Surveillance
Dell EMC Surveillance Networking

Reference Architecture

H16965

Dell EMC
Surveillance Lab
Validated

DELL EMC

Published March 2018

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

CHAPTER 1

Overview

This document provides an architectural overview of the Dell EMC™ surveillance solutions enabled by Dell EMC storage platforms, Dell EMC Networking, VMware™, RSA™, and other Dell™ family products.

Solution purpose

This reference architecture is intended to provide a high level architectural considerations for designing effective surveillance networks. This paper focuses on resilient network architectures although simple, non-redundant architectures could also be used.

From the moment the initial information is captured and throughout the initial response, increased asset protection and conviction rates can be observed when using integrated Dell EMC, VMware, and RSA™ solutions.

Dell EMC Networking provides a number of network architectures including campus topologies for small to mid-sized implementations, leaf-spine implementation for maximum resilience and scale, and ring topologies.

Business challenge

Private businesses and public entities generally respond to the rising concerns about theft, fraud, and terrorism by sharpening their focus on physical security and surveillance systems. Organizations such as retailers, casinos, financial institutions, higher education institutions, transportation companies, law enforcement, school systems, prison systems, and government agencies all need to manage and protect their ever-growing volume of physical security information.

The ability to access the right data at the right time from anywhere is crucial to supporting physical security and surveillance needs. However, the following factors can hinder achieving a comprehensive solution:

- Proprietary software
- Closed hardware platforms
- Lack of manageable archival capabilities
- Data-retrieval wait times
- Lost data
- Unproven content authenticity
- Information management limitations
- Networking issues

Amplifying these limitations are the high expansion costs of legacy video surveillance systems, which are based on closed-circuit television (CCTV), digital video recorders (DVRs), or network video recorder (NVR) technologies and non-integrated IT and physical security systems.

Terminology

Layer 2 switch

Layer 2 switching works at Layer 2 of the OSI model and is often equated as a broadcast domain.

Layer 3 switch

Layer 3 switching works at Layer 3 of the OSI mode. A Layer 3 switch intelligently routes traffic between multiple Layer 2 and other Layer 3 networks. The Layer 3 function only forwards meaningful data to the next network that is appropriate

for the traffic. The routing function (Layer 3) defines the scope of a broadcast domain by not forwarding broadcast messages.

Routed protocols

A routed protocol carries usable (payload) traffic, for example SMB, CIFS, and iSCSI.

Routing protocols

These protocols are used by Layer 3 switches and router for determining the next hop traffic must follow, such as Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and Intermediate System to Intermediate System (IS-IS).

VLT

Virtual link trucking (VLT) is a layer-2 link aggregation protocol between end-devices, such as servers, that are connected to different access-switches. This protocol offers servers and edge switches a redundant, load-balancing connection to the core-network in a loop-free environment eliminating the requirement to use a spanning-tree protocol.

VLT Domain

A VLT Domain consists of a pair of VLT coupled switches.

PoE

Power over Ethernet (PoE) describes a standard or ad-hoc system which passes electric power along with data on twisted pair Ethernet cabling.

NSX

VMware NSX™ is the network virtualization platform for the Software-Defined Data Center (SDDC).

FRRP

Force10 Resilient Ring Protocol (FRRP) provides fast network convergence to Layer 2 switches interconnected in a ring topology. This is ideal in a metropolitan area network (MAN) encompassing small to large campuses.

VRRP

Virtual Router Redundancy Protocol (VRRP) provides an automatic gateway IP path selection. This ability allows the IP gateway path to be automatically selected to increase availability and reliability of the cameras' or end stations' connectivity.

CHAPTER 2

Key Components

Incumbent physical security systems initially consisted of legacy analog monitoring capabilities and analog cameras. Advancements in surveillance technology sparked an exodus from analog video to state-of-the-art digital IP cameras. Video encoders were developed to convert standard NTSC/PAL video from coax-attached analog cameras to a digital video stream over TCP/IP accelerating this transition and providing investment protection.

The Dell EMC surveillance solution focuses on IP cameras, which are supplied by the customer or integrator. The IP cameras connect to a surveillance specific IP network or an enterprise IP network. Video recording engines collect, analyze, and store the video with associated metadata to enterprise class storage. This reference architecture references Dell EMC storage platforms, PowerEdge Servers, Dell EMC Networking, and other Dell products providing a single-tiered or multitiered storage architectures for centralized or decentralized enterprise requirements.

Technology solution

Dell EMC Surveillance Labs create proven solutions. These validated solutions provide a tested infrastructure for the flexibility to control video surveillance and analyze security incidents in real time, collect evidence faster, and easily review archived data from anywhere.

Dell EMC storage arrays provide quality storage for the smallest to the largest customers by using a variety of storage topologies including SAN (FC and iSCSI) and NAS (NFS and CIFS).

Dell EMC Networking designs switches that meet requirements from a small office, home office (SOHO) deployment to enterprise scale data centers. Adding the leading Dell EMC PowerEdge servers to this network ensures a successful implementation.

Virtualization with VMware consolidates the number of Surveillance servers that are required at a particular site. Aggregating multiple virtualized Surveillance servers onto VMware ESX/ESXi hosts enables more bandwidth per physical host than is normally available from a physical host.

The Dell EMC Surveillance Lab primarily uses VMware ESXi, Dell EMC storage arrays, Dell EMC servers and Dell EMC Networking. The lab therefore provides tested architectures and solutions that are optimized for various implementation tiers.

Network

Surveillance is an end-to-end solution that is connected using a simplistic to complex network infrastructure. A typical solution spans multiple network layers, ranging from the access layer providing power over Ethernet (PoE) for video cameras, to the data center that provides the centralized network that is used to interconnect all of the surveillance components.

With cameras on the edge, the data center infrastructure is made of aggregation switches that are known as leaf switches, and a core switch, which is known as the spine. A small campus network has an aggregation layer, but not a data center or core. The network must be correctly sized in terms of capacity, efficiency, and resilience to effectively resolve the user's business challenges.

Dell EMC PowerEdge servers

Dell EMC PowerEdge™ servers are ideal for recording and managing terabytes of video from distributed locations.

PowerEdge 1U servers are used where external NAS clusters or block arrays are planned for surveillance storage.

PowerEdge 2U rack servers are used for local video storage where external surveillance storage will not be used.

Dell EMC storage

This reference architecture uses Dell EMC Untiy, Dell EMC SC, Dell EMC ECS, and Dell EMC Isilon storage platforms. However, you can integrate different Dell EMC storage platforms and array sizes with VMS to provide a physical security solution to meet the requirements of any size application.

CHAPTER 3

Surveillance physical architecture

A video surveillance network architecture can span multiple networks to move distributed surveillance camera video from edge switches through a central switching infrastructure to distributed servers and storage.

There are multiple design considerations for a surveillance network: campus, distributed ring, and data center. A campus network is based on an aggregation layer. The distributed ring topology interconnects campus networks. The data center converges video surveillance and data center traffic into a low latency resilient network.

Dell EMC Surveillance Lab test environment

The Dell EMC Surveillance Lab has been in existence for over a decade. Focusing on determining how different video management software (VMS) implementations operate on various Dell EMC platforms, we test the various VMS under failing or failed conditions. Products that are tested in the lab include Dell EMC storage, PowerEdge servers, and Dell EMC Networking components, as well as many Dell offerings, such as VMware and RSA.

To adequately evaluate how Dell EMC Networking switches operate in a surveillance network, the day-to-day high-volume test traffic was added by moving from the legacy Layer 2 network to the Layer 3 network based on Dell EMC Networking switches. This move allows the networking test traffic to include the Dell EMC production testing activities, allowing dual purpose testing for day to day sizing test and high volume validation tests.

The design of the network encompasses various specific architectures that are discussed in this reference architecture. The basic hierarchical architecture is both a standalone architecture as well as the primary building block for the other two architectures. An unintentional benefit of building the network in the Surveillance Lab is the ability to show that the various architectures can be integrated to allow maximum flexibility meeting the needs of any surveillance implementation.

The Dell EMC Surveillance Lab focuses on technologies that provide zero packet loss. Therefore, the goal of our network tests is based on maintaining zero packet loss.

Three network architectures were studied:

- Large campus: standalone surveillance and converged surveillance
- Highly distributed surveillance using ring architecture
- Data center leaf-spine architecture

Dell EMC Surveillance Lab switches

PoE - Access Layer

Typically the camera network starts where each camera can be connected to a port on a power over Ethernet (PoE) switch. PoE reduces the cost associated with installing cameras because the switch eliminates the need to provide an independent power source to each camera position.

- S3100 Series
- N3000 Series
- N1500 Series
- N2000 Series
- N1100 Series

Aggregation

- S4048-ON

Core

- Z9100-ON

Basic hierarchical architecture

The basic hierarchical architecture could be perceived as an augmented star architecture which is ideally suited for small to large scale surveillance deployments.

Although the architecture can be used for smaller implementations and will gain in terms of reliability, the architecture is best suited for large implementations.

Features

- Well suited for video surveillance
- Ideal for buildings, airport terminals, and campus buildings
- Accommodates a large number of cameras per deployment
- Serves as the basis of a leaf-spine data center architecture or the site/building construct in an FRRP ring network

Building a campus network

- Install two switches that are interconnected into a VLT domain for each building in a campus
- The edge switches connect to each switch in the VLT domain
- Use virtual router redundancy protocol (VRRP) to establish a gateway for each VLAN
- Connect servers to both switches using teamed NICs

Resilience

Surveillance networks require a resilient solution. Unfortunately, not every component can be fully redundant unless pairs of components are deployed.

- A camera and an edge switch are considered single points of failure
- The aggregation switches in a VLT configuration provide redundancy
- VRRP is so the IP gateway path is automatically selected

This deployment is required to create a network that is as resilient as possible. If a core switch is taken offline, the remaining switch continues to handle the surveillance traffic. A resilient network is required in any high risk or 24x7 implementation.

This deployment is required to create a network that is as resilient as possible. Redundancy using VLT provides failure protection at the switch and the link level. In this design, if any aggregation switch (S4048) or core switch (Z9100) goes offline, traffic still continues. Also, if any one link or combination of links goes down, traffic still continues. A resilient network is required in any high risk or 24x7 implementation.

Virtual Link Trucking (VLT)

VLT is implemented in switch pairs and configured to form a VLT Domain. From an overall network view, the VLT domain appears to be a single switch. The VLT domain is key to implementing resilient surveillance networks.

VLT reduces the role of spanning tree protocols (STPs) by allowing link aggregation group (LAG) terminations on two separate distribution or core switches and supporting a loop-free topology.

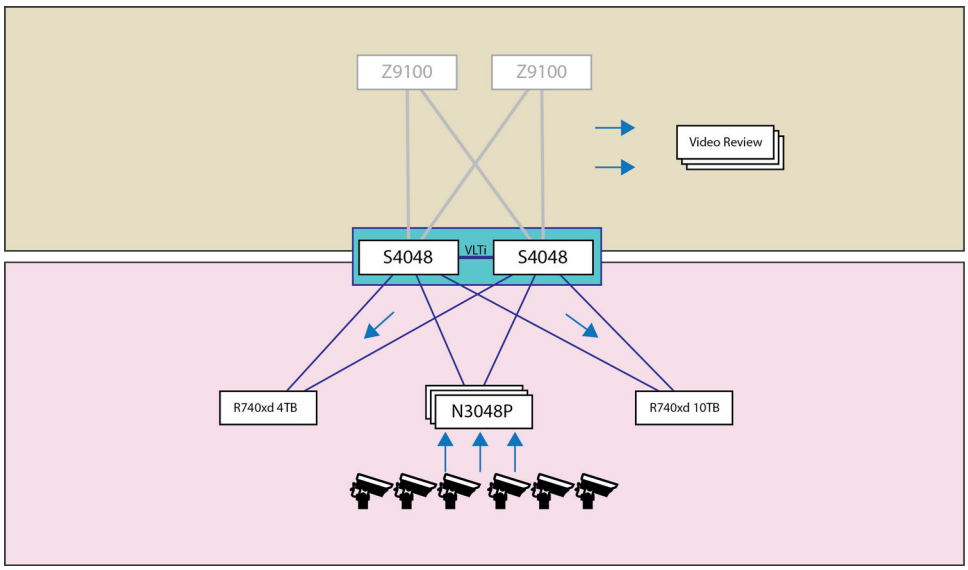
To prevent the initial loop that may occur prior to VLT being established, use a spanning tree protocol. After VLT is established, you may use rapid spanning tree protocol (RSTP) to prevent loops from forming with new links that are incorrectly connected and outside the VLT domain.

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

Virtual link trunking offers the following benefits:

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

Figure 1 Star network architecture



The cameras are connected directly to the Dell EMC Networking switches. The cameras initially send unicast or multicast video through the switch to which they are directly connected. The video then flows through the VLT domain pair to the dual attached (teamed) NICs on the server. Redundancy using VLT provides failure protection at the switch and the link level.

Ring architecture

The Force10 Resilient Ring Protocol (FRRP) allows sites to be interconnected with a minimum number of point-to-point (PTP) links. The weak link in any network with extended network cables is the network cables themselves. The ring topology recovers from failures much faster than other similar topologies.

Features

- Large and highly distributed surveillance deployments such as in city surveillance or school district surveillance implementations.
- Thousands of cameras can be supported per ring.

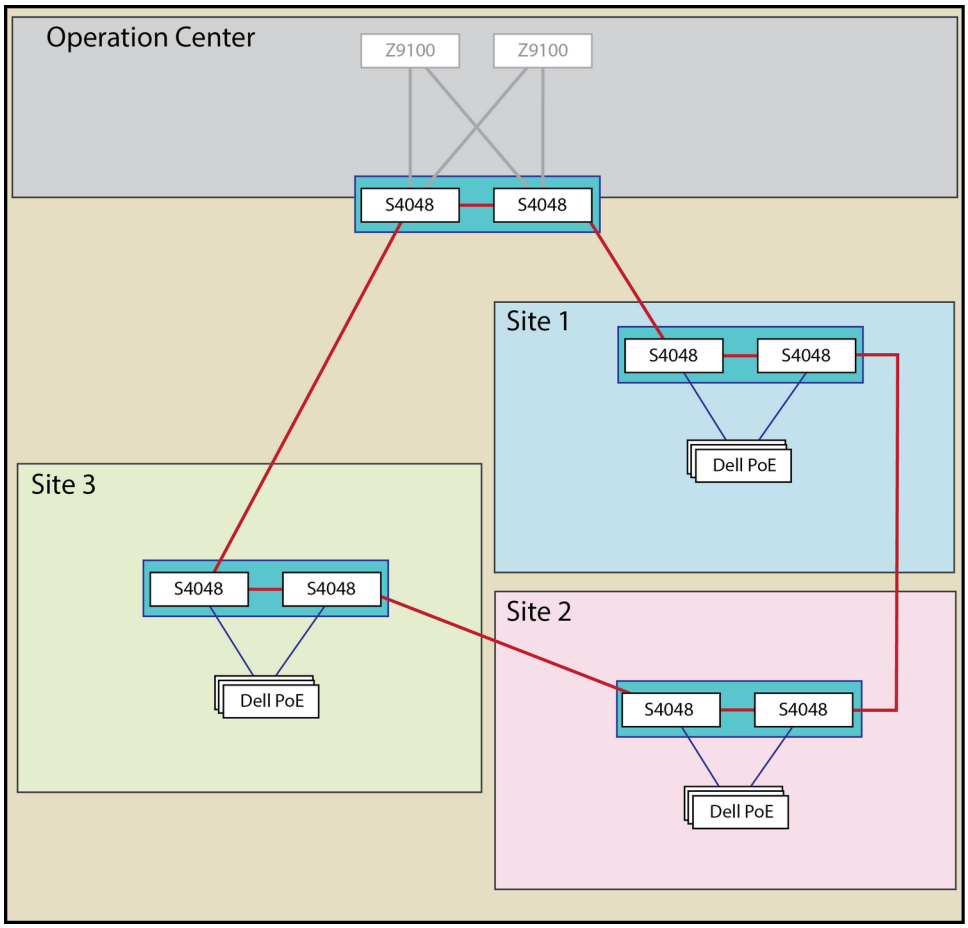
Building an FRRP ring

- Each site is constructed as basic hierarchical network
- The aggregation switches which make the VLT domain are interconnected with a single port channel from each switch to an adjacent site
- Member VLANs are overlaid for video traffic

FRRP is a Layer 2 topology that is built as a Ring where one node is connected to its adjacent node until a ring is formed. Multiple rings can be created and each switch (or VLT domain) may be in one to 255 rings. Each FRRP ring can use a single VLAN for all video traffic, use multiple VLANS, and can isolate VLANs between nodes.

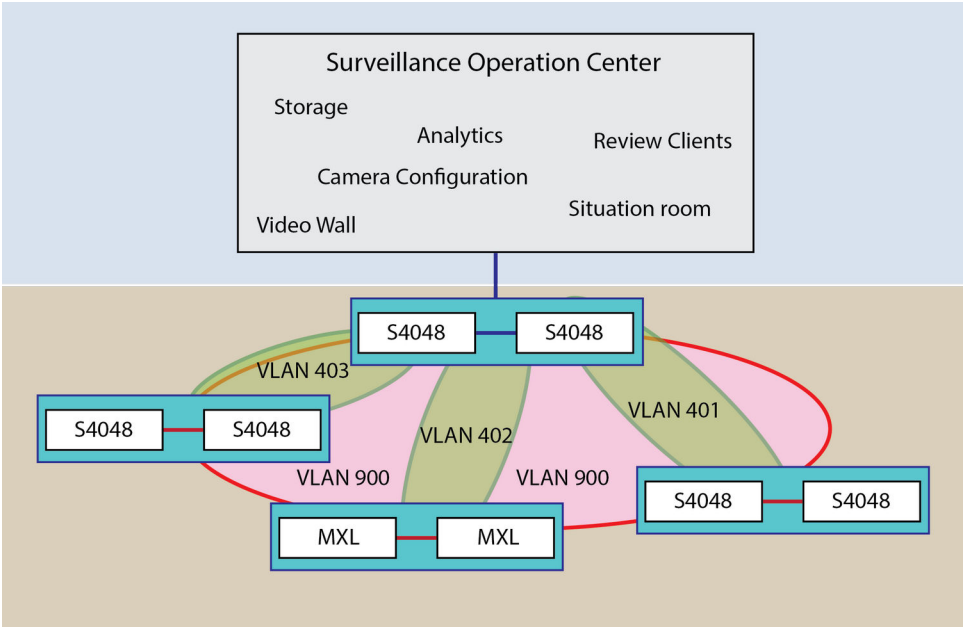
In the following illustration, the red line creates a ring of S4048 nodes.

Figure 2 FRRP network architecture for large distributions



This topology is ideal for implementations such as a college campus, government complex, or airport. Each site is constructed using the basic hierarchical network. It is very important to understand where the video is stored. The bandwidth concerns are greatly different if the video is stored local to each basic hierarchical network or if the video is stored in the centrally located Operation Center.

Figure 3 FRRP network architecture for interconnecting star topologies



The FRRP is very flexible. VLANs can encompass all nodes in the ring or can be configured between select nodes. An interesting application for surveillance is to bring extended VLANs from the edge sites to the central site on a per site bases. This application allows the people in the surveillance operation center to configure new cameras when camera configuration tools operate at Layer 2 while restricting the size of the broadcast domain. This could reduce the expertise required when replacing failed cameras or installing new cameras.

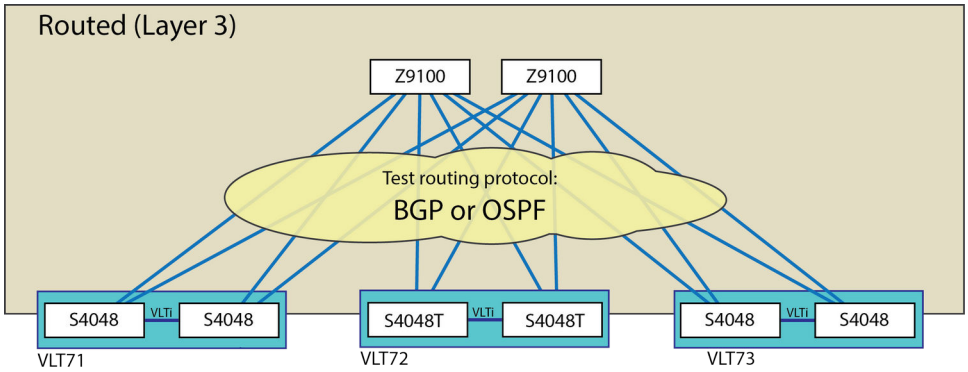
Data center architecture

Dell EMC Networking is extremely formidable in terms of capability and performance. In many instances, the required network for surveillance is converged with the network for the data center. This design achieves minimum latency with maximum resilience while providing maximum scaling. In this architecture, quality of service (QoS) might be required to ensure surveillance traffic delivery. For increased security of video traffic, virtual routing and forwarding (VRF) can be used.

Features

- Large camera deployment scalable to thousands of cameras
- Integrated video surveillance traffic and data traffic in a data center, or IT maintained network
- Minimized hops and latency between endpoints (East-West traffic)

Figure 4 Data center network architecture



The VLT Domain incorporates two switches for maximum resilience. The VLT domain creates a single data plane where each switch is an independent control plane, which essentially creates a single logical switch. This design has many advantages, such as eliminating network issues from loop avoidance protocols such as STP. Another technique that can augment resilience is to use VRRP for automatic gateway path selection.

Layer 3 switching, also referred to as Routing, occurs between each leaf switch and the spine switches. The use of Layer 3 eliminates broadcasts through the core network thereby improving scalability and resilience.

Building a data center network

- Top-of-rack or end-of-row switching uses the basic hierarchical architecture. The aggregation switch in this case is called the leaf. Each leaf is a VLT domain.
- An independent pair of core switches forms the spine of the network.
- Layer 3 switching is used between each leaf and the spine
- BGP is the preferred routing protocol although OSPF or IS-IS could be used

Each leaf in the core network is constructed using the basic hierarchical architecture built on a VLT domain. The VLT domain creates a single data plane with each switch being an independent control plan, basically creating single logical switch. BGP is used as the routing protocol because it quickly converges when required. Therefore, the slow and sometimes inaccurate spanning tree convergence combines with the quick re-routing provided by BGP to create a highly resilient network.

Multicast

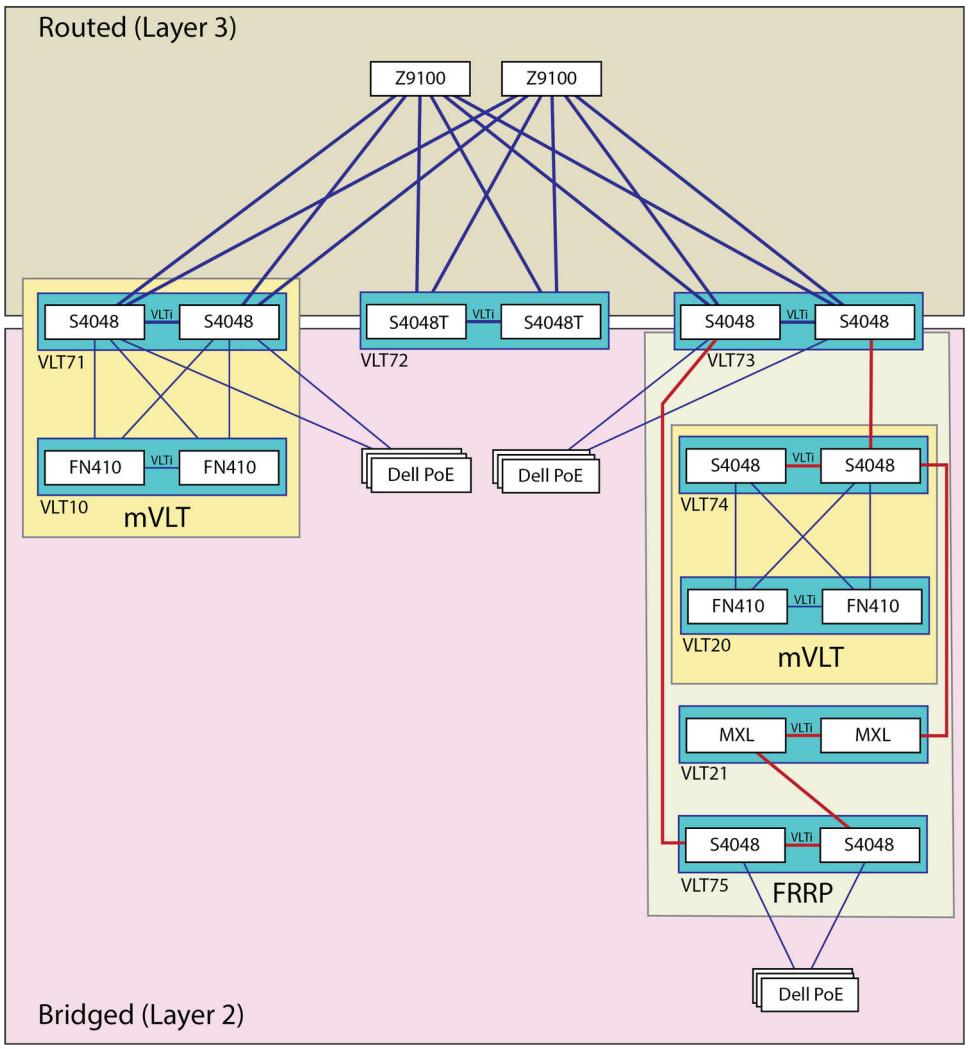
Multicast must be planned into the network. Ideally the Rendezvous-Point (RP) is defined towards the network's center. In the converged leaf-spine network, the RP was defined on one of the spine switches with the second spine switch defined as the candidate RP.

There is no need for multicast to be defined to all the VLANs. Only enable protocol-independent multicast (PIM) on the VLANs that require multicast traffic. The VLANs with the highest potential for multicast traffic are server VLANs and camera VLANs.

Dell EMC Surveillance Lab network design

The diagram depicts a subset of the overall network deployed in the surveillance lab. This design shows a more complex, and integrated architecture. All the architectures discussed are included as well as expansions to those architectures.

Figure 5 Dell EMC Surveillance Lab network design



VLT domain 71 and VLT domain 72 illustrate the data center architecture with a full leaf-spine architecture that includes edge PoE switches. Also included is an FX2 modular system with modular servers and storage.

Any 10G-BaseT or 1G-BaseT (CAT6) devices not on the edge are connected to VLT domain 72. For the duration of these tests, SCv3000 storage and 1GbE attached PowerEdge servers were attached.

A star topology is implemented with VLT domain 73. Video surveillance recording servers, Dell EMC iSCSI, and SMB storage are attached directly to VLT 73. To maximize resilience, servers are attached directly to each switch of the VLT domain using teamed NICs.

The FRRP ring also uses VLT domain 73 as its route into the converged network. As illustrated previously, each VLT domain in the FRRP represents a building in a metropolitan area network (MAN) or multi building complex.

This drawing also introduces the concept of a multiple VLT (mVLT) architecture. This is a highly resilient architecture that is often used to connect modular systems, such as the PowerEdge FX2 or PowerEdge M1000e, to a VLT domain.

PoE switches are loaded with PoE cameras. To load more traffic onto the power over Ethernet (PoE) switch, video simulators were used.

CHAPTER 4

Conclusion

Summary

Dell EMC Surveillance solutions enabled by Dell EMC storage arrays, optional RSA Security®, and Dell EMC Networking solutions provide flexible and highly scalable infrastructures that meet a broad range of demanding physical security requirements.

As requirements change and become more sophisticated, this Dell EMC Physical Security solution's flexibility and modular architecture can be enhanced to meet any customer's individual needs.

This paper focused on three distinct architectures. The ring topology and campus topology can be used for video traffic only. The data center topology is designed to carry both surveillance and data center traffic.

The campus architecture and the ring topology, which can be used to connect multiple buildings in the campus. create a very flexible environment with quick recovery.

As requirements change and become more sophisticated, these architectural solutions provide the flexibility that can interconnect modular architectures. These architectures meet the need for a resilient surveillance network infrastructure for any environment and can scale to accommodate future needs.