesh network

A network with converged traffic that transports all user generated traffic and surveillance traffic is a cost effective way to support all business needs. The administration, power, and physical space can be consolidated to realize savings in addition to the hardware costs.

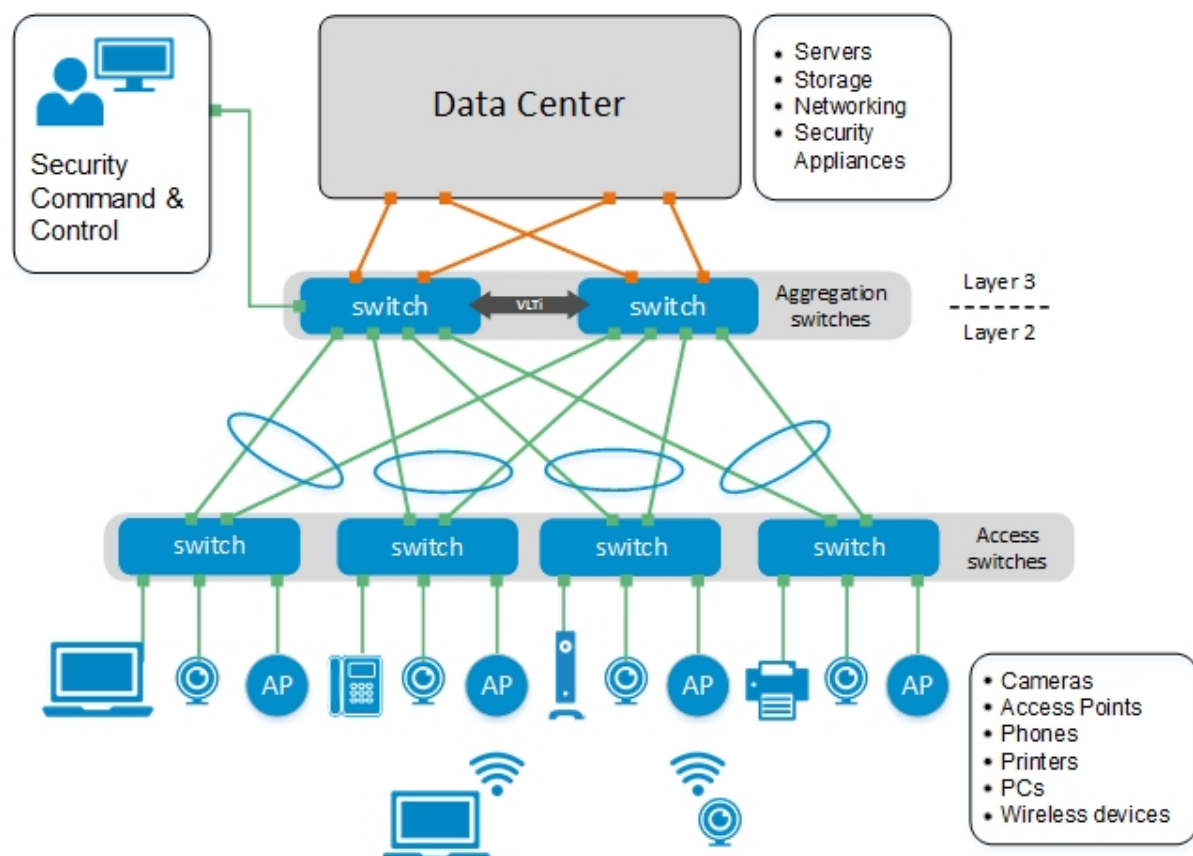


Figure 4 Converged full mesh network

The converged full mesh network uses the same topology as the dedicated full mesh network. To increase security, network administrators may choose to deploy Virtual Routing and Forwarding (VRF) to separate the sensitive surveillance and security traffic from the user traffic. Configuration examples for VRF can be found in the [Dell EMC Surveillance Implementation Guide](#).

3.1.4 Small scale traditional network for SMB

Small to medium-sized businesses without a central data center often have smaller scale network topologies. Dell EMC Networking offers many options based on performance and cost without sacrificing security requirements for the surveillance solution.

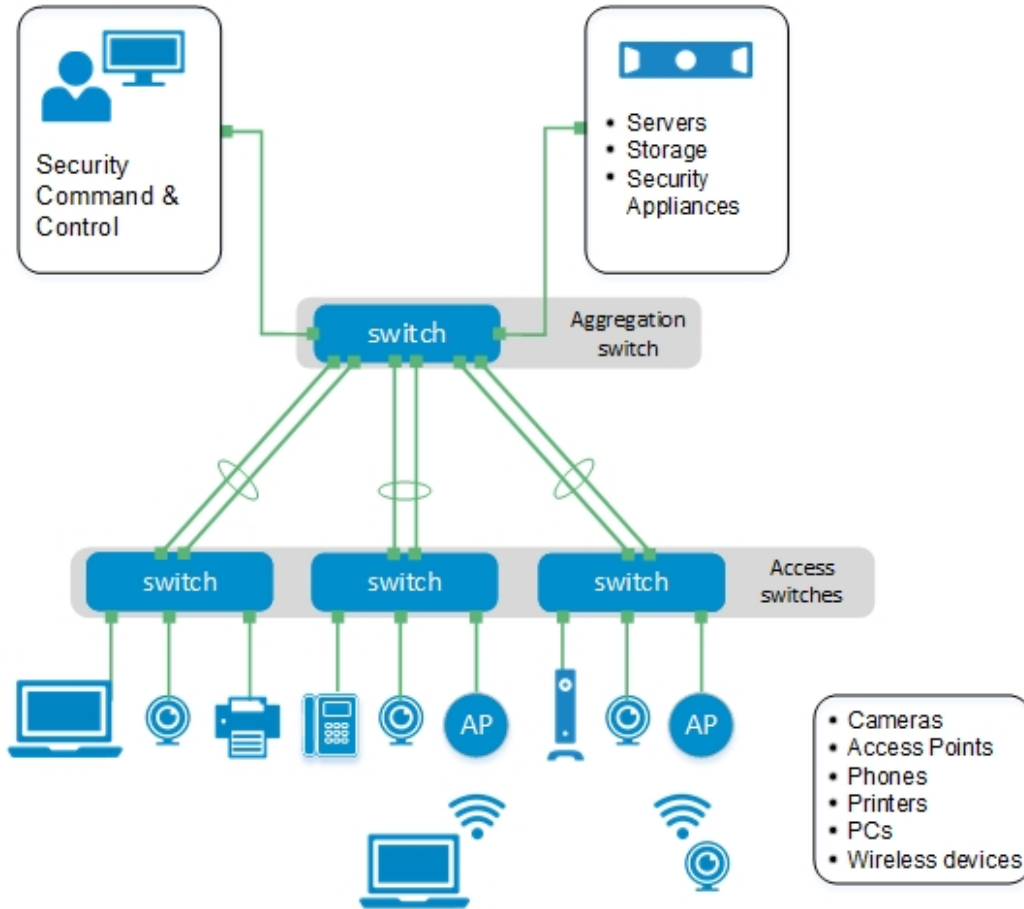


Figure 5 Small scale converged network for SMB

4 Networking switch models

Dell EMC Networking offers switch models for use within a campus network and the data center. This section provides basic details on switches that can be used in all of the topologies shown in the preceding sections.

4.1 Dell EMC Networking S4048 Series

The Dell EMC Networking S4048 Series switches are 1RU, multilayer switches with forty-eight 10GbE ports and 6x 40GbE QSFP+ ports. These switches are ideal for the aggregation layer in the campus network, in addition to top of rack duties within the data center. The S4048-ON has 48x 10GbE SFP+ ports, while the S4048T-ON has 48x 10GBASE-T ports. The S4048-ON switch supports OS 9.



Figure 6 Dell EMC Networking S4048-ON

4.2 Dell EMC Networking X4012

The Dell EMC Networking X4012 is a 1RU, layer 2+ switch with twelve 10GbE SFP+ ports. This switch is ideal for SMB customers who still require an aggregation layer for their campus networks and pairs well with the X1000 Series switches. The X4012 switch supports OS 3.



Figure 7 Dell EMC Networking X4012

4.3 Dell EMC Networking S3100 Series

The Dell EMC Networking S3100-ON Series switches are 1RU, multilayer PoE+ capable switches that are available in a variety of port configurations. As a campus access switch, the S3124P and S3148P provide PoE+ ports to power video surveillance cameras in the campus network. The S3100 Series switches support OS 9.



Figure 8 Dell EMC Networking S3148P-ON

4.4 Dell EMC Networking N3000 Series

The Dell EMC Networking N3000 Series switches are 1RU, multilayer PoE+/PoE 60W switches that are available in a variety of port configurations. As a campus access switch, the N3024P and N3048P provide PoE+/PoE 60W ports to power video surveillance cameras in the campus network. The N3000 Series switches support OS 6.

The Dell EMC Networking N3132PX-ON is a 1RU, multilayer PoE 60W switch with twenty-four 1GbE ports, eight 2.5/5GbE ports, and four 10GbE SFP+ ports. This switch is ideal as a campus access switch for customers that require PoE 60W and multi-rate 2.5/5GbE ports.

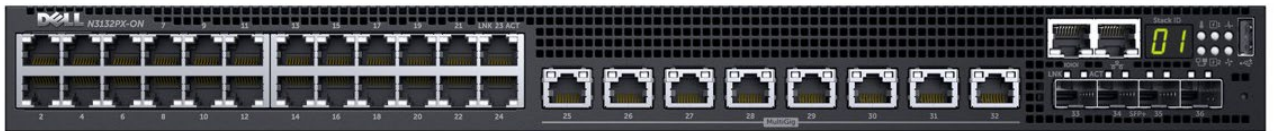


Figure 9 Dell EMC Networking N3132PX-ON

4.5 Dell EMC Networking N2000 Series

The Dell EMC Networking N2000 Series switches are 1RU, multilayer PoE+ switches that are available in a variety of port configurations. As a campus access switch, the N2024P and N2048P provide PoE+ ports to power video surveillance cameras in the campus network. The N2000 Series switches support OS 6.

The Dell EMC Networking N2128PX-ON is a 1RU, multilayer PoE+/PoE 60W switch with twenty-four 1GbE ports (PoE+), four 2.5GbE ports (PoE 60W), and two 10GbE SFP+ ports. This switch is ideal as a campus access switch for customers that require PoE 60W and 2.5GbE ports.



Figure 10 Dell EMC Networking N2128PX-ON

4.6 Dell EMC Networking N1500 Series

The Dell EMC Networking N1500 Series switches are 1RU, multilayer (Layer 3 Lite) PoE+ switches that are available in a variety of port configurations. As a campus access switch, the N1524P and N1548P provide PoE+ ports to power video surveillance cameras in the campus network. This switch is ideal as a campus access switch. The N1500 Series switches support OS 6.



Figure 11 Dell EMC Networking N1524P

4.7 Dell EMC Networking N1100 Series

The Dell EMC Networking N1100 switches are 1RU, layer 2 PoE/PoE+ switches that are available in a variety of port configurations. As a campus access switch, the N1108P-ON, N1124P-ON, and N1148P-ON provide PoE+ ports to power video surveillance cameras in the campus network. This switch is ideal as a campus access switch for customers with smaller deployments. The N1100 Series switches support OS 6.



Figure 12 Dell EMC Networking N1108P-ON

4.8 Dell EMC Networking X1000 Series

The Dell EMC Networking X1000 Series are layer 2+, web-managed, PoE/PoE+ switches that are available in a variety of port configurations. The X1008P and X1018P provide PoE port capability, while the X1026P and X1052P provide PoE+ ports to power video surveillance cameras in the campus network. This switch is ideal as a campus access switch for customers with smaller deployments. The X1000 Series switches support OS 3.

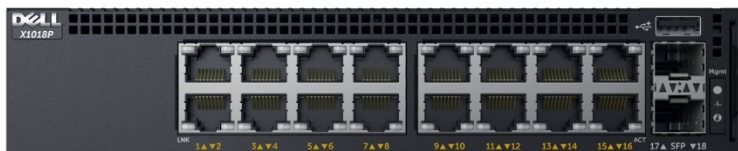


Figure 13 Dell EMC Networking X1018P

5 Surveillance networking features

Surveillance networks and the devices used to collect and transmit video require common features found on most networks. Dell EMC Networking switches provide those features to enable high-performing, quality video transmission. In addition to video, Dell EMC Networking switches include features used for client, application, and management traffic on the campus or data center networks.

5.1 802.1X authentication

Securing the network through authentication is necessary for users, clients, and devices. Surveillance cameras include 802.1X functionality to allow network administrators secure all access ports, especially those within public reach.

802.1X authentication process includes a supplicant, an authenticator, and an authentication server. The supplicant in terms of a surveillance network is typically the camera. In a converged network, PCs and printers may be other common supplicants. The authentication server is traditionally a RADIUS server, and is located within the data center. This section will detail the configuration of the authenticator, which is the Dell EMC access switch connected directly to the cameras.

In each of the subsections below, the examples show how to configure the switch for an 802.1X enabled camera on each switch OS type.

Note: The configuration steps in the subsequent sections show only the commands to enable 802.1X with a RADIUS server. Commands for general port functionality are not shown. For additional assistance with authentication or other switch features, see the appropriate user's guide.

5.1.1 Dell EMC Networking OS 6

This section details the basic configuration for a switch running OS 6.

1. Configure the RADIUS server IP address and shared secret (secret).

```
Dell#configure
Dell(config)#radius-server host 10.10.10.10
Dell(config-auth-radius)#key "secret_key_string"
Dell(config-auth-radius)#exit
```

2. Enable 802.1X port-based access control on the switch.

```
Dell(config)#dot1x system-auth-control
```

3. (Optional) Configure any port to remain in the authorized state, which allows connection without authentication.

```
Dell(config)#interface Te1/0/1
Dell(config-if)#dot1x port-control force-authorized
Dell(config-if)#exit
```


5.1.2 Dell EMC Networking OS 9

This section details the basic configuration for a switch running OS 9.

1. Configure the RADIUS server IP address and shared secret (secret).

```
Dell#configure
Dell#(conf)radius-server host 10.10.10.10
Dell#(conf)radius-server key 0 secret_key_string
```

2. Enable 802.1X globally.

```
Dell#configure
Dell(conf)#dot1x authentication
```

3. Enter INTERFACE mode on the interface or range of interfaces which require authentication and enable 802.1X on each interface.

```
Dell(conf)#interface range gigabitethernet 1/1 - 1/10
Dell(conf-if-range-gi-1/1-1/10)#dot1x authentication
```

5.1.3 Dell EMC Networking OS 3

This section details the basic configuration for a switch running OS 3.

1. Globally configure 802.1X authentication.
 - a. Click **Network Administration > Security > Dot1 Authentications**
 - b. Edit the **Port Based Authentication - Global** settings by clicking **Edit**.
 - i. **Port Based Authentication State** select **Enabled**.
 - ii. **Authentication Method** select **RADIUS**.
 - iii. Leave all remaining settings at defaults, Click **OK**.
2. Configure the RADIUS server IP address and shared secret (secret).
 - a. Click **Switch Management > Management Security**.
 - i. Edit the **RADIUS** server setting by clicking **Edit**.
 - ii. Click **+Add**.
 - iii. Enter the **Host IP Address** of the RADIUS server.
 - iv. Enter a **Priority** value. Enter **0** if only using a single RADIUS server.
 - v. Enter a **Key String** for the RADIUS shared secret.
 - vi. Select **802.1x** for the **Usage Type**.
 - vii. Leave all remaining settings at defaults, Click **OK**.
3. Configure 802.1X authentication on each interface that requires authentication.
 - a. Click **Network Administration > Security > Dot1 Authentications**
 - b. Edit the **Port Based Authentication - Interface Settings** by clicking **Edit**.
 - i. Click the **Edit** icon  of the interface that requires authentication.
 - ii. Change **Admin Interface Control** to **Auto**.
 - iii. Ensure **Authentication Type** is set to **802.1x Only**.
 - iv. Leave all remaining settings at defaults, Click **OK**.

5.2 Quality of Service (QoS)

Surveillance network traffic can be classified as critical in many deployments. The quality of the surveillance video can be impacted if networks are oversubscribed and start dropping traffic. This section provides details on configuring basic QoS features on Dell EMC Networking switches. The examples provided apply to different levels of complexity and depend on the type of traffic on the network.

5.2.1 Differentiated Services (DiffServ)

DiffServ is a QoS mechanism that can be utilized over a layer 3 network and is the most common standardized method for managing network traffic. DiffServ uses a Differentiated Services Code Point (DSCP) value to classify different types of network traffic. Surveillance cameras can be configured to apply a DSCP value to its traffic. Dell EMC Networking switches can use the DSCP marking from the camera to perform QoS services.

Note: This guide does not provide instructions for a specific model of surveillance camera. Consult the camera's user guide to confirm DSCP marking capability and configuration steps.

5.2.2 Single priority example

The example detailed in this section assumes that video surveillance traffic has the highest priority and all other traffic on the network is best effort. This type of QoS plan is simple and easy to implement.

A typical customer that implements this type of QoS configuration may have occasional bursts of file transfer traffic alongside the surveillance video traffic. A network that also services voice, multimedia, or critical application traffic should implement a QoS scheme detailed in the next example.

5.2.2.1 Surveillance camera setup

The camera in this example assumes that all traffic originating from the camera is marked with the same DSCP value. Some cameras have advanced features to include audio, alarms, and management. This example places all of those traffic categories into a single DSCP value. If desired, any of the less critical traffic types on the camera can be marked with the default value of 0.

1. Locate the QoS settings for the camera with the camera's management interface.
2. Set the video traffic's DSCP value to 46.
3. Set all other traffic types to 46 if critical, or 0 for best effort.

Note: All other traffic on the network will be considered best effort, or an equivalent DSCP value of 0.

5.2.2.2 Dell EMC Networking OS 6

This section details the basic configuration for a switch running OS 6.

Example summary:

- N-Series access switch using OS 6.5.0.2
- Camera connected to interface Gi1/0/10
- Uplink interfaces Te1/0/1 and Te1/0/2 connected to aggregation layer switches
 - Uplink interfaces are configured as a LAG (LAG commands not shown)

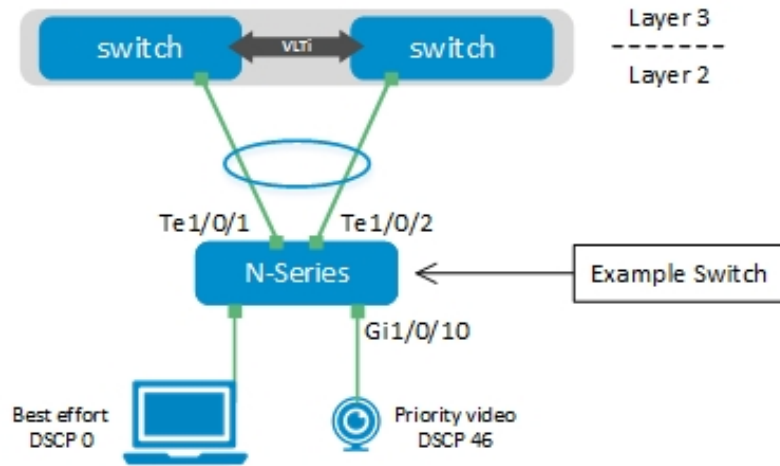


Figure 14 Single priority example diagram

1. Enable diffserv:

```
Dell#configure
Dell(config)#diffserv
```

2. Set interface to the camera to trust DSCP:

```
Dell(config)#interface Gi1/0/10
Dell(config-if-Gi1/0/10)#classofservice trust ip-dscp
Dell(conf-classmap)#exit
```

3. Repeat the steps above for each interface on the switch that connects to a camera.
4. Globally set queue 6 on all ports to use strict priority mode:

```
Dell(config)#cos-queue strict 6
```

5. Create a class-map to match all DSCP values of 46:

```
Dell(config)#class-map match-all class_46
Dell(config-classmap)#match ip dscp 46
Dell(conf-classmap)#exit
```

6. Create a policy-map to assign the class-map to the strict queue:

```
Dell(config)#policy-map pol_camera out
Dell(config-policy-map)#class class_46
Dell(config-policy-classmap)#assign-queue 6
Dell(conf-classmap)#exit
```

7. Assign the policy-map to the uplink interfaces outbound:

```
Dell(config)#interface range Te1/0/1-2
Dell(config-if)#service-policy out pol_camera
```

```
Dell(config-if)#exit
Dell(config)#exit
```

The configuration above prioritizes all traffic with a DSCP marking of 46 on the outbound uplink interfaces. Strict priority traffic classes have unlimited bandwidth and are serviced before all other CoS queues. If more than one strict queue is defined, they are serviced in order from queue priority 6 to 0.

Note: The above example can be applied to any switch in the network that is experiencing congestion. This example shows an access switch, but the same methodology can be used on aggregation switches.

5.2.2.3 Dell EMC Networking OS 9

This section details the basic configuration for a switch running OS 9.

Example summary:

- S-Series access switch using OS 9.13 (0.0)
- Camera connected to interface Gi1/10
- Uplink interfaces Te1/25 and Te1/26 connected to aggregation layer switches
 - Uplink interfaces are configured as a LAG (LAG commands not shown)

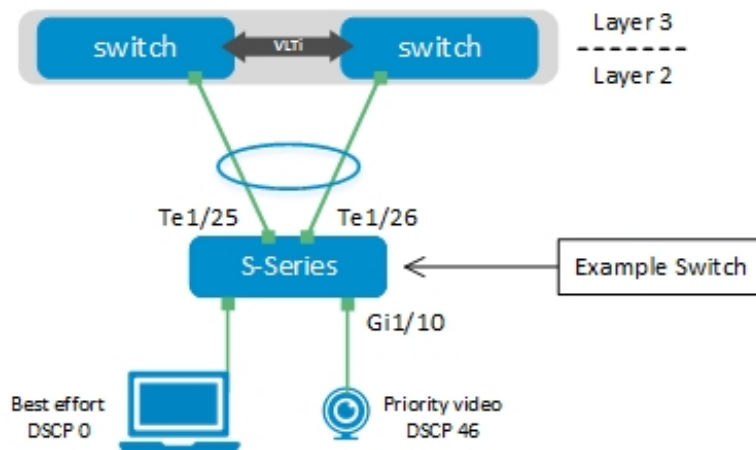


Figure 15 Single priority example diagram

1. Create a class-map to match all DSCP values of 46:

```
Dell#configure
Dell(conf)#class-map match-any class_46
Dell(conf-class-map)#match ip dscp 46
Dell(conf-class-map)#exit
```

2. Create an input policy-map to assign the class-map to a queue.

```
Dell(conf)#policy-map-input pin_camera
Dell(conf-policy-map-in)#service-queue 3 class-map class_46
```

```
Dell(conf-policy-map-in)#exit
```

3. Assign the input policy-map to the camera interfaces.

```
Dell(conf)#interface Gi1/10
Dell(conf-if-gi-1/10)#service-policy input pin_camera
Dell(conf-if-gi-1/10)#exit
```

4. Create a qos output policy for the video traffic.

```
Dell(conf)#qos-policy-ouput qos_camera
Dell(conf-qos-policy-out)#scheduler strict
Dell(conf-qos-policy-out)#exit
```

5. Create an output policy map for the video traffic.

```
Dell(conf)#policy-map-ouput pout_camera
Dell(conf-policy-map-out)#service-queue 3 qos-policy qos_camera
Dell(conf-policy-map-out)#exit
```

6. Apply the output policy to each switch uplink.

```
Dell(conf)#interface range Te 1/25 - 1/26
Dell(conf-if-range-te-1/25-1/26)#service-policy output pout_camera
Dell(conf-if-range-te-1/25-1/26)#exit
Dell(conf)#exit
```

The configuration above prioritizes all traffic with a DSCP marking of 46 on the outbound uplink interfaces. Strict priority traffic classes have unlimited bandwidth and are serviced before all other CoS queues. If more than one strict queue is defined, they are serviced in order from queue priority 3 to 0 on 4 queue switches, and 7 to 0 on 8 queue switches.

Note: The above example can be applied to any switch in the network experiencing congestion. This example shows an access switch, but the same methodology can be used on aggregation switches.

5.2.2.4 Dell EMC Networking OS 3

This section details the basic configuration for a switch running OS 3.

Example summary:

- X-Series access switch using OS 3.0.0.95
- Camera connected to interface Gi1/1
- Uplink interface Gi1/3 connected to an aggregation switch

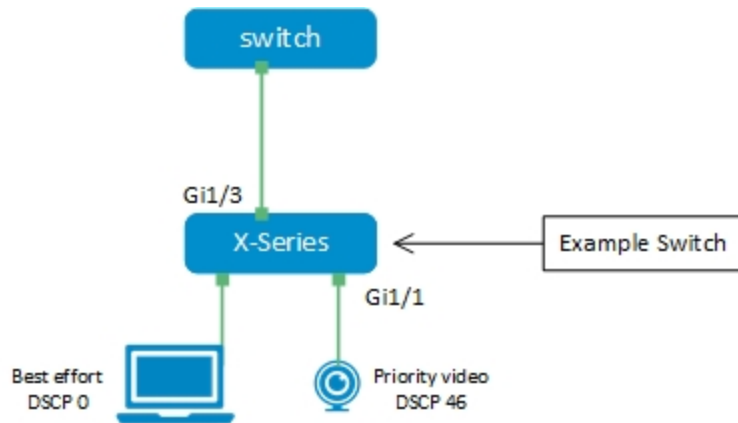


Figure 16 Single priority example diagram

1. Set the QoS priority method to strict for all queues:
 - a. Click **Network Administration > Quality of Service > Global Settings > Queue Scheduling**
 - i. Ensure **Strict Priority** (default) is configured by viewing the scheduling method settings
2. Map the DSCP value of 46 to Queue 4:
 - a. Click **Network Administration > Quality of Service > Global Settings > DSCP to Queue**
 - i. Edit the **DSCP to Queue** settings by clicking **Edit**.
 - ii. Set the **DSCP In** value of 46 to Queue **4** by using the dropdown menu in the Queue column.

Note: This example uses the X1018P, which has a total of 4 queues.

- iii. Click **OK**.
3. Create an Access Control List (ACL) to hold the Access Control Entry (ACE) that filters all traffic with DSCP marking of 46.
 - a. Click **Network Administration > Security > ACL and ACE**.
 - b. Edit the **IPv4 Based ACL** by clicking **Edit**.
 - c. Click on the **+Add** link to add a new ACL
 - d. Enter an **ACL Name**, for example *ACL_46*
 - e. Click **OK**
4. Create an ACE to filter all traffic with DSCP marking of 46.
 - a. Click **Network Administration > Security > ACL and ACE**.
 - b. Edit the **IPv4 Based ACE** by clicking **Edit**.
 - c. Click on the **+Add** link to add a new ACE. Ensure the *ACL_46* name is shown in the ACL dropdown box.
 - d. Enter a priority for the **New ACE Priority**, for example *100*.
 - e. Scroll down to **Classification** setting and check the checkbox. Enter a value of *46* for the **Match DSCP** setting.
 - f. Leave all other settings at defaults
 - g. Click **OK**
5. Create a class map to define the camera traffic.
 - a. Click **Network Administration > Quality of Service > QoS Mapping > Class Mapping**.
 - b. Edit the **Class Mapping** settings by clicking **Edit**.
 - i. Click on the **+Add** link to add a new class map.

- ii. Enter a **Class Map Name**, for example *class_46*.
 - iii. For **IP ACL**, check **IPv4**, ensure the *ACL_46* name appears in the drop-down box.
 - iv. Leave all remaining settings at defaults.
 - v. Click **OK**.
6. Create a Policy Table to hold the Policy Class Map.
 - a. Click **Network Administration > Quality of Service > QoS Mapping > Policy Table**
 - b. Click on the **+Add** link to add a new policy table
 - c. Enter a **Policy Name**, for example *pol_table_camera*
 - d. Click **OK**
7. Create a Policy Class Map to contain the Class Map.
 - a. Click **Network Administration > Quality of Service > QoS Mapping > Policy Class Maps**
 - b. Edit the **Policy Class Maps** settings by clicking **Edit**
 - c. Click on the **+Add** link to add a new policy class map. Ensure the *pol_table_camera* name is shown in the drop-down box.
 - d. Ensure the **Class Map Name** is *class_46*.
 - e. Set **Action Type** to **Trust CoS-DSCP**.
 - f. Leave all remaining settings at defaults
 - g. Click **OK**
8. Bind the Policy Class Map to the appropriate uplink interface.
 - a. Click **Network Administration > Quality of Service > QoS Mapping > Policy Binding**
 - b. Edit the **Policy Binding** settings by clicking **Edit**
 - c. Click on the **+Add** link to add a new policy binding
 - d. Select the **Interface**, in this example *Gi1/0/3*
 - e. Select the **Policy Name**, in this example *pol_table_camera*
 - f. Click **OK**.

The configuration above prioritizes all traffic with a DSCP marking of 46 on the outbound uplink interfaces. Strict priority traffic classes have unrestricted bandwidth and are serviced before all other CoS queues. If more than one strict queue is defined, they are serviced in order from queue priority 4 to 1.

5.2.3 Multiple priority example

Converged networks with both security and user traffic may have multiple types of traffic that can be a priority. One of the most common types of priority user traffic is Voice over IP (VoIP). This section will expand on the single priority example in the previous section, and use VoIP traffic as another high priority traffic class.

This example uses the same assumptions on the source DSCP marking of traffic. Both the camera and the VoIP phone have the ability to mark their own DSCP traffic from the device.

Note: The generic camera and VoIP phone setup instructions are the same as the previous example. The only change is in the value assigned to each type of traffic type.

Typical standard practice is to set VoIP traffic to a DSCP value of 46, and video traffic to a DSCP value of 34. A DSCP value of 46 is classified as Expedited Forwarding (EF), or critical priority. A DSCP value of 34 is classified as Flash Override, and has a low drop probability when using default QoS policies. The examples in

this document do not use default policies in to fully demonstrate the flexibility of the features. Each DSCP value is mapped to a specific queue to show how to configure the switch for any situation or requirement.

5.2.4 Multiple priority with WRED

The Dell EMC Networking switches use DSCP marking to place the appropriate traffic into separate queues for prioritization. The configuration example in this section places higher priorities on VoIP and video traffic, and a lower priority on other user traffic.

Dell EMC Networking switches provide a high degree of customization for QoS. Some options available include bandwidth limitations, Weighted Random Early Detection (WRED) and Explicit Congestion Notification (ECN). There is not a generic, one-size-fits-all approach to QoS. The strict queuing used in this example could easily be substituted with explicit bandwidth assignments. Administrators can use this example as a starting point for their QoS strategy.

The configuration example below accomplishes the following:

- Uses the DSCP values as configured on the distributed port groups
- Maps DSCP input traffic to specified queues and DSCP color
- Prioritizes egress traffic on uplinks through strict queuing and WRED

5.2.4.1 Dell EMC Networking OS 6

This section details a basic configuration for a switch running OS 6.

Example summary:

- N-Series access switch using OS 6.5.0.2
- Camera connected to interface Gi1/0/10
- VoIP phone connected to interface Gi1/0/11
- Uplink interfaces Te1/0/1 and Te1/0/2 connected to aggregation layer switches
 - Uplink interfaces are configured as a LAG (LAG commands not shown)

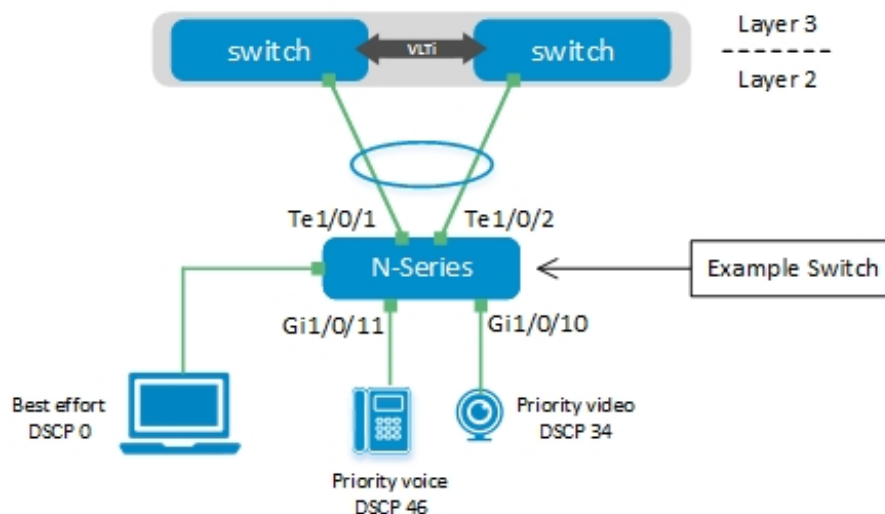


Figure 17 Single priority example diagram

1. Enable diffserv.

```
Dell#configure  
Dell(config)#diffserv
```

2. Set interfaces to the camera and phone to trust DSCP.

```
Dell(config)#interface range Gi1/0/10-11  
Dell(config-if)#classofservice trust ip-dscp  
Dell(config-if)#exit
```

3. Repeat steps 1 and 2 for each interface on the switch that connects to a camera or phone.
4. Create a class-map to match all DSCP values of 46.

```
Dell(config)#class-map match-all class_46  
Dell(config-classmap)#match ip dscp 46  
Dell(config-classmap)#exit
```

5. Create a class-map to match all DSCP values of 34.

```
Dell(config)#class-map match-all class_34  
Dell(config-classmap)#match ip dscp 34  
Dell(config-classmap)#exit
```

6. Globally set queue 6 on all ports to use strict priority mode.

```
Dell(config)#cos-queue strict 6
```

7. Globally set queue 5 on all ports to use strict priority mode.

```
Dell(config)#cos-queue strict 5
```

8. Create a policy-map to assign the class-map to the strict queues.

```
Dell(config)#policy-map pol_phone_camera out  
Dell(config-policy-map)#class class_46  
Dell(config-policy-classmap)#assign-queue 6  
Dell(conf-classmap)#exit  
Dell(config-policy-map)#class class_34  
Dell(config-policy-classmap)#assign-queue 5  
Dell(conf-classmap)#exit
```

9. Assign the policy-map to the uplink interfaces outbound.

```
Dell(config)#interface range Tel1/0/1-2  
Dell(config-if)#service-policy out pol_phone_camera  
Dell(config-if)#exit  
Dell(config)#exit
```

10. Configure thresholds for standard traffic.

```
Dell(config)#random-detect queue-params 0 min-thresh 150 30 20 100 max-thresh 200 90 80 100 drop-prob-scale 2 10 10 100
```

11. Enable WRED on cos-queue 0.

```
Dell(conf)#cos-queue random-detect 0
```

The configuration above prioritizes voice traffic with a DSCP marking of 46 on the outbound uplink interfaces, followed by video traffic with a DSCP marking of 34. Strict priority traffic classes have unlimited bandwidth and are serviced before all other CoS queues. The WRED configuration is a starting point for tuning the congestion behavior of all other traffic. As configured above, all traffic is considered green since the color-aware policer is not enabled. Cos-queue 0 is the default queue for all non DSCP marked traffic. This WRED configuration has user traffic dropping at a drop probability of 2% between the thresholds of 150% to 200% of the switch buffer. Administrators should monitor the switch congestion with the command **show interfaces traffic** and adjust the WRED parameters as needed.

Note: The size of the switch buffer varies according to the switch model. Consult the specifications of the appropriate switch model to determine the size of the buffer on each switch.

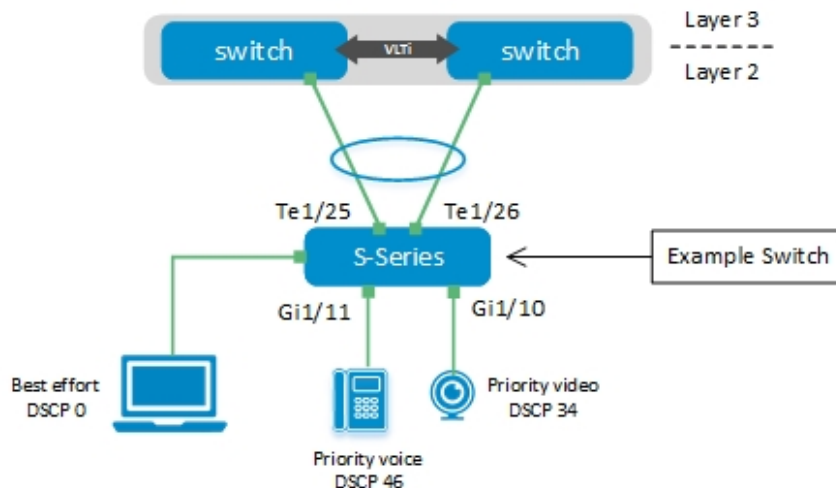
5.2.4.2 Dell EMC Networking OS 9

This section details the basic configuration of a switch running OS 9.

Example summary:

- S-Series access switch using OS 9.13 (0.0)
- Camera connected to interface Gi1/10
- VoIP phone connected to interface Gi1/11
- Uplink interfaces Te1/25 and Te1/26 connected to aggregation layer switches

Uplink interfaces are configured as a LAG (LAG commands not shown)



1. Access the command line and enter configuration mode.

```
Dell#configure
```

2. Create a class to match traffic for each DSCP value.

```
Dell(conf)#class-map match-any class_34  
Dell(conf-class-map)#match ip dscp 34  
Dell(conf-class-map)#class-map match-any class_46  
Dell(conf-class-map)#match ip dscp 46  
Dell(conf-class-map)#exit
```

3. Create an input policy map to map each class of traffic to a specific queue.

```
Dell(conf)#policy-map-input pin_phone_camera  
Dell(conf-policy-map-in)# service-queue 2 class-map class_34  
Dell(conf-policy-map-in)# service-queue 3 class-map class_46  
Dell(conf-policy-map-in)#exit
```

4. Create a DSCP color map profile for the application traffic.

```
Dell(conf)#qos dscp-color-map colormap_user  
Dell(conf-qos)#dscp yellow 0  
Dell(conf-qos)#exit
```

5. Apply the input service policy to each camera and phone interface.

```
Dell(conf)#interface range GigabitEthernet 1/10 - 1/11  
Dell(conf-if-range-gi-1/10-1/11)# service-policy input pin_phone_camera  
Dell(conf-if-range-gi-1/10-1/11)# exit
```

6. Apply the input service policy to each user interface.

```
Dell(conf)#interface GigabitEthernet 1/9  
Dell(conf-if-gi-1/9)# qos dscp-color-policy colormap_user  
Dell(conf-if-gi-1/9)# exit
```

7. Create a qos output policy for the storage traffic.

```
Dell(conf)#qos-policy-output qos_phone_camera  
Dell(conf-qos-policy-out)# scheduler strict  
Dell(conf-qos-policy-out)# exit
```

8. Create a WRED profile for the color used in Step 4.

```
Dell(conf)#wred-profile yellow_user_profile  
Dell(conf-wred)# threshold min 1000 max 1500 max-drop-rate 50  
Dell(conf-wred)# exit
```

9. Create a qos output policy for the application traffic.

```
Dell(conf)#qos-policy-output qos_user  
Dell(conf-qos-policy-out)#wred yellow yellow_user_profile
```

```
Dell(conf-qos-policy-out)#exit
```

10. Create an output policy map for each qos policy.

```
Dell(conf)#policy-map-output pout_egress
Dell(conf-policy-map-out)#service-queue 2 qos-policy qos_phone_camera
Dell(conf-policy-map-out)#service-queue 3 qos-policy qos_phone_camera
Dell(conf-policy-map-out)#service-queue 0 qos-policy qos_user
Dell(conf-policy-map-out)#exit
```

11. Apply the output policy with an output service policy to each switch uplink interface.

```
Dell(conf)#interface range TengigabitEthernet 1/25 - 1/26
Dell(conf-if-range-te-1/25-1/26)#service-policy output pout_egress
Dell(conf-if-range-te-1/25-1/26)#exit
```

The configuration above prioritizes voice traffic with a DSCP marking of 46 on the outbound uplink interfaces, followed by video traffic with a DSCP marking of 34. Strict priority traffic classes have unlimited bandwidth and are serviced before all other CoS queues. The WRED configuration is a starting point for tuning the congestion behavior of all other traffic. As configured above, all user traffic is classified as yellow. Cos-queue 0 is the default queue for all non DSCP marked traffic. This WRED configuration has user traffic dropping at a drop probability of 50% between the thresholds of 1000KB to 1500KB of the switch buffer. Administrators should monitor the switch congestion with the command **show qos statistics egress-queue interface X/X** and adjust the WRED parameters as needed.

Note: The size of the switch buffer varies according to the switch model. Consult the specifications of the appropriate switch model to determine the size of the buffer on each switch.

5.2.5 Multiple priority with strict queuing

The simplest way to implement multiple priorities is to assign the most critical traffic to the highest queue, and then assign the next class to the second highest queue. In strict priority queuing, the highest strict queue will be serviced first followed by the next highest strict queue. The remaining queues that are not configured as strict will then be serviced based on their weighted value.

In the example provided in Section 4.2.2, a single high priority strict queue is used for video surveillance. All other traffic is considered as best effort traffic. This example can be expanded to include another traffic class. Using the generic instructions below, apply the same configuration methodology for each OS type:

1. Define a traffic class for voice, set a DSCP value of 46.
2. Define a traffic class for video (cameras), set a DSCP value of 34.
3. Set the two highest CoS queues to strict priority queuing.
4. Map the voice class to the highest queue.
5. Map the video class to the second highest queue.
6. Apply the class maps to the appropriate policy maps.
7. Apply the policies to the appropriate interfaces, in most cases the uplinks.

Note: The instructions above are for a generic switch. Follow the methodology and specific CLI commands as appropriate for the Dell Networking OS being used.

5.3 Multicast features

Multicast features on Dell EMC Networking switches reduce flooding traffic to all network segments or all ports in a VLAN. This reduction in traffic delivers increased bandwidth efficiency, resulting in better quality video or overall capacity of users. The next sections will describe multicast within the context of layer 2 and layer 3 networks.

5.3.1 L2 Multicast features

Layer 2 multicast features provide desired forwarding behavior, sending traffic to only the hosts joining the group in a VLAN. The features associated with managing this behavior are Internet Group Management Protocol (IGMP) snooping for IPv4, and Multicast Listener Discovery (MLD) snooping for IPv6. The following sections describe these features within their respective OS.

Note: MLD and all IPv6 features are not within the scope of this document.

5.3.1.1 Dell EMC Networking OS 6

This section details the multicast features and universal configurations for a switch running OS 6.

IGMP snooping

IGMP snooping is enable by default on all N-Series switches running OS6. No further configuration is required for L2 operation.

5.3.1.2 Dell EMC Networking OS 9

This section details the multicast features and universal configurations for a switch running OS 9.

IGMP snooping

IGMP snooping is disabled by default on all switches running OS 9. To configure OS9 for IGMP snooping on L2 operation, enter the following commands:

```
Dell(conf)#ip igmp snooping enable
Dell(conf)#no ip igmp snooping flood
```

Note: The first command enables IGMP snooping, while the second command disables multicast flooding.

5.3.1.3 Dell EMC Networking OS 3

This section details the multicast features and universal configurations for a switch running OS 3.

IGMP snooping

IGMP snooping is disabled by default on all switches running OS 3. To configure OS 3 for IGMP snooping on L2 operation, use the following GUI configuration steps:

1. Navigate to **Multicast settings for IGMP snooping**.
2. Click **Network Administration > Multicast > Global Parameters**.
3. Edit **Global Parameters** settings by clicking **Edit**.
 - a. Set **IGMP Snooping Status** by selecting **Enabled**.
 - b. Set **IGMP Querier Status** by selecting **Enabled**.
 - c. Click **OK**.

Note: The IGMP Querier simulates the behavior of a Multicast router.

5.3.2 L3 Multicast features

Layer 3 multicast features enable efficient use of network bandwidth by transmitting multicast traffic only once on each network link. The multicast source host sends multicast traffic to a destination multicast group address, and multicast routers forward the traffic to hosts who are members of the multicast group.

In large deployments of surveillance cameras and video management appliances, multicast is an important part of the operation of the network. Cameras routinely transmit multicast traffic to a variety of recipients to include monitoring stations and video management appliances.

Protocol Independent Multicast Sparse Mode (PIM-SM) is a multicast routing protocol that leverages the unicast routing table for forwarding multicast. PIM-SM does not have its own discovery mechanisms, as it uses the routing information from routing protocols such as OSPF and BGP.

5.3.2.1 Dell EMC Networking OS 9

For the video surveillance topologies containing significant routing and a central data center, OS 9 switches are the preferred layer 3 implementation. This section details the OS 9 features and configurations to enable multicast features on layer 3, utilizing a high level example.

Note: The following configuration example does not include a specific topology. It is not intended to use in any specific use case or network deployment. For a fully validated example topology see the [Dell EMC Surveillance Implementation Guide](#).

All switches in the following example use the BGP routing protocol.

1. Enable multicast routing on all switches utilizing routing protocol.

```
ip multicast-routing
```

2. Choose a logical location for the rendezvous points (RP). They should be located in a central area of the network using the multicast groups in the network.
3. Configure an interface to serve as the RP. This example uses a loopback interface.

```
interface loopback 0
  ip address 10.0.1.1/32
  ip pim sparse-mode
```

4. Configure the switches for RP candidates using the following command:

```
ip pim rp-candidate Loopback 0 100
```

Note: Configuring more than one RP will load balance the multicast groups assigned to each RP based on the PIM bootstrap in the next step. More than one RP candidate is also recommended for redundancy.

5. Choose a logical location for the PIM bootstrap router (BSR). Configure the BSR candidates.

```
ip pim bsr-candidate Loopback 0 30 10
```

Note: This example utilizes the same switch for both the RP and BSR. More than one BSR candidate is recommended for redundancy.

The BSR determines the multicast group assignments to the RPs.

6. Configure PIM-SM on each interface using multicast routing on the layer 2/3 boundary and layer 3 network. This is in addition to the command in step 1. The following commands show interfaces that are located within the layer 3 network:

Note: Querier messages are generated from interfaces that are ip pim enabled.

```
interface fortyGigE X/Y/Z
  ip pim sparse-mode
  exit
```

```
interface vlan X
  ip pim sparse-mode
  exit
```

7. Enable the IPv4 multicast address family on each BGP ASN

```
router bgp ASN
  address-family ipv4 multicast
  neighbor peer-group-name activate
  exit-address-family
  exit
```

5.4 Automatic port configuration

Dell EMC Networking N-Series switches have the capability to automatically configure port interfaces through a combination of Python scripting and CLI macro support. Organizations can dramatically reduce deployment time of cameras and other devices by enabling automatic port configuration.

Dell EMC Networking has published a paper providing detailed instructions on how to use Python scripting and CLI macros to customize automatic port configuration behavior. This document can be accessed by the following link: [Automatic Port Configuration for Dell EMC Networking N-Series Switches](#).

This section summarizes the features and steps needed to use automatic port configuration.

5.4.1 Device identification with Link Layer Discovery Protocol (LLDP)

Python scripts use device identification information to determine the device type and model in order to execute the proper commands predetermined by network administrators. The networking feature used to identify the device is LLDP.

LLDP is a layer 2, industry standard protocol used by network devices to identify themselves and their capabilities to neighboring devices on the network. Identifying information must be obtained through LLDP in order for the Auto Port Profile script to work. Any number of fields resulting from a `show lldp` command may be used to identify devices. It is up to the Python script developer to determine which field(s) are best used for their purpose. The following list shows some of the standard LLDP fields that may be used:

- Model Name
- Media Policy Application Type
- System Name
- System Description
- System Capabilities Supported
- System Capabilities Enabled

5.4.1.1 LLDP switch configuration

LLDP is enabled by default on N-Series switches. No configuration is required and the settings to modify intervals, timers, and other options do not need modification in most cases.

To identify LLDP information provided by a camera on an interface, use the following command:

```
show lldp remote-device detail gigabitethernet x/y/z
```

5.4.1.2 CLI macros

The Python scripts that perform the automatic port configuration include CLI macros. CLI macros may have up to three variables replaced by values provided from a parameters (.prm) file upon application of the macro. Macros can be applied to specific interfaces, a range of interfaces, or the global configuration.

Dell EMC recommends selecting and testing the CLI macros required for the job prior to automating and implementing on a large scale.

There are two types of macros:

- Built-In: predefined macros available in the switch OS, which cannot be changed or deleted.
- Custom: user-defined macros, which allow the operator to bundle multiple built-in macros and/or add-remove commands as desired. Up to 50 user-defined macros are supported.

5.4.1.3 Python scripts

The Auto Port Profile scripting tool uses the CLI macros along with the switch's Python capabilities (polling, parsing, etc.) to automate port configurations. Link Layer Discovery Protocol (LLDP) packet information entering the switch is used to identify the type of device being connected to the switch in order to apply an applicable switch configuration to the corresponding interface.

A Python script file (with .py extension) and associated parameter file (with .prm extension) are used to enable the Auto Port Profile capability.

The Python script contains all of the instructions to properly configure the switch upon connection of the camera device. The following list shows the main components and functionality of the Python script:

- Initiates variable
- Open session for switch administration
- Obtain LLDP information
- Read parameters from .prm file
- Read device capabilities
- Identify device
- Apply CLI macros
- Log and display error messages

5.4.1.4 Installing and executing python scripts

After developing the parameter and python script files, the files are loaded onto the switch and installed.

Use the following steps to copy and install the .prm and .py files.

1. Gzip and tarball the python (.py) app file with a .tgz or .tar.gz extension.

Note: Permissions are required to be set on the application file prior to packaging. Application file names can be up to 15 characters.

2. Copy the parameter (.prm) to the switch (tftp method shown).

```
Dell#copy tftp://<ipaddress>/filepath/prmfilename.prm application  
prmfilename.prm
```

3. Copy the application file to the switch.

```
Dell#copy tftp://<ipaddress>/filepath/appfilename.tgz application  
appfilename.tgz
```

4. Install the application.

```
Dell#application install appfilename.py auto-restart
```

5. Execute the Python script.

```
Dell#application start appfilename.py
```

6. Verify that the application process is running.

```
Dell#show process app-resources-list
```

Note: Be sure to save the running-configuration to the startup-configuration if the script needs to run after a switch reload.

For a detailed CLI macro and Python script example with troubleshooting and best practices, see [Automatic Port Configuration for Dell EMC Networking N-Series Switches](#).

6 Power over Ethernet

Power over Ethernet (PoE) is a technology that allows Ethernet cables to provide electrical power to devices such as cameras. Dell EMC Networking offers many PoE enabled models and can be identified by the model name ending in a letter "P".

6.1 PoE features

Dell EMC Networking switches provide several configuration features to help manage device behavior and the overall power budget of the switch. This section provides some information on options available to the network administrator.

6.1.1 PoE, PoE+, PoE 60W

There are three PoE standards that Dell EMC Networking switches support. The following list shows the common name, standard or type, and power supplied to each PoE port:

- PoE, 802.3af, 15.4 watts
- PoE+, 802.3at, 30.0 to 34.2 watts
- PoE 60W, 4-pair, 60.0 watts

All Dell EMC Networking PoE switch models support PoE and PoE+ capability. PoE 60W is supported on a select number of N2000 and N3000 series models. Power requirements for the types of cameras and operating conditions should be taken into account when choosing the switch model to deploy.

6.1.2 Dell EMC Networking OS6 PoE features

The N-Series line of switches running OS6 provides several features to manage PoE behavior and control the PoE budget of the switch.

Note: Power management mode is controlled at the switch level and not at the port level.

6.1.2.1 Static power management

Static power management reserves the full power of a configured port. This type of power management is useful if device operation is critical, and cannot afford a reduction or loss of power once configured.

The switch may not be able to source enough power for all ports at maximum configurable power. The simple equation below can be used to determine the amount of available power remaining after configuring ports for PoE.

Available Power = Power Limit of the Power Supply Sources - Total Configured Power

Total Configured Power can be determined by adding the maximum power for each port based on the PoE mode configured. In two-pair mode, the port reserves 32W, and in four-pair mode it reserves 60W. Administrators can optionally configure an explicit upper limit.

6.1.2.2 Dynamic power management

Dynamic Power management uses class signatures that are detected from the device. It allocates power based on the class but does not reserve that power.

Available Power = Power Limit of the Power Supply Sources - Total Allocated Power

Allocation in this case is the total power consumed by the device. The device can draw power up to an additional 5% above the class detected.

6.1.2.3 Class-based power management

Class-based power management allocates power based on the detected powered device signature and LLDP-MED. The switch allows the device to draw power up to the maximum limit of the class signature. Although the power draw limit is based on the class signature, the switch reserves power for the port at a fixed 33W. This behavior may not be suitable for devices that draw power consistently below 33W.

Note: Class-based power management is not recommended in most use cases. The reservation of power above the class may cause the total power budget of the switch to be exceeded. When the total power budget is exceeded, the switch will disable power to the port with the least configured priority.

6.1.3 Dell EMC Networking OS9 PoE features

The S-Series line of switches running OS9 provides several features to manage PoE behavior and control the PoE budget of the switch.

6.1.3.1 Power priority algorithm

The Dell Networking OS9 uses a port priority algorithm to determine which ports receive power based on the inline power available. The power inline mode or prioritization is configured at the port interface. The priority list below contains the parameters used in the priority algorithm:

- Power inline mode: class or static
- Power inline priority configuration
- LLDP-MED priority
- Slot and port number

When static mode is used, the inline power is allocated based on the actual power consumed by the device. Class mode allocates the maximum power for the class of device connected. The power inline modes are global commands, and total inline power remaining should be carefully calculated when designing and deploying the network.

6.1.4 Dell EMC Networking OS3 PoE features

The X-Series line of switches running OS3 utilizes a simple PoE management structure.

Available Power = Power Limit of the Power Supply Sources - Total Power Consumed

Dell EMC Networking OS3 provides the administrator with three levels of priority (Critical, High, and Low), to manage which devices receive power. When inline power reaches the limit of the power supply, the lowest priority devices configured by port will be denied power.

6.2 PoE budget planning methodology

This section provides some universal guidance to assist in the planning and procurement of PoE switches. By following these recommendations, administrators can plan for the maximum amount of devices per switch and their uptime.

1. Determine the number of devices physically located within the cable length limits of the switch.

Note: Maximum allowed cable length is 100 meters for a standard cat5e or cat6 cable. Some devices may be more susceptible to the voltage drop incurred by long cable runs. See your device voltage specifications.

2. Determine the number of ports needed for PoE cameras and other PoE devices such as wireless access points.
3. Calculate the maximum power required for all PoE devices.
4. Determine if the switch and its connected devices need redundant power supplies for reliability and critical uptime.
5. Determine if any PoE devices have low priority and can be powered off in the event of a power supply failure.
 - a. If the answer is yes, the redundant power supply's available power can increase the number of supported PoE devices on a switch, when both power supplies are available. The power management mode can also be set to allow for high priority devices to always receive power due to increased power usage.
 - b. If the answer is no, the redundant power supply's available power should only be used for the purpose of redundancy. The power management mode should be set to reserve power based on the device maximum power requirements.
6. Many switch models have several power supply options. Choose the switch that has the required available power options needed for your deployment.
7. Determine the features and other specifications required for your devices and network. Each switch model and OS type has its own set of features and specifications.

Note: PoE 60W is not supported on all switch models. Features such as stacking, L2/L3 capabilities, and port data rates can vary.

6.2.1 PoE budget example

This section will describe a simple exercise in determining the switch model options available for deployment. This example only provides information in reference to PoE functionality, it does not consider cost or other networking features.

When evaluating the building layout and surveillance, it is determined that a wiring closet in one part of the building needs to support the devices in the list below.

PoE device list:

- 16qty standard surveillance cameras
 - PoE+, maximum 30W, average 15W
- 4qty outdoor surveillance cameras
 - 60W PoE, maximum 60W, average 40W
- 3qty Wireless Access Points (APs)
 - PoE+, maximum 30W, average 20W

Total power required:

- Standard surveillance cameras
 - Max: (16qty) x (30W) = 480W
 - Average: (16qty) x (15W) = 240W
- Outdoor surveillance cameras
 - Max: (4qty) x (60W) = 240W
 - Average: (4qty) x (40W) = 160W
- Wireless Access Points (APs)
 - Max: (3qty) x (30W) = 90W
 - Average: (3qty) x (20W) = 60W

Maximum power total: 810W

Average power total: 460W

Total number of ports: 23

Dell EMC Networking switch models possible candidates:

- N2128PX-ON
 - 1000W internal PSU, 1000W optional external PSU
 - > **Inline power budget 800W (1qty PSU), 1600W (2qty PSU)**
- N3024P
 - 715W internal PSU, 715W optional internal PSU
 - > **Inline power budget 550W (1qty PSU), 1100W (2qty PSU)**
 - 1100W internal PSU, 1100W optional internal PSU
 - > **Inline power budget 950W (1qty PSU), 1900W (2qty PSU)**
- N3048P
 - 1100W internal PSU, 1100W optional internal PSU
 - > **Inline power budget 950W (1qty PSU), 1900W (2qty PSU)**
- N3132PX-ON
 - 1100W internal PSU, 1100W optional internal PSU
 - > **Inline power budget 750W (1qty PSU), 1700W (2qty PSU)**

Switch model choice summary:

N2128PX-ON

The base N2128PX-ON can supply power to all devices in this example when each device is operating at its average power consumption. A single PSU could not guarantee all devices would receive power if the devices operated at maximum power. Adding the optional external PSU would allow for guaranteed PoE device operation when both PSUs are operational. The administrator can choose to assign a lower priority to at least one device to ensure a critical device is not shutdown in the event of a single PSU failure.

N3024P

The base N3024P (715W PSU) can supply power to all devices in this example when each device is operating at its average power consumption. A single PSU could not guarantee all devices would receive power if the devices operated at maximum power. Adding the optional PSU would allow for guaranteed PoE device operation when both PSUs are operational. The administrator can choose to assign a lower priority to several devices to ensure a critical device is not shutdown in the event of a single PSU failure.

If the customer orders the N3024P with the 1100W PSU, all devices could be guaranteed to operate throughout their power consumption limits. Additionally, if a second 1100W power supply is added, full redundancy in addition to inline power to all PoE ports is guaranteed.

This device only has 24qty 1GbE ports. In this example, the switch would be almost fully populated and have little room for future growth.

N3048P

The base N3048P can supply power to all devices in this example throughout their power consumption limits. Additionally, if a second 1100W power supply is added, full redundancy in addition to inline power to all PoE ports is guaranteed.

N3132PX-ON

The base N3132PX-ON can supply power to all devices in this example when each device is operating at its average power consumption. A single PSU could not guarantee all devices would receive power if the devices operated at maximum power. However, if a second 1100W power supply is added, full redundancy in addition to inline power to all PoE ports is guaranteed.

PoE budget example summary:

Although not shown above, there are several more models of PoE switches offered by Dell EMC Networking. These models were not candidates in this example due to the absence of support for 60W PoE. Those models from the X-Series and S-Series could be candidates for deployments only requiring PoE+ or PoE.

Each switch candidate above can provide inline power to all devices in the example. If the administrator determines all devices are critical and requires guaranteed operation with redundancy, then the number of model options is less. In addition to PoE, administrators should also look at other features supported by the switch model. For example, only two switch models above support 2.5/5GbE data rates.

This example is for a single wiring cabinet in a limited area of one building. If the switch and surveillance deployment includes many buildings or a very large area, simply adding ports and power supply limits is not sufficient. Most PoE devices rely on cat5e or cat6 cables which have a limitation on operational cable length. A careful study of switch location and serviceable device locations must also be taken into account.

7 Networking features for topologies

This section highlights networking features used in specific topologies and deployments. Many networking features can be used regardless of the size or purpose of the networking deployment. Other features are designed specifically for the topologies type and end use of the network. The next sections will identify several networking features and how they are best used in each topology.

7.1 Virtual Link Trunking

Virtual Link Trunking (VLT) is a networking feature that allows two Dell EMC switches to appear as a single switch from the perspective of devices outside the VLT domain. The main benefit of this technology is the ability to use the full bandwidth capacity of two switches while providing redundancy. Full bandwidth capacity is realized by the ability of the two switches to eliminate spanning tree (STP) blocked ports.

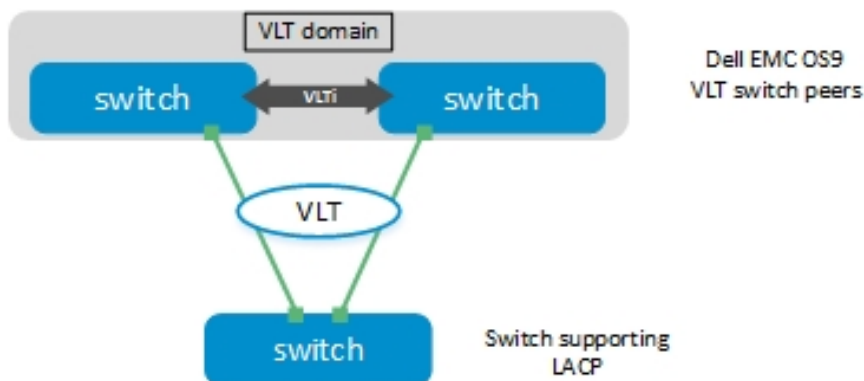


Figure 18 Dell EMC switch running OS9 in a VLT configuration

VLT benefits summary:

- High availability
- Active-Active load sharing with VRRP and L3 VLAN peer routing
- Fast convergence for link or device failure
- Loop-free topology, eliminates STP blocked ports
- Full uplink bandwidth utilization

VLT can be used with any topology utilizing Dell EMC switches running OS 9.

The following topologies shown in section 3.1 utilize pairs of switches configured as VLT peers:

[Dedicated full mesh network](#)

[Distributed ring network](#)

[Converged full mesh network](#)

7.2 Force10 Resilient Ring Protocol

Force10 Resilient Ring Protocol (FRRP) is a layer 2 networking feature used to create ring topologies with fast convergence without the use of STP. FRRP provides protection against single link or switch failure. Combined with redundancy through VLT, ring topologies can provide greater network uptime.

FRRP is best utilized in deployments that include a campus or municipality with distributed buildings. Cabling costs can prohibit a full mesh network and FRRP can provide superior connectivity when compared to traditional public WAN solutions.

FRRP functions through the use of a single master node and multiple transit nodes. Each node (switch) is monitored by the master node to ensure the health of the ring. In the event of a link or switch failure, the master node sends out topology change information to the transit nodes. After the forwarding tables are flushed, the network converges on the new topology.

FRRP benefits summary:

- No limit to number of nodes on a ring
- Multiple physical rings on same switch allowed
- Up to 255 rings in a system
- Fast convergence time, 150ms to 1500ms
- Single switch or link failure protection
- Compatible with VLT

FRRP can be used with any topology utilizing Dell EMC switches running OS 9.

The following topologies shown in section 3.1 utilize FRRP:

[Distributed ring network](#)

7.3 Virtual Routing and Forwarding

Virtual Routing and Forwarding (VRF) is a layer 3 networking feature that allows a single router to partition itself into multiple virtual routers (VR). With VRF, multiple routing tables exist within the same router. Traffic within each VR is isolated, each with a separate control and data plane. VRF is conceptually similar to a layer 2 switch and its use of VLANs.

VRF is essential in many multi-vendor or multi-tenant environments, but it can also be used within a single organization. VRF can be used to separate the sensitive surveillance and security traffic from the standard employee or user traffic in a converged network. Network security administrators may require separation through VRF to comply with local government laws or organizational policies.

VRF benefits summary:

- Security – Isolated control and data plane for each VR
- Cost – Reduce number of layer 3 switches compared to physically separate network
- Compliance – Conform to security policies and directives

VRF can be used with any topology utilizing Dell EMC switches running OS 9.

The following topologies shown in section 3.1 can utilize VRF:

[Converged full mesh network](#)

7.4 VLAN routing for X-Series switches

X-Series switches supported by Dell Networking OS 3, support layer 2+ static routing. The X1052/P and X4012 support layer 2+ from the factory; while the X1008/P, X1018/P, and X1026/P must be placed into layer 2+ mode manually.

The capability of X-Series switches layer 2+ feature set allows SMB organizations to separate and secure surveillance traffic from normal business traffic in a cost effective way.

X-Series layer 2+ summary:

- Static routes can be configured for addresses not on a directly connected network
- Next hop determined according to longest prefix match
- Metric values from 1 to 255
- Default route assigned on in-band interfaces statically or by a DHCP server
- UDP Relay feature for specific UDP broadcasts between IP subnets

Layer 2+ static routing can be used with any topology utilizing Dell EMC X-Series switches.

The following topologies shown in section 3.1 include X-Series switches:

[Small scale traditional network for SMB](#)

A Validated hardware and components

The following table lists the hardware and components used to configure and validate the example configurations in this guide.

Item	OS/Firmware version
S31424-ON	DNOS 9.13.0.0
N3132PX-ON	DNOS 6.5.0.2
X1052P	DNOS 3.0.0.95

B Technical support and resources

[Dell.com/support](https://dell.com/support) is focused on meeting customer 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.

[Networking Technical Documents](#) on Dell TechCenter provide expertise that helps to ensure customer success on Dell EMC Networking platforms.

[Storage Solutions Technical Documents](#) on Dell TechCenter provide expertise that helps to ensure customer success on Dell EMC Storage platforms.

B.1 Related resources

[*Dell EMC Surveillance Networking Reference Architecture*](#)

[*Dell EMC Surveillance Implementation Guide*](#)

[*Automatic Port Configuration for Dell EMC Networking N-Series Switches*](#)

[*Dell Networking Campus Switching and Mobility Reference Architecture 3.0*](#)

[*Leaf-Spine Deployment and Best Practices Guide*](#)

B.2 Feedback

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