Dell Networking Campus Switching and Mobility Reference Architecture 3.0

Dell Network Solutions Engineering

April 2016

A Dell EMC Reference Architecture

Revisions

Date	Version	Description	Authors
April 2016	1.0	New campus networking product, C9010 with C1048P. New N-Series features	Manjesh Siddamurthy, Gerald Myers, Colin King, Ed Blazek

THIS DOCUMENT IS PROVIDED “AS-IS”, AND WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED. IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE SPECIFICALLY DISCLAIMED. PRODUCT WARRANTIES APPLICABLE TO THE DELL PRODUCTS DESCRIBED IN THIS DOCUMENT MAY BE FOUND AT: http://www.dell.com/learn/us/en/vn/terms-of-sale-commercial-and-public-sector-warranties Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell’s recommendation of those products. Please consult your Dell representative for additional information.

Table of contents

Revisions....2

1 Introduction....5

2 Campus networks designed for end-user connectivity....7

2.1 Dell Networking C9010 Network Director and C1048P Rapid Access Node....8

2.2 Dell Networking N-Series Ethernet switches....9

2.2.1 Dell Networking N4000 Series....9

2.2.2 Dell Networking N3000 Series....10

2.3 Dell Networking W-Series wireless LAN....11

2.3.1 Dell Networking W-7200 Series controllers....11

2.3.2 Dell Networking W-AP220 Series 802.11ac Access Point....11

2.3.3 Dell Networking Instant W-IAP220 Series controller-less 802.11ac access point....12

2.3.4 Dell Networking Instant W-IAP155/P controller-less 802.11n access point....13

2.3.5 Dell Networking W-Series ClearPass access management system....13

2.4 Network management solutions....14

2.4.1 Wired management solution....14

2.4.2 Wireless management solutions....15

2.5 Dell SonicWALL NSA Series....15

3 Campus reference design....17

3.1 Campus reference design topology....18

3.2 Large campus....19

4 Campus switching architecture....23

4.1 Campus switching architecture using C-Series switches and VLT....23

4.1.1 Important features and best practices....24

4.2 Campus switching architecture using N-Series switches and MLAG....34

4.2.1 Important features and best practices....35

4.2.2 Dell Networking OS 6.3 functionality enhancements....45

5 Campus mobility architecture....46

5.1 W-Series controller-based WLAN....46

5.1.1 W-Series controller topology....47

5.1.2 WLAN main campus configuration....48

5.2 W-Series Instant Access Point – remote deployments 57

5.2.1 W-Series Instant Access Point networks 57

5.2.2 W-Series Instant Access Points for teleworkers 57

5.3 W-ClearPass Access Management 58

5.3.1 W-ClearPass Policy Manager 58

5.3.2 W-ClearPass applications 62

6 Campus Network Management System 64

6.1 OpenManage Network Manager 64

6.2 W-Airwave 69

6.2.1 W-Airwave interface 69

6.2.2 W-Airwave features 72

7 Campus firewall 78

7.1 Best practices and important features 78

7.1.1 Active/standby high availability 78

7.1.2 Security services licenses 80

7.1.3 NAT policies, zones and firewall 81

A Resources and references 83

B Attachments 84

C Firmware versions in this document 85

D Support and feedback 86

About Dell EMC 86

1 Introduction

Campus network deployments change at a rapid pace. IT managers must support an increasing variety of users and devices throughout their organizations. Simultaneously, they must adapt their networks to address the needs of key business functions while providing reliability, performance and flexibility. Today's businesses require campus networks to provide reliable, high-performance wired and wireless connectivity. These networks must be capable of delivering rich applications and access to corporate resources regardless of device form factors.

In addition, business owners today ask their IT staff to be more agile by delivering network access in ever-shorter deployment times with fewer resources.

The Dell Networking Campus Reference Architecture (CRA) provides solutions to address these key problems facing businesses both large and small. The Reference Architecture is a blue print for a modern campus network, as shown in Figure 1, providing an understanding of the network design principles and best practices. This Reference Architecture enables network designers to get a running start on their deployments so they can quickly deliver valued solutions to their businesses.

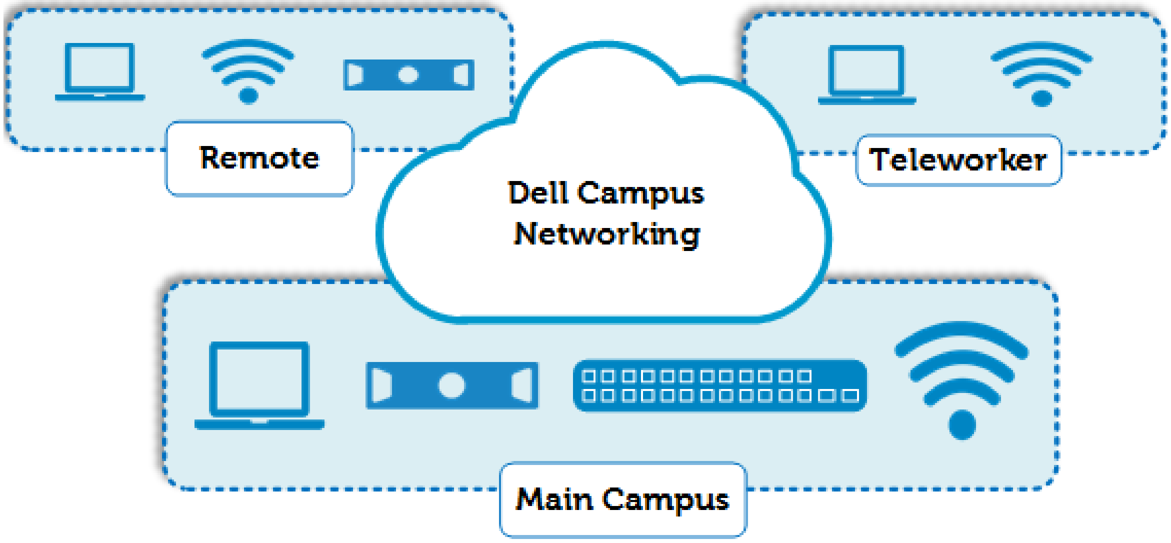


Figure 1 Campus: global view

The Reference Architecture addresses the following:

- Designing a modern, end-to-end campus network to deliver wired and wireless user connectivity incorporating switching, mobility and security
- Simplifying the complex deployment and manageability of separate sites in a campus or across branches
- Delivering a modern approach to access and aggregation that minimizes downtime in campus networks
- Enabling role-based access management and dynamic policy assignment for guests, employees and contractors
- Enabling users to self-provision corporate and guest access on a variety of devices (Bring Your Own Device [BYOD])
- Providing the latest technology to address speed, bandwidth, redundancy and failure-resistant networks
- Providing architectural options utilizing different product types (modular and fixed form factor stackable products)

A network that performs best is one that meets current business and user needs. It is built on a solid infrastructure and enables the business and its goals to scale as needed.

2 Campus networks designed for end-user connectivity

Dell Networking products provide all the pieces of the puzzle to enable your workforce to perform both efficiently and reliably, as shown in Figure 2:

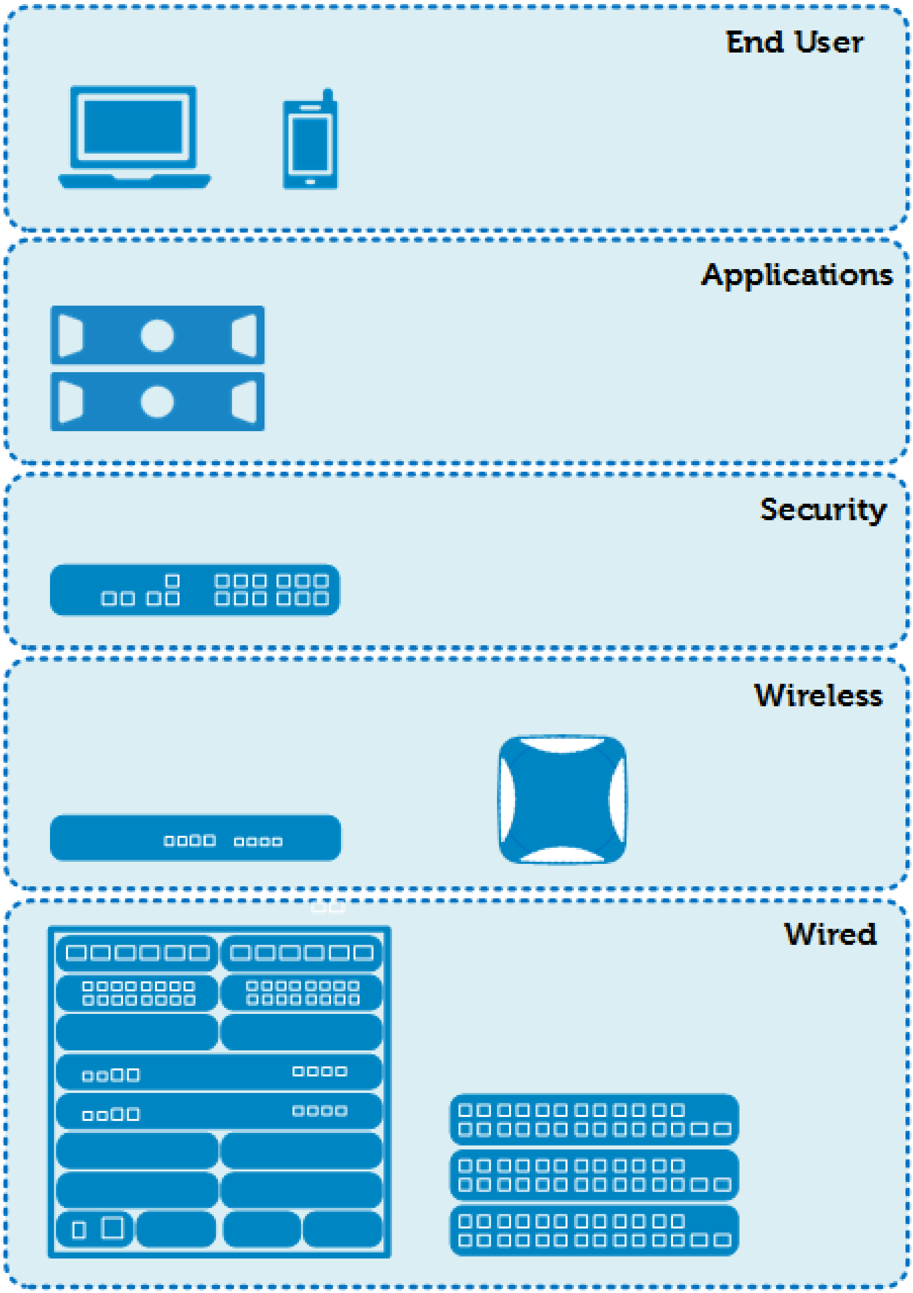


Figure 2 Dell EMC campus network components

2.1 Dell Networking C9010 Network Director and C1048P Rapid Access Node

The Dell Networking C9010 Network Director is a next-generation, multi-rate-capable, modular switching platform designed as the core/aggregation for medium to large enterprise campus and mid-market data center networks. The C9010 is the first platform delivering on the Dell EMC unified enterprise network architecture, ushering in a new way to design and manage networks when used in conjunction with the C1048P Rapid Access Node.

The Dell EMC unified enterprise network simplifies network deployment and management and extends the functionality of core devices all the way to the network edge. It achieves this by collapsing separate network tiers into a single logical switching tier. This removes complex protocols running between access and core/aggregation tiers and centralizes management and control.

Deployments can include the C9010 as a traditional switching platform without the C1048P, serving to aggregate legacy switching platforms in wiring closets and server racks. This deployment model can introduce C1048P Rapid Access Nodes at any time to benefit from the new architecture while maintaining investment protection for legacy switches.

The C9010 is an intelligently designed 8-rack unit (RU) platform with modular slots for up to 10 line card modules, 2 route processor modules (RPM), 3 fan modules and 4 power supply modules. The integrated backplane is 100GbE, multi-rate capable (up to 600Gbps to each line card slot) and provides the investment protection necessary to deploy a modular chassis.

For line-rate designs, two RPMs provide the required bandwidth to each line card slot for inter-line card switching. Line cards themselves manage intra-line card switching. The C9010 offers the following three line card options for design flexibility:

- SFP+ (24-ports)
- 10GBASE-T (24-ports)
- QSFP+ (6-ports)

The Dell Networking C1048P extends the capabilities of the C9010, shown in Figure 3, by providing 48 10/100/1000BASE-T PoE+ ports for user/server access. Two 10G SFP+ uplinks provide connectivity to the C9010. Deploy the C1048P in a stand-alone or stacked configuration depending on the required density, supported configuration and deployment model.

This architecture deploys the C1048P using high performance stacking to connect and power the following:

- W-AP220 series Access Points (APs)
- End-user wired client devices
- IP cameras
- VoIP phones
- Security and Control devices

Figure 3 Dell Networking C9010 Network Director

The C1048P Rapid Access Nodes, shown in Figure 4, receive their configuration and software updates centrally from the C9010 Network Director. This greatly simplifies initial deployment as well as ongoing maintenance and operation.

Figure 4 Dell Networking C1048P Rapid Access Node

2.2 Dell Networking N-Series Ethernet switches

The Dell Networking Ethernet switch product line delivers end-to-end modern campus-network solutions utilizing the latest switching technologies. The topology and features used in the CRA enable a loop-free and fully active/active design for high-performance, fault-tolerant campus switching networks. The design of these energy-efficient, 1/10GbE switches enables modernization and scaling of campus networks.

2.2.1 Dell Networking N4000 Series

The heart of the modern campus consists of N4000 Series 10GbE Layer 3 switches, shown in Figure 5. These switches provide a power-efficient and flexible 10GbE switching solution for simple scalability and high density.

Figure 5 Dell Networking N4000 Series

The N4000 series switches also feature Multi-chassis Link Aggregation (MLAG) to support loop-free redundancy without spanning tree.

The architecture with MLAG allows two Dell Networking switches to act as a single switch providing multiple paths across the network. The benefits of MLAG include:

- Failover in cases of failed cables or switches
- Increased bandwidth of up to double that of a single switch
- Elimination of port blocking and re-convergence delays of spanning tree

Note: For further information on Dell MLAG technology, please refer to Appendix A, Resources and References.

2.2.2 Dell Networking N3000 Series

The Access Layer of this architecture is comprised of N3000 Series 1GbE Layer 3 switches, shown in Figure 6:

Figure 6 Dell Networking N3000 Series

N3000 Series switches provide a resilient 1GbE switching solution for advanced Layer 3 distribution and dense stacking. Dual hot swappable 80 Plus-certified power supplies add resiliency and the capacity to provide up to 48 ports of PoE+ in a 1RU footprint.

This architecture deploys the N3000 Series switches using high performance stacking across the campus to connect and power the following:

- W-AP220 series Access Points (APs)
- End-user wired client devices
- IP cameras
- VoIP phones
- Security and Control devices

2.3 Dell Networking W-Series wireless LAN

Dell Networking's wireless product line is a best-in-class enterprise solution. The W-Series offers the latest in wireless technology and access solutions to better manage, secure and maintain your network.

Dell Networking's W-Series wireless LAN (WLAN) products offer both centralized controller-based and distributed controller-less solutions. With this architectural flexibility, the W-Series product line offers a wide variety of capacity and performance options to fit any campus, branch or teleworker deployment.

2.3.1 Dell Networking W-7200 Series controllers

The W-7200 Series controllers are high-density, power-efficient, 1U devices that support up to 2048 APs and 32,000 users with 40Gbps of encrypted throughput, shown in Figure 7:

Figure 7 Dell Networking W-7200 Series mobility controller

The campus reference design utilizes the W-7210 Controller, which provides support for up to 512 APs and over 16,000 concurrent users/devices. This centralized controller-based solution's features include:

- Policy Enforcement
- Application-aware monitoring and enforcement
- Redundancy topologies and centralized licensing
- Spectrum monitoring
- Wireless Intrusion Protection™
- Advanced Cryptography™
- VPN termination

2.3.2 Dell Networking W-AP220 Series 802.11ac Access Point

Dell Networking W-AP220 Series Access Points, shown in Figure 8, are purpose-built 802.11ac Enterprise access points. The campus reference design utilizes the W-AP225 Access Point to support the fastest performance and largest capacity available. Its features include:

- 1.9 Gbps aggregate throughput
  - 1.3 Gbps in 5GHz
  - 600 Mbps in 2.4GHz
- Adaptive Radio Management®
  - Active RF spectrum management for optimal WLAN performance
- ClientMatch® technology
  - Infrastructure-controlled client connectivity and roaming optimization
- Internal and external antenna options

Figure 8 Dell Networking W-AP220 Series Access Point

2.3.3 Dell Networking Instant W-IAP220 Series controller-less 802.11ac access point

The campus reference design utilizes the W-IAP225, shown in Figure 9, for remote buildings and offices. These Instant Access Points (IAPs) feature a virtual controller for a distributed, controller-less solution. The simplicity of configuration and deployment make Instant products a perfect solution for remote sites with limited IT expertise onsite.

IAPs offer many of the same enterprise class features as normal APs, including:

- Over-the-air provisioning
- VPN
- Integrated firewall
- Airwave® and ClearPass® integration

Figure 9 Dell Networking W-IAP220 Series Instant Access Point

2.3.4 Dell Networking Instant W-IAP155/P controller-less 802.11n access point

The W-IAP155/P Access Points, shown in Figure 10, have the same software as the W-IAP220 Series IAPs above. They support 802.11n and have a form-factor that makes them perfect for desktop or small business applications. They include four GbE Ethernet ports to enable the connection of peripherals. The PoE version provides two ports for connecting devices requiring PoE power. The CRA uses the W-IAP155/P as a remote access point solution.

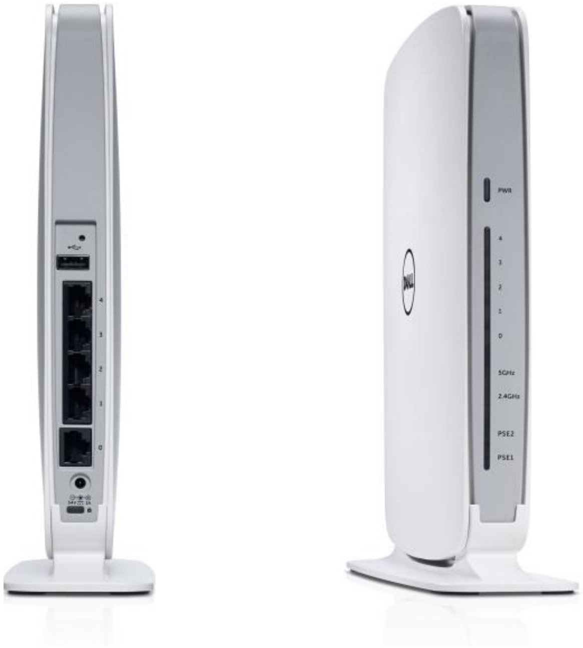


Figure 10 Dell Networking instant W-IAP155

2.3.5 Dell Networking W-Series ClearPass access management system

A modern campus must deliver appropriate access to users with context-aware policies that take into account the following:

- Who the user is
- What their role is
- What type of device they are using
- When are they connected
- Where they are located
- What applications they are using on the network

The W-ClearPass, shown in Figure 11, is a highly integrated access management solution incorporating AAA (Authentication, Authorization and Accounting), Guest/Visitor Management, Employee Onboarding and Network Access Control (NAC). It provides role- and device-based network access control for employees, contractors and guests across wired, wireless and VPN infrastructures. Built-in Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control System (TACACS+), profiling, onboarding, guest access, health checks and the ability to leverage third-party mobile device management solutions ensure seamless policy enforcement across the entire network. Centrally managed network access policies provide the comprehensive authentication capabilities that are required for today's highly mobile workforce, regardless of the type of device or device ownership. Automated services let users securely connect their own devices, register AirPlay- and AirPrint-enabled devices for sharing, and create guest access credentials. The result is a consistent and scalable network access control solution that exceeds the security requirements for Bring Your Own Device (BYOD) and IT managed devices.

Figure 11 W-ClearPass appliance

Key features of W-ClearPass include:

- Policy management – role enforcement for WLAN, LAN, and VPN networks
- Onboard – BYOD, auto-provisioning
- OnGuard – Posture, health checks
- Guest – self-service guest access
- Third-party Mobile Device Management (MDM) and Network Access Control (NAC) integration
- Built-in Authentication, Authorization and Accounting (AAA) services – RADUIS, TACACS+, Kerberos
- Web, 802.1X, non-802.1X authentication and authorization

2.4 Network management solutions

2.4.1 Wired management solution

Dell Networking OpenManage Network Manager

OpenManage Network Manager (OMNM) is a centralized management solution for Dell EMC networking environments. OMNM provides discovery, configuration management, monitoring and reporting for the entire Dell Networking family of products as well as Cisco, Juniper, HP and Brocade network devices. Its other benefits include:

- Resource group management for one-to-many device configuration
- Automated discovery of network devices
- Inventory reporting

- Advanced scheduling for key tasks, such as backup and configuration changes
- Event management
- Customizable web-based UI
- Flexible dashboards for fault, availability and performance monitoring

2.4.2 Wireless management solutions

2.4.2.1 Dell Networking W-Airwave Wireless Management Suite

The W-Airwave Wireless Management Suite (AWMS) delivers operational efficiency for teams managing rapidly changing networks and mobile users who connect via the wireless LAN as well as wired Ethernet ports. AWMS provides a wide range of actionable information, from time-sensitive alerts to historical reporting. With data that spans days, months, and seasons, the information is always available to spot trends, plan capacity and design the right strategies for the organization.

Key features in W-Airwave include:

- Efficient configuration management
- VisualRF – real-time wireless coverage maps
- Planning and provisioning
- Multi-vendor support
- MDM integration
- Intrusion Detection System (IDS) and rogue Access Point (AP) containment

2.5 Dell SonicWALL NSA Series

The Dell SonicWALL Next-Generation Firewall Series, shown in Figure 12, secures distributed enterprises, small-to-medium-sized organizations, branch offices, school campuses and government agencies with features such as:

- Next-generation firewall security
- Multi-core architecture
- Deep packet inspection technology
- Lowered complexity and cost
- Intrusion prevention
- Gateway anti-malware
- SSL decryption

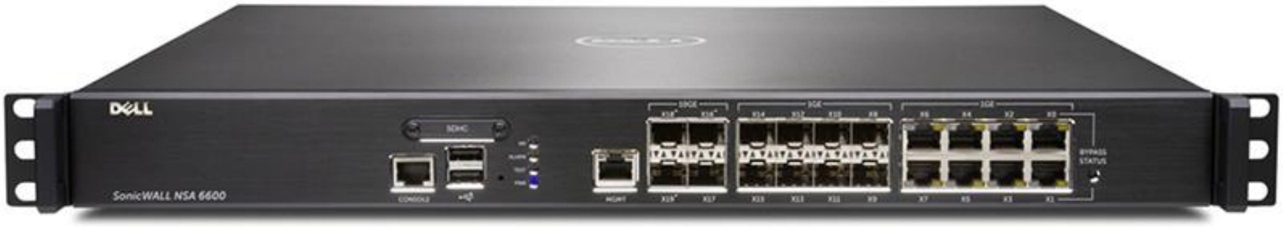


Figure 12 Dell SonicWALL NSA 6600

Dell SonicWALL Next-Generation Firewalls provide industry-leading protection, performance and scalability with the highest number of concurrent connections, lowest latency, no file-size limitations and class-leading connections per-second.

The Dell SonicWALL Network Security Appliance (NSA) Series utilizes the same architecture found in the flagship SuperMassive Next-Generation Firewall line. Dell EMC initially developed the SonicWALL NSA Series for the most demanding carriers and enterprises. It delivers that same enterprise-class security and performance while also providing Dell EMC’s acclaimed expertise in delivering ease-of-use and high value to small and medium-sized organizations.

3 Campus reference design

The goal of the CRA is to help IT managers evaluate and plan for an end-to-end campus network. This document shows how wired, wireless, network access and network management fit together.

The campus network design scales around the number and type of users, and device types (wired and mobile). This Reference Architecture is built for 3000 users on a modern campus who connect using both wired and wireless devices.

This document presents two topologies with each topology differentiated by the Ethernet switching products and features used at the Aggregation/Core and Access Layers. The first example uses Dell Networking N-Series with Multi-chassis Link Aggregation (MLAG). The second example uses the Dell Networking C-Series with Virtual Link Trunking (VLT). Each topology uses identical mobility, security and network management products.

Note: This section presents the topology using C-Series with VLT first, followed immediately by the topology with N-Series switches with MLAG. Chapter 4 presents a complete description of VLT and MLAG technologies.

3.1 Campus reference design topology

Figure 13 and Figure 14 show the entire campus network, including all the key parts needed for medium- to large-campus deployments.

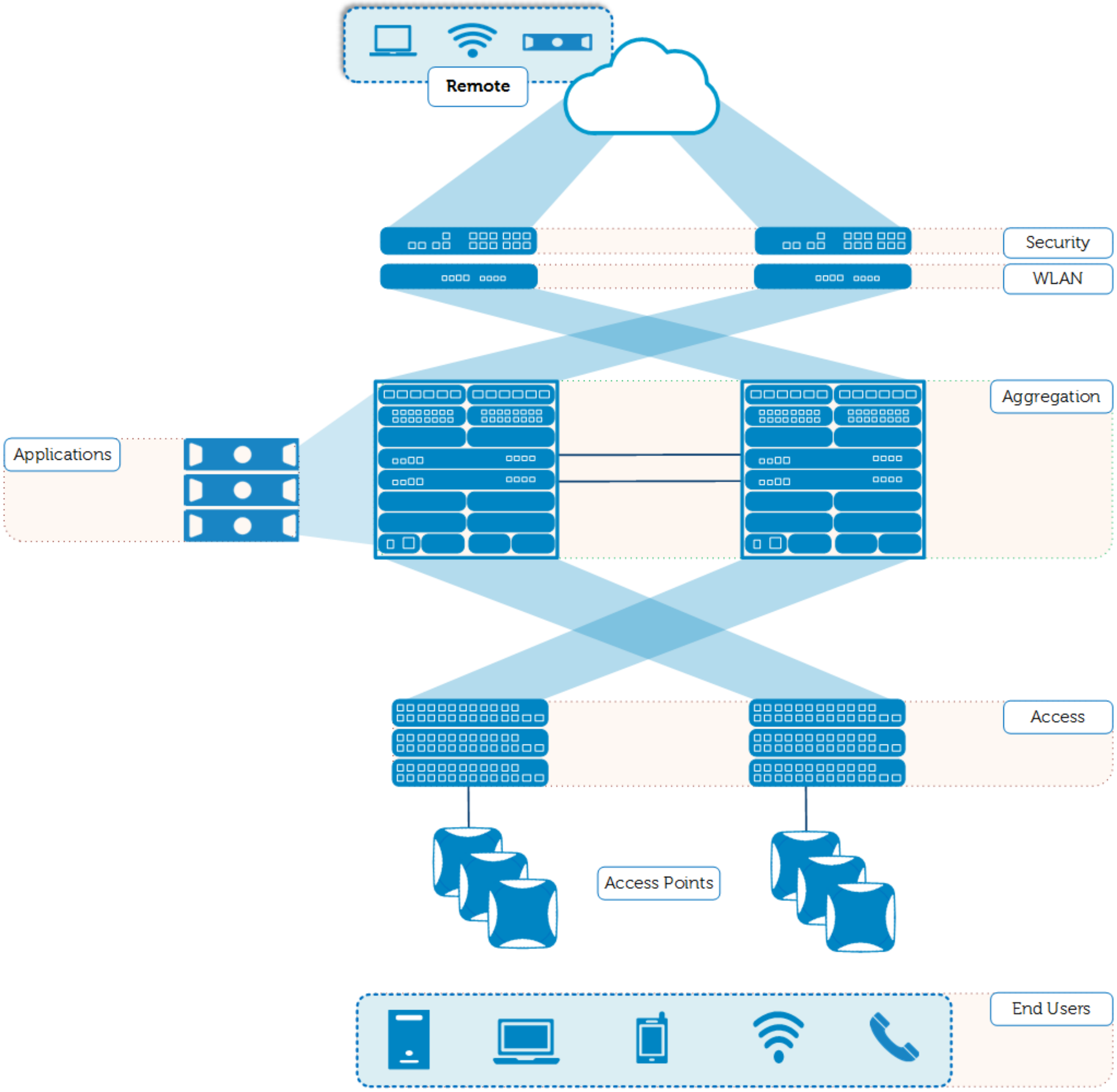


Figure 13 Featured campus network – C-Series with VLT

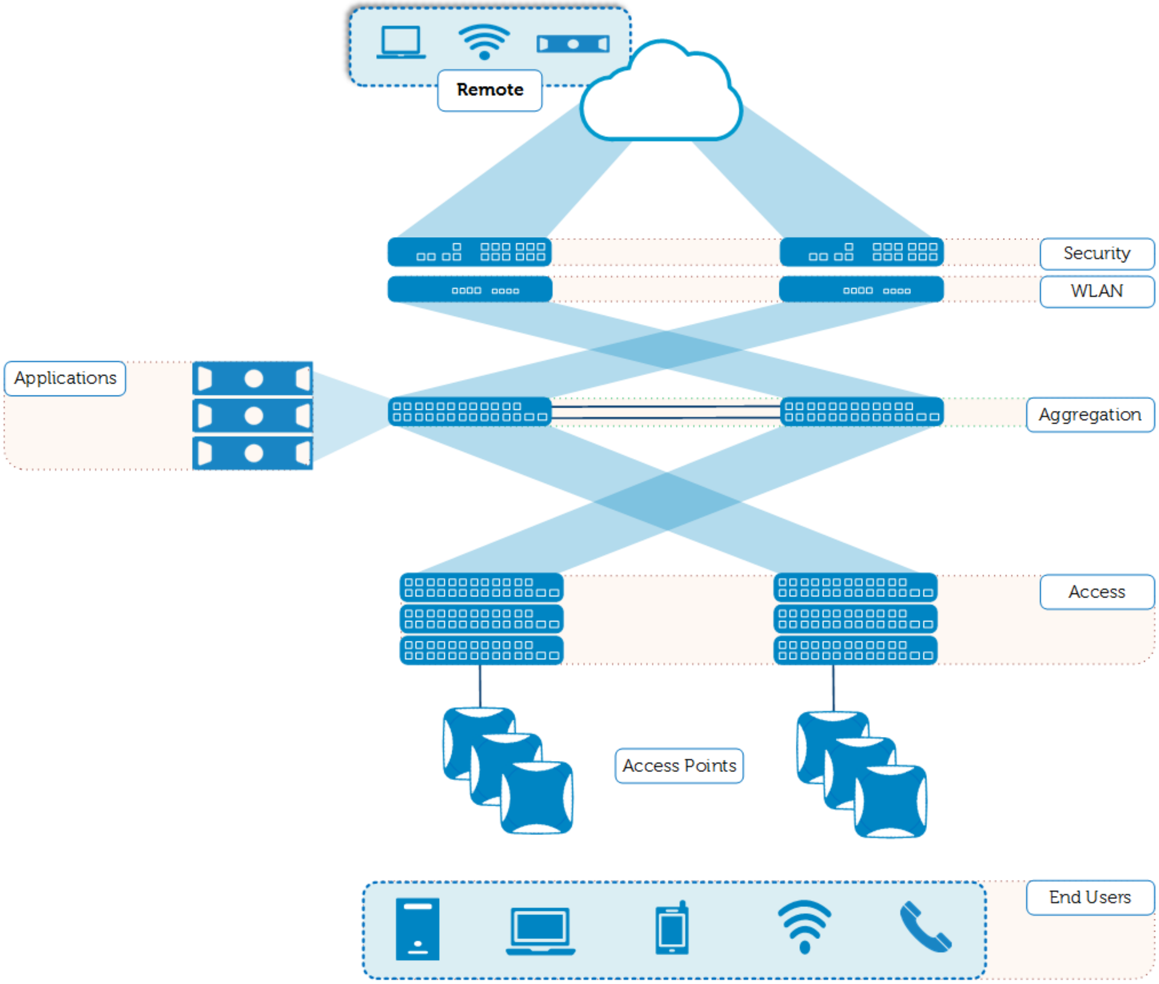


Figure 14 Featured campus network – N-Series with MLAG

3.2 Large campus

This reference architecture covers a simple illustration for a large campus with 3000 users accessible throughout two 5-story buildings. Both buildings include one server room, and each floor has multiple wiring closets. The server room contains the aggregation switches, wireless controllers, firewalls as well as network and policy management appliances.

Any network build-out must allow for future growth. A best practice is to add unoccupied ports at approximately 10% of occupied ports to allow for future network expansion without equipment additions.

The following lists provide an example for a single building for both the C-Series and N-Series topologies. Each building services 1500 users.

C-Series with VLT topology — Access Layer

For an example of this topology, see the Access Layer Section of Figure 13.

C-Series Access:

- C1048P Rapid Access Nodes: 42
  - Ethernet ports: 2000
  - Ports reserved for future growth: 200
  - Ports for current users and VoIP phones: 1500
  - Ports for access points: 75
  - Ports for miscellaneous devices (printers, sensors, cameras and so on): 225

This example uses a single Aggregation Layer in each building. IT managers may prefer to implement a multiple-tiered design or use existing routing infrastructure to connect buildings. The lists below provides an example for a single building for both the N-Series and C-Series topologies. Each building services 1500 users. Future firmware releases of the C9010 support 4000 Ethernet ports with the C1048P Rapid Access Node.

C-Series with VLT topology — Aggregation Layer

For an example of the topology, see the Aggregation/Core Layer Section of Figure 13.

Aggregation with VLT Topology:

- C-9010 Chassis: 2
- C9000 24-port 10GbE SFP+ line cards: 3 per chassis
  - SFP+ ports : 72
  - Ports used for VLTi link: up to 8
  - 10GbE to WLAN controllers: 4
  - 10GbE to firewalls: 4
  - 10GbE to access stacks: 14
  - 10 GbE ports to connect misc. servers/appliances: 42
- C9000 24-port 10GbE 10GBASE-T line card: 1
  - Ports used for server based appliances (W-ClearPass, W-Airwave, OMNM) : 3
- Empty line card slots for misc. servers/appliances/devices: 6-7 per chassis
- Route Processor Modules (1+1 redundancy): 2 per chassis

The C-Series chassis products have a large degree of flexibility. Administrators can choose from a large array of line cards with different technologies. Administrators should keep in mind the oversubscription rates for each line card when planning their networks. They can add more line cards for future growth at any time.

N-Series with MLAG topology — Access Layer

For an example of this topology, see the Access Layer Section of Figure 13.

N-Series access:

- N3048P switches: 42
  - POE+ ports: 2016
  - Ports reserved for future growth: 200
  - Ports for current users and VoIP phones: 1500
  - Ports used for access points: 75 (approximately)
  - POE+ ports for auxiliary devices (printers, sensors, cameras and so on): 241

N-Series with MLAG topology — Aggregation Layer

For an example of the topology, see the Aggregation/Core Layer Section of Figure 13.

Aggregation with MLAG Topology:

- N4064F switches: 2
  - SFP+ ports: 128
  - Ports reserved for future growth: 12
  - Ports used for MLAG link: 2
  - Ports used to connect Access Stacks: 14
  - Ports used to connect 2 firewalls: 4
  - Ports used to connect 2 WLAN controllers: 4
  - Ports to connect misc. severs/appliances: 92

C-Series (Figure 13) and N-Series (Figure 14) topologies use identical mobility, security, and network management products.

Wireless Controllers and APs:

- W-7210 controllers: 2
  - W-7210 - 512 campus or remote AP capacity
  - APs for future growth: 51
  - APs used for main campus (20 users per AP): 150
  - APs used as Air Monitors (optional, 1 Air Monitor per 4 APs): 37
  - APs for teleworkers: 274
  - Instant APs (remote site)- quantity dependent on users at remote site

W-ClearPass:

- 5K appliances: 1
  - Supports up to 5,000 authenticated devices
  - Administrators can add an additional 5,000 appliances to form a cluster at any time

W-Airwave:

- W-Airwave is sold as a per-device license.
  - Purchase additional licenses at any time.
  - Number of devices limited by server size and capability.

Open Manage Network Manager:

- OMNM is sold as a per-device license
  - Purchase additional licenses at any time.
  - Number of devices limited by server size and capability

SonicWALL:

- NSA6600: 2
  - License per HA pair
  - 10 GbE SFP+ ports for optimal bandwidth to/from Aggregation Switches: 4
  - Maximum users for single sign-on: 4,000
  - Firewall inspection throughput: 12.0 Gbps

This Reference Architecture discusses organizations with remote offices or remote workers in Chapter 5, Campus Mobility Architecture. This example does not include traditional, wired switching solutions for the remote sites. However, Chapter 5 validates and discusses the wireless features to connect to the corporate campus network.

4 Campus switching architecture

4.1 Campus switching architecture using C-Series switches and VLT

The Dell Networking C9000-series chassis switches provide a high-density, resilient, end-to-end campus network infrastructure that offers flexibility, expansion and broad customization options including 10GbE/40GbE/10GBT line cards and Rapid Access Nodes (port extenders). POE/POE+ currently is only supported with associated C1048P port extender (PE). Additionally, the C9000 switch can remotely manage the C1048P. Chassis features such as dual controllers and fully redundant power supplies help reduce downtime. The Virtual Link Trunking (VLT) feature brings node resiliency to Layer 2 networks providing more network availability in the event of a node failure.

The C9000-series switches with Rapid Access Node do the following:

- Alleviate bottlenecks and congestion to enable high-performance back-end infrastructure for end-user mobility with PoE+ where needed.
- Provide several deployment options including resilient campus core, campus aggregation and wiring closet access.
- Support more client connectivity compared to the competition and Virtual Desktop Infrastructure (VDI) workloads across a global workforce with scalable user density and performance on-demand.

When building the Campus Switching Architecture 3.0, a pair of C9010 switches running VLT work the same as a pair of N4000s running MLAG (refer to section 4.2) but with higher port density and flexibility.

Their POE+ capabilities make C1048Ps and N3048Ps a good fit at the Access Layer. The POE+ feature can help power up and integrate access points, security cameras, IP phones and other powered devices.

In this architecture, the Access Layer consists of a mix of stacked C1048P PEs and/or stacks of traditional Access switches, connected to pair of C9010s using VLT-LAG, shown in Figure 15. Administrators can plan the number of switches per stack and number of uplinks per stack connected to core depending on oversubscription at the Access Layer.

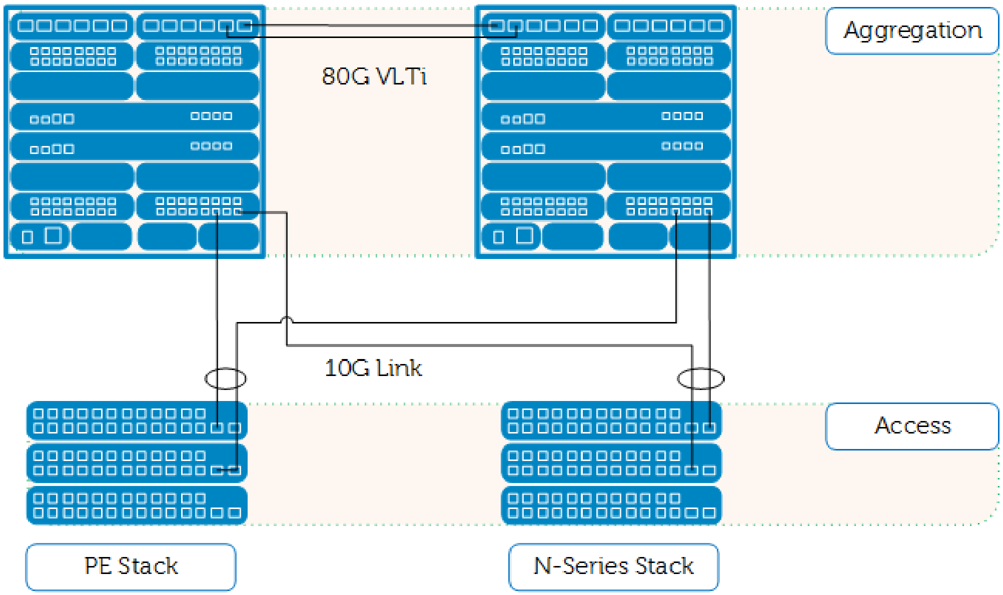


Figure 15 Dell EMC campus aggregation and access switch topology with C-Series and N3000s

Like the MLAG architecture, VLT architecture provides increased bandwidth by overcoming the limitation of spanning tree to block redundant ports. The design is highly redundant in terms of both link failure and switch failure.

4.1.1 Important features and best practices

The following sections outline some of the features and guidelines to consider while designing a campus network.

4.1.1.1 Virtual Link Trunking

VLT allows physical links between two chassis to appear as a single virtual link to the network core or other switches (Edge, Access, or Top-of-Rack [ToR]).

By supporting a loop-free topology, VLT reduces the role of the Spanning Tree Protocol (STP) by allowing Link Aggregation Group (LAG) terminations on two separate Aggregation/Core Switches. Rapid Spanning Tree Protocol (RSTP) is used only to prevent loops due to human errors.

Similar to MLAG on N4000's topology, VLT on C-series provides Layer 2 multi-pathing, creates redundancy with increased bandwidth, enables multiple parallel paths between nodes and load-balances traffic where alternative paths exist.

The VLT interconnect must consist of either 10G or 40G ports. It supports a maximum of eight 10G or four 40G ports.

Note: Dell Networking does not support mixing 10G and 40G ports in VLT interconnect (VLTi).

To scale and combine VLT domains, administrators can use an enhanced VLT (eVLT) configuration. An eVLT configuration allows the connection of two different VLT domains by creating a port channel between them. This configuration supports a maximum of four units, increasing the number of available ports and allowing for dual redundancy of the VLT. Figure 16 shows sample eVLT configurations:

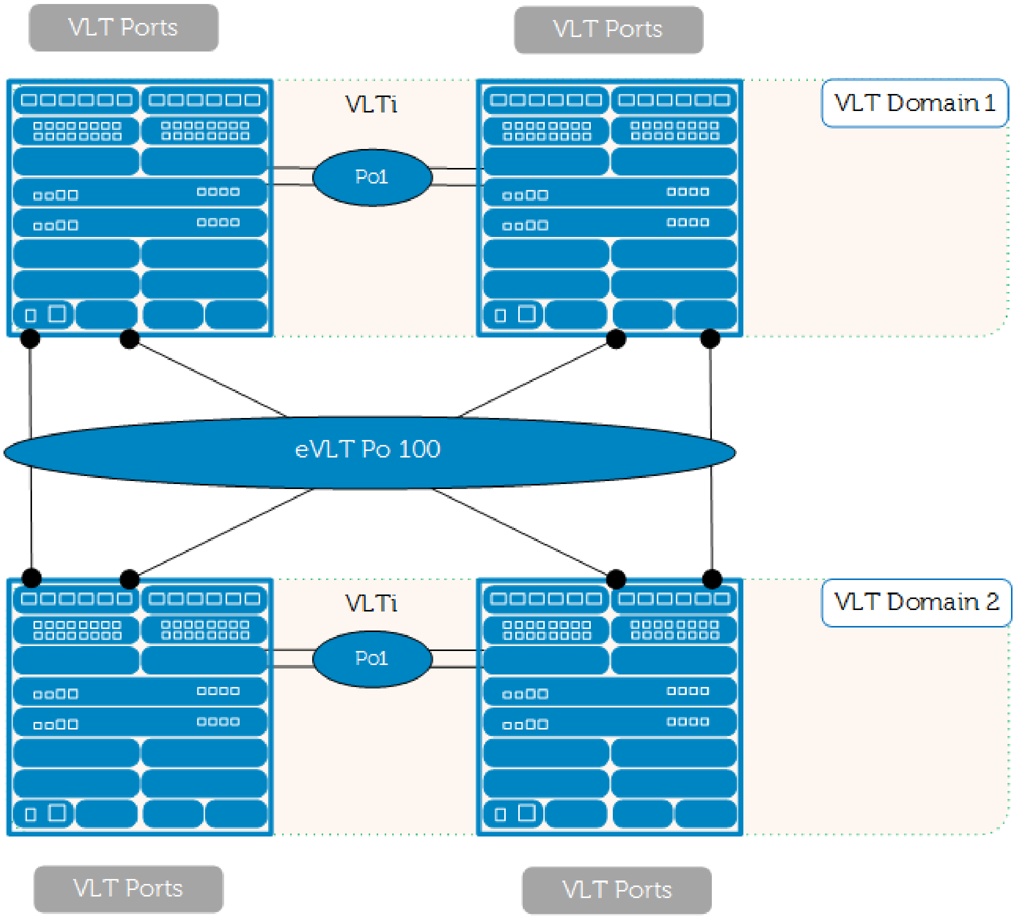


Figure 16 Sample eVLT configurations

Note: For additional information on VLT on Dell Networking C-series switches, refer to the *Dell Networking OS Configuration Guide* at Dell EMC's Support Site.

Figure 17 shows an example of the VLT configuration on the Core/Aggregation switches (Dell Networking C9000 series).

```
vlt domain 1
 peer-link port-channel 12
 back-up destination 172.25.169.67
 system-mac mac-address 00:11:22:33:44:55
 unit-id 0

interface Port-channel 12
 description VLT peer link
 no ip address
 channel-member fortyGigE 1/20
 no shutdown

interface Port-channel 10
 description VLT lag
 no ip address
 portmode hybrid
 switchport
 no shutdown
 vlt-peer-lag port-channel 10

interface TenGigabitEthernet 3/10
 no ip address
 port-channel-protocol LACP
  port-channel 10 mode active
 no shutdown

interface fortyGigE 1/20
 no ip address
 no shutdown
```

Figure 17 VLT configuration on the core/aggregation switches

Note: Throughout this document, the configuration examples contain specific VLAN, IP, and port channel numbers. These specific settings were used to validate the network in a lab setting. The numbers are included in the examples to allow the reader to follow the configurations.

4.1.1.2 Virtual LANs and Virtual Redundancy Routing Protocol (VRRP)

Virtual LANs (VLANs) offer a method of dividing one physical network into multiple broadcast domains. However, VLAN-enabled switches cannot forward traffic across VLANs by themselves. For VLAN to VLAN communication, a Layer 3 switch/router is required. In this architecture, Dell Networking C9010s are used as Aggregation/Core Switches to handle all inter-VLAN routing activities, helping devices from two different VLAN segments to communicate.

Virtual Router Redundancy Protocol (VRRP) eliminates the single point of failure associated with static default routes by enabling a backup router to take over from a master router without affecting the end stations using the route. In this design, the end stations use a VRRP defined virtual IP address as a gateway.

In a VLT domain, VRRP inter-operates with virtual link trunks that carry traffic to and from access devices. The VLT peers belong to the same VRRP group and are assigned master and backup roles. Each peer actively forwards L3 traffic, reducing the traffic flow over the VLT interconnect.

Note: Although both VLT peers actively participate in L3 forwarding as the VRRP master or backup router, the `show vrrp` command output displays one peer as *master* and the other peer as *backup*.

In this reference architecture, several VLANs and VRRP groups are configured at a minimal level to provide what a typical large campus might need. Figure 18 shows an example of a VLAN configuration. To see the full configuration of the Dell Networking C9010 used in this example, refer to the attachment.

```
interface Vlan 5
 description engineering
 ip address 10.1.5.2/24
 tagged Port-channel 1-2,4-5,12

 vrrp-group 5
  virtual-address 10.1.5.10
 no shutdown

interface Vlan 6
 description finance
 ip address 10.1.6.2/24
 tagged Port-channel 1-2,4-5,12

 vrrp-group 6
  virtual-address 10.1.6.10
 no shutdown

interface Vlan 7
 description guest
 ip address 10.1.7.2/24
 tagged Port-channel 1-2,4-5,12

 vrrp-group 7
  virtual-address 10.1.7.77
 no shutdown

interface Vlan 50
 ip address 10.1.50.2/24
 untagged Port-channel 8-9

 vrrp-group 50
  virtual-address 10.1.50.10
 no shutdown

interface Vlan 57
 description NMS
 ip address 10.1.57.2/24
 tagged Port-channel 1-2,4-5,12

 vrrp-group 57
```

```
  virtual-address 10.1.57.10
 no shutdown

interface Vlan 100
 description general
 ip address 10.1.100.2/24
 untagged Port-channel 1-5,12

 vrrp-group 100
  virtual-address 10.1.100.50
 no shutdown
```

Figure 18 Example of the VLAN configuration on the core/aggregation switches (Dell Networking C9000)

4.1.1.3 Spanning tree

A properly configured VLT network provides a loop-free, redundant topology and does not normally require spanning-tree to prevent loops. However, it is best practice to enable either RSTP or PVST+ on all network devices. This prevents loops due to misconfiguration or improper connections during the initial setup. VLT's Layer 2 multi-pathing provides full use of all VLT connections and eliminates path blocking. The enabling of either RSTP or PVST+ provides for the detection and prevention of potential loops caused by non-system issues such as cabling errors or incorrect configurations.

RSTP can cause temporary port state blocking and may cause topology changes after link or node failures. Spanning tree topology changes reach the entire Layer 2 network.

Note: Follow these recommendations in setting up a VLT network.
Ensure that the primary VLT node is the Root Bridge and the secondary VLT peer node has the second-best bridge ID in the network. Ensure all other devices have a higher bridge priority to keep the VLT core as the Root Bridge.
Ensure any end device interfaces are configured as edge ports to prevent spanning-tree forwarding delays.

Table 1 VLT node spanning tree settings

Primary VLT node	Secondary VLT node	All other devices
protocol spanning-tree rstp no disable bridge-priority 4096	protocol spanning-tree rstp no disable bridge-priority 8192	protocol spanning-tree rstp no disable bridge-priority default 32768

4.1.1.4 Port extender (Rapid Access Node)

To provide capacity at the Access Layer typically requires 10/100/1000BaseT interfaces with limited reach and requires locating Layer 2 switches closer to the users. These network devices must be linked to the Aggregation/Core network to reach other networks. This requires individual management of many devices. The C9000 series solves this issue by implementing IEEE 802.1BR on port extenders (PEs). PEs get their configuration from the C9000 chassis, enabling all configuration, management and monitoring from a single device.

The C9000 series switch supports local or remotely located C1048P PEs to provide 10/100/1000BaseT and PoE/PoE+ to end devices at the Access Layer. The PE is a Layer 2 device that extends line card functionality to the access layer at distances up to 40 km from the chassis. All PE management is from the C9000; individual units do not require independent management. PE interface configuration is the same as the line card interfaces. Also, future upgrades for PEs are handled automatically by the chassis, which reduces maintenance work.

Note: Catering to the majority of campus traffic patterns, all PE traffic traverses the C9010. This alleviates the need for local switching on the C1048P so all intra-port PE traffic travels to and from the chassis via the 10G uplinks. Keep this in mind when planning or deploying the system.

A Layer 2 device, the PE is designed primarily to support edge devices. The list of supported Layer 2 protocols on PEs includes the following:

- 802.1X
- BDPU Guard
- PoE
- LAG
- LACP
- LLDP
- Loop Detection
- Switch stacking
- QoS

```
Dell#configure terminal
Dell(conf)# feature extended-bridge

Dell(conf)# pe provision 0
Dell(conf-pe)#cascade interface tegig 2/20
Dell(conf-pe)#cascade interface tegig 3/20
Dell(conf-pe)#stack-unit 0 type C1048P
```

Figure 19 Activating a PE with two uplink ports

4.1.1.5 Port Extender stacking

The PE stacking feature increases scalability and enhances redundancy. The feature allows up to eight switches to operate as a single unit. A PE (also known as a Rapid Access Node) has two fixed mini-SAS stacking connectors at the rear for this purpose. Stacking allows a higher concentration bandwidth of Access ports to uplinks if desired (ranging from 2.4-to-1 through 19.2-to-1, based on number of stack members).

PE stacking enhances redundancy by allowing the stacked PE to use any uplink in the stack. To minimize bandwidth loss if an uplink or stack member fails, spread multiple uplinks across the stack members. If the Master stack-unit fails, then the Standby stack-unit immediately takes over and elects another member unit to be Standby as pre-determined by configured priority. Traffic on the unaffected members continue carrying the traffic with minimal impact to service.

Dell EMC strongly recommends connecting the stack in a full ring topology, as discussed in subsection Figure 31, so that each PE connects to two other PEs. Using this topology allows the stack to utilize the redundant communication path to each PE. If a switch in a ring topology fails, the stack can automatically establish a new communications path to the other PEs. PEs not stacked in a ring topology may split into multiple independent stacks upon the failure of a single PE or stacking link.

Note: PE stacking should be wired in a full ring topology as shown in Figure 32.

```
Dell#configure terminal

Dell(conf)# pe provision 0
Dell(conf-pe)#cascade interface tegig 2/0-3
Dell(conf-pe)#cascade interface tegig 3/0-3
Dell(conf-pe)#stack-unit 0 type C1048P
Dell(conf-pe)#stack-unit 1 type C1048P
Dell(conf-pe)#stack-unit 2 type C1048P
Dell(conf-pe)#stack-unit 3 type C1048P
Dell(conf-pe)#stack-unit 4 type C1048P
Dell(conf-pe)#stack-unit 5 type C1048P
Dell(conf-pe)#stack-unit 6 type C1048P
Dell(conf-pe)#stack-unit 7 type C1048P
```

Figure 20 Activating maximum PEs in a stack with 8 uplinks to chassis (4.8-to-1).

4.1.1.6 Port Extender dual-homing

For C9000 chassis deployed in a VLT topology, PEs may be deployed so that uplinks are homed to both VLT peers to provide additional redundancy. This fully utilizes all PE uplinks so that there is no wasted bandwidth. If either C9000 VLT peer fails, the remaining redundant chassis services all traffic. Figure 21 shows dual-homed PE configuration.

```
Dell(conf)# pe provision 0
Dell(conf-pe)#cascade interface tegig 5/0-7
Dell(conf-pe)#cascade interface tegig 5/0-7 peer
Dell(conf-pe)#stack-unit 0 type C1048P
Dell(conf-pe)#stack-unit 1 type C1048P
Dell(conf-pe)#stack-unit 2 type C1048P
Dell(conf-pe)#stack-unit 3 type C1048P
Dell(conf-pe)#stack-unit 4 type C1048P
Dell(conf-pe)#stack-unit 5 type C1048P
Dell(conf-pe)#stack-unit 6 type C1048P
Dell(conf-pe)#stack-unit 7 type C1048P
```

Figure 21 Configuring PE in dual-homing mode

Note: Dual-homed PEs are limited to 16 uplinks, eight uplinks to each C9000 chassis in VLT domain.

In dual-homed configurations, the PE interface configurations must match between VLT peers at the core chassis. A provided configuration batch mode supports single unit provisioning. A ‘commit’ operation must be submitted before deploying configurations to either Primary or Secondary VLT peers. See Figure 22:

```
Dell#configure terminal batch
Peer is registered
Dell(conf-b)#int pe 0/0/1
Dell(conf-b-if-pegi-0/0/1)#switchport
Dell(conf-b-if-pegi-0/0/1)#no shutdown
Dell(conf-b-if-pegi-0/0/1)#commit

Logs:
Nov 20 20:00:15: %RPM0-P:CP %CLIBATCH-6-CLI_BATCH_CONFIG_IN_PROGRESS_TRAP:
Batch configuration commit is in progress
Nov 20 20:00:15: %RPM0-P:CP %CLIBATCH-6-CLI_BATCH_CONFIG_COMPLETE_TRAP:
Batch configuration commit is success
```

Figure 22 Dual-homing batch commands

Note: Batch command mode only applies to PE interface configurations. Refer to Dell EMC Support for the Dell Networking C9000 series configuration guide and more information on batch and non-batch configurations

4.1.1.7 Port Extender loop detection and prevention

Network loops can be detrimental to performance and service quality. Layer 2 networks prevent this by implementing STP on all switching devices, which blocks redundant paths. However, PE interfaces do not support STP. Network loops can result if a Layer 2 switch interface attaches to a PE while connected to another part of the network.

BDPU Guard, which is assigned by default to all PE interfaces, resolves this issue. If an STP-enabled network device attaches to a PE port, the PE detects the STP BDPUs and sets that interface to an error-disable state. This prevents some accidental loops.

Dell EMC recommends using the CLI command `MAC-address-table Station-move threshold` to detect loops. This fully addresses loop detection and prevention with PEs (for example, a link between two PE interfaces), Then, when different interfaces in a VLAN learn the same MAC address within a given time period, the offending interfaces are set to an error-disabled state automatically. The network administrator determines these thresholds and intervals. Figure 23 shows that when this threshold is exceeded, all but the lowest numbered port is placed in error-disabled state:

```
Dell(conf)# mac-address-table station-move threshold 5 interval 30

Jun 18 09:55:35: %RPM0-P:RP %MACMGR-1-PE LOOP DETECTION: Loop occurred on PE
interfaces:oldInterface: peGigE 1/0/47, newInterface: peGigE 1/0/48,vlanId:
7, macAddr: 00:aa:01:02:03:

Dell#show mac learning-limit violate-action
Interface      Violation-Type Violate-Action      Status
Te 2/3         station-move   log                 Normal
PeGi 1/0/48    Pe-Loop        Shutdown            PEloop-disable
Po   1         Pe-Loop        Shutdown            PEloop-disable
```

Figure 23 Recommended loop-detection and prevention on PEs

4.1.1.8 Security and authentication

IEEE 802.1x is an IEEE standard defining a method of port security. The standard enables the authentication of system users through a local internal server or an external server. A port that is enabled with 802.1X disallows connected devices from sending or receiving network traffic before verification of the device's identity.

The device attempting to access the network is the supplicant. The device with which the supplicant communicates is the authenticator. The authenticator (Dell EMC switch) is the gate keeper of the network. It translates and forwards requests and responses between the authentication server and the supplicant.

IEEE 802.1X allows manually placing ports into any of three states:

- **ForceAuthorized** is an authorized state. A device connected to a port in this state does through the authentication process but can communicate on the network. To place a port in this state is the same as disabling 802.1X on the port.
- **ForceUnauthorized** is an unauthorized state. A device connected to a port in this state never goes through the authentication process and cannot communicate on the network. To place a port in this state is the same as shutting down the port. The authenticator ignores any attempt by the supplicant to initiate authentication.
- **Auto** is an unauthorized state. A device connected to a port in this state goes through the authentication process. Successful authentication authorizes the connected device to communicate on the network. All ports’ default state is the auto state.

Note: Any port participating in dot1x authentication requires assignment of ‘dot1x authentication’ at the global and interface levels. Interfaces without ‘dot1x authentication’ are authorized by default. To globally remove ‘dot1x authentication’ is to authorize all interfaces.

The C-Series switches support dynamic VLAN assignment when using 802.1X. The process of 802.1X authentication overwrites the existing VLAN configuration of a port assigned to a non-default VLAN and assigns that port to a new specified VLAN.

To disable 802.1X authentication on a port, re-assigns the port to the previously-configured VLAN.

- Failure of 802.1X authentication on a port with authentication-fail VLAN enabled assigns the port to the authentication-fail VLAN.

Note: Configure ports using MAC-based authentication in hybrid mode, which places 802.1X-enabled ports in unauthorized state by default. Verify global enabling of 802.1X, as well as at the interface level.

In the CRA configuration, administrators must enter the global commands and interface/port specific commands that Figure 24 shows for each client port that requires authentication.

```
dot1x authentication
radius-server key 7 fea175715f6aa1df0e5759990c631269
radius-server host 10.1.100.128

interface peGigE 1/0/25
 portmode hybrid
 switchport
 dot1x authentication
 dot1x host-mode multi-auth
 dot1x mac-auth-bypass
 dot1x auth-type mab-only
 power inline
 no shutdown

interface peGigE 1/0/27
 switchport
 dot1x authentication
 no shutdown

interface Vlan 100
 ip address 10.1.100.1/24
 untagged peGigE 1/0/25,27
 untagged Port-channel 8-11
 no shutdown
```

Figure 24   802.1X authentication on C-Series access switches

4.1.1.9 VoIP QoS implementation

Today, many IT departments use softphone applications deployed on laptops and personal computers (for example, Microsoft Skype for Business) for voice communications. These applications apply DSCP markings, which can be used to ensure QoS priority across the network.

The C9010 provides eight queues to which traffic can be directed. Figure 25 shows the creation of a QoS policy on the C9010. In this case, queue five provides VoIP streams priority over other traffic. Unclassified traffic (DSCP=0) identifies best effort traffic.

```
configure

class-map match-any voice
 match ip dscp 46

policy-map-input skype_voice
 trust diffserv
 service-queue 5 class-map voice

policy-map-output Strict_Q
 service-queue 5 qos-policy VoIP_Q

qos-policy-output VoIP_Q
 scheduler strict

interface peGigE 2/0/41
 portmode hybrid
 switchport
 service-policy input skype_voice
 service-policy output Strict_Q
 no shutdown
```

Figure 25 QoS policy on the C9010 for VoIP streams

Note: There is a generic document for QOS VoIP configuration that may apply to all Dell Networking products except for strict queuing on C9010:
Reliable Skype for Business Voice with Dell Networking Switches and Wireless

4.2 Campus switching architecture using N-Series switches and MLAG

The Dell Networking N-Series-based campus switching architecture modernizes the campus network by doing the following:

- Supporting loop-free redundancy without spanning tree by using MLAG to create high availability and full bandwidth utilization
- Interfacing seamlessly with existing infrastructure for greater interoperability and integration
- Uniting various networking products with the latest open standard protocols for more network choice

The Dell Campus Switching Architecture, shown in Figure 26, is based on the MLAG feature running on the Dell Networking N-Series operating system (DNOS). Two N4064F aggregation switches form peers to each other while the two stacks of N3000-series access switches form partners to MLAG peers in this architecture. Each switch stack serves part of one floor of a campus building, which is aggregated by two 10GbE uplinks. The N4064F aggregation layer switches easily scale and support up to 24 stacks of Access switches.

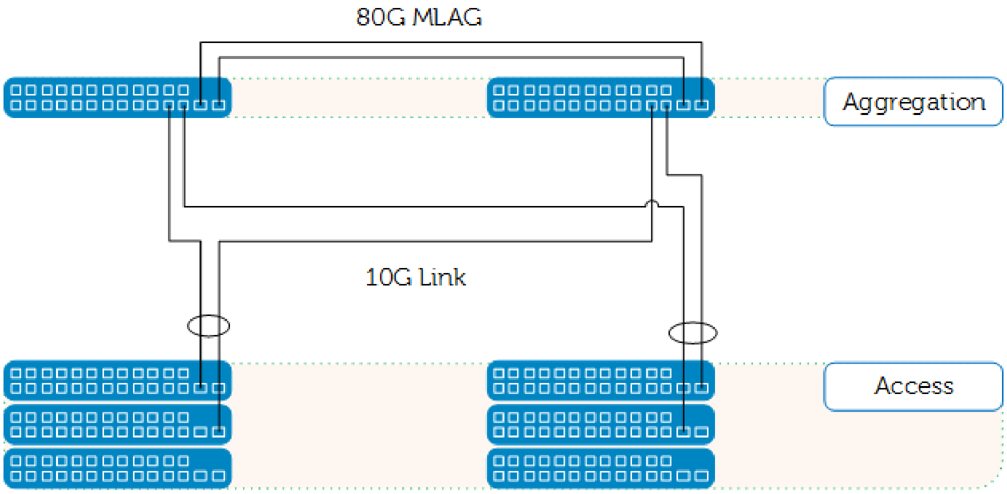


Figure 26 Dell EMC campus aggregation and access switch topology with N4000s and N3000s

This architecture provides increased bandwidth by overcoming the limitation of spanning tree to block redundant ports. The design is highly redundant in terms of both link failure and switch failure.

4.2.1 Important features and best practices

The following sections outline some of the features and guidelines to consider while designing a network.

4.2.1.1 Multi-switch Link Aggregation (MLAG)

In older network deployments, a LAG bundles redundant links between two switches. This allows the links to appear as a single link in the spanning tree topology. The advantage is that all LAG member links can be in the forwarding state allowing link failure recovery in milliseconds. This allows utilization of the bandwidth on the redundant links. However, LAGs are limited to connecting multiple links between two partner switches, which leaves the switch as a single point of failure in the topology.

Dell Networking MLAG extends the LAG's bandwidth advantage across multiple Dell Networking Switches connected to a LAG partner device. The LAG partner device is oblivious to the fact that it is connected over a LAG to two peer Dell Networking Switches; instead, the two switches appear as a single logical switch to the partner. All links carry data traffic across a physically diverse topology and in the case of a link or switch failure, traffic continues to flow with minimal disruption.

MLAGs provide an Active-Active split aggregation deployment across two switches behaving as one. MLAG creates a more resilient network with higher bandwidth capabilities.

Note: The peer link between peer switches requires configuration of a native VLAN to communicate keep-alive messages. MLAG peer switches must be from the same vendor.

Dell Networking N-Series switches provide a very flexible MLAG feature that enables creation of multiple topologies, such as those shown in Figure 27.

Note: The topologies that follow are for informational purposes only and are not part of the Large Campus deployment referenced throughout this reference architecture.

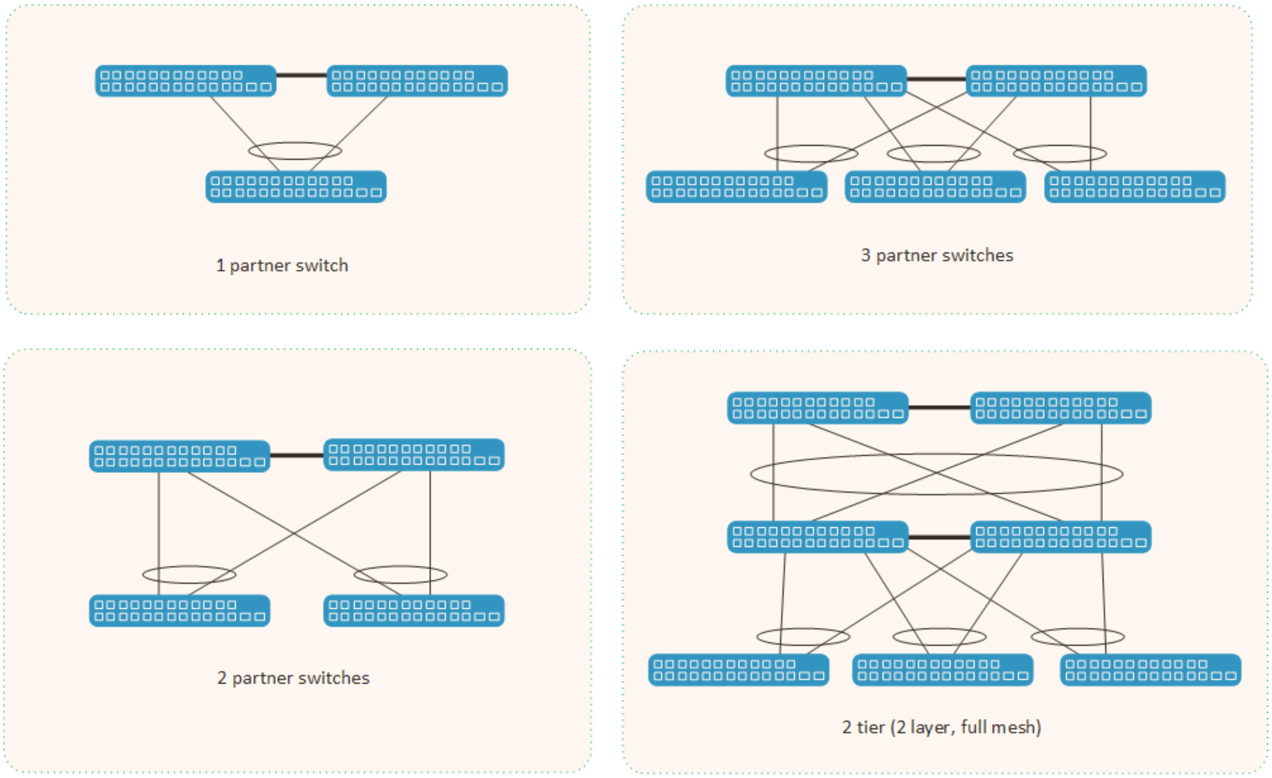


Figure 27 Examples of MLAG topologies

Note: For details on deploying MLAG on Dell Networking N-series switches, refer to the following white paper: Using MLAG in Dell Networks.

Figure 28 shows an example of MLAG configuration on the Core/Aggregation Switches (Dell Networking N4064F):

```
feature vpc
vpc domain 1
peer-keepalive enable

interface port-channel 1
description "MLAG-Peer-Link"
spanning-tree disable
switchport mode trunk
switchport trunk native vlan 100
switchport trunk allowed vlan 1-172,174-4093
vpc peer-link
exit

interface port-channel 17
description "MLAG-Partner-Link"
switchport mode trunk
switchport trunk native vlan 100
switchport trunk allowed vlan 1-172,174-4093
vpc 17
exit

interface Fo1/0/1
channel-group 1 mode active
description "MLAG-Peer-Link"
exit

interface Te1/0/17
channel-group 17 mode active
description "MLAG-Partner-link"
switchport mode trunk
switchport trunk native vlan 100
exit
```

Figure 28 MLAG configuration

Note: Throughout this document, the configuration examples contain specific VLAN, IP, or Port Channel numbers. These specific settings were used to validate the network in a lab setting. The numbers are included in the examples to allow the reader to follow the configurations.

4.2.1.2 VLANs and VLAN routing

VLANs offer a method of dividing one physical network into multiple broadcast domains. However, VLAN-enabled switches cannot forward traffic between VLANs by themselves. VLAN-to-VLAN communication requires a Layer 3 switch/router. This architecture uses Dell Networking N4064Fs as aggregation switches to handle all inter-VLAN routing activities, helping devices from two different VLAN segments to communicate.

This reference architecture discusses the configuration of several VLANs to provide what a typical large campus might need. Figure 29 shows an example of a VLAN configuration. For the full configuration of the Dell Networking N4064F used in this example, refer to the attachment.

```
vlan 5-7,57,100,173
exit
vlan 5
name "Engineering"
exit
vlan 6
name "Finance"
exit
vlan 7
name "Guest"
exit
vlan 57
name "NMS"
exit
vlan 100
name "General"
exit
vlan 173
name "Lab"
exit
vlan 200
name “VoIP”
exit
interface vlan 5
ip address 10.1.5.1 255.255.255.0
exit
interface vlan 6
ip address 10.1.6.1 255.255.255.0
exit
interface vlan 7
ip address 10.1.7.1 255.255.255.0
exit
interface vlan 50
ip address 10.1.50.2 255.255.255.0
exit
interface vlan 57
ip address 10.1.57.1 255.255.255.0
exit
interface vlan 100
ip address 10.1.100.1 255.255.255.0
exit
interface vlan 173
ip address 172.25.173.145 255.255.255.0
exit
interface vlan 200
ip address 172.25.200.1 255.255.255.0
exit
```

Figure 29 VLAN configuration example for core/aggregation switches (Dell Networking N4064F)

4.2.1.3 Spanning tree

To avoid network loops, enable MLAG on the aggregation layer switches. Links from the partner switch behave as if the switch were lagged to one peer switch and are unaware of redundant links. To be safe and prevent human error, enable spanning tree (RSTP). N-series switches support most standard spanning tree protocols. Dell EMC recommends disabling spanning tree on MLAG peer links. MLAG-based solutions support MSTP and RSTP but not RSTP-PV.

4.2.1.4 Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol (VRRP) eliminates the single-point-of-failure associated with static default routes by enabling a backup router to take over from a master router without affecting the end stations using the route. In this design, the end stations use a VRRP-defined virtual IP address as gateway.

VRRP also helps to create redundancy and greater uptime by using a secondary or backup L3 switch/router failover configuration.

Note: If VRRP is enabled on a VLAN that has an MLAG port as its member, both VRRP routers become VRRP masters operationally in the VLAN. This allows load balancing of the northbound L3 traffic on the MLAG

In this example, VRRP is configured between both Core/Aggregation Layer switches (Dell Networking N4064Fs) to provide for L3 redundancy in the event of any kind of default-route single point failure.

Figure 30 provides an example of VRRP configured on the core/aggregation switches.

```
ip vrrp
interface vlan 5
vrrp 5
vrrp 5 mode
vrrp 5 ip 10.1.5.10
vrrp 5 accept-mode
exit
interface vlan 6
vrrp 6
vrrp 6 mode
vrrp 6 ip 10.1.6.10
vrrp 6 accept-mode
exit
interface vlan 7
vrrp 7
vrrp 7 mode
vrrp 7 ip 10.1.7.77
vrrp 7 accept-mode
exit
interface vlan 57
vrrp 57
vrrp 57 mode
vrrp 57 ip 10.1.57.10
vrrp 57 accept-mode
exit
interface vlan 100
vrrp 100
vrrp 100 mode
vrrp 100 ip 10.1.100.50
vrrp 100 accept-mode
exit
```

Figure 30 VRRP configuration on core/aggregation switches (Dell Networking N4064F)

4.2.1.5 Security and authentication

With 802.1X authentication, system user authentication takes place through an internal or external server. Only authenticated and approved system users can transmit and receive frames over the port.

MAC-based authentication allows multiple supplicants connected to the same port to each authenticate individually. For example, a system attached to the port might be required to authenticate in order to gain access to the network, while a VoIP phone might not need to authenticate in order to send voice traffic through the port.

If the port is in the authorized state, the port sends and receives normal traffic without client-port-based authentication. When a port is in an unauthorized state, it ignores supplicant authentication attempts and does not provide authentication services to the client. By default, when 802.1X is globally enabled on the switch, all ports are in Auto, meaning the port is unauthorized until a successful authentication exchange takes place.

Note: By default, all ports are in VLAN Access mode. Configure ports that use MAC-based authentication in General mode

In CRA configuration, enter the global and interface-specific/port-specific commands shown in Figure 31 for each client port to be authenticated.

```
authentication enable
dot1x system-auth-control
aaa authentication dot1x default radius
radius-server host auth 10.1.100.128
name "Default-RADIUS-Server"
key "Dell1234$"
exit

interface Gi2/0/33
spanning-tree portfast
switchport mode general
switchport general pvid 57
switchport general allowed vlan add 5,57
dot1x port-control mac-based
dot1x reauthentication
dot1x timeout guest-vlan-period 3
dot1x mac-auth-bypass
authentication order dot1x mab
exit
```

Figure 31 802.1X authentication on access switches (Dell Networking N3048)

4.2.1.6 Stacking

The Dell Networking N-Series switches include a stacking feature that allows up to 12 switches to operate as a single unit. Stack switches of the same series with other members of the same series, that is, N2000 series switches stack with other N2000 switches, N3000 with other N3000, and so on. N2000 and N3000 series switches have two fixed mini-SAS stacking connectors at the rear. N4000 series switches connect through user ports located on the front panel.

Dell EMC strongly recommends keeping the stacking bandwidth equal across all stacking connections; that is, avoid mixing single and double stacking connections within a stack.

Dell EMC also strongly recommends connecting the stack in a ring topology, as shown in Figure 32, so that each switch connects to two other switches. Using this topology allows the stack to use a redundant communication path to each switch. If a switch in a ring topology fails, the stack automatically establishes a new communications path to the other switches. Switches not stacked in a ring topology may split into multiple independent stacks upon the failure of a single switch or stacking link. Also, a best practice for added resiliency is to connect uplinks from multiple stack members.

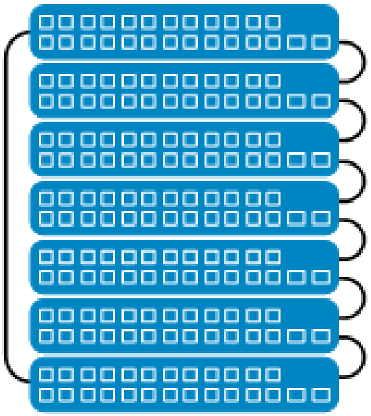


Figure 32 Stacking in ring topology

The Nonstop Forwarding (NSF) feature allows the forwarding plane of stacked units to continue to forward packets while the control and management planes restart as a result of a power failure, hardware failure, or software fault on the stack master.

Note: Today's stack-enabled switches do not support MLAG. MLAG and stacking features are mutually exclusive.

The following document provides details about stacking on Dell Networking N4000 series switches: Stacking Dell Networking Switches. Locate additional N2000 and N3000 stacking details in the 6.3
N-Series User Guide.

The CRA configuration example includes stacks of N3048P and N3048 series switches. See Figure 33 for an example configuration showing the stacking of POE, copper and fiber switches.

```
slot 1/0 2     ! Dell Networking N3024F
slot 2/0 1     ! Dell Networking N3024
slot 3/0 7     ! Dell Networking N3048P
stack
member 1 2     ! N3024F
member 2 1     ! N3024
member 3 5     ! N3048P
exit
```

Figure 33   Stacking on Dell Networking N3048 access layer switches

4.2.1.7 Quality of service

The quality of service (QoS) differentiated services (DiffServ) feature allows classification of traffic into streams of certain QoS treatment in accordance with defined per-hop behaviors.

Class of service (CoS)

The CoS queuing feature lets users directly configure certain aspects of switch queuing. This allows configuring the desired QoS behavior for different types of network traffic when traffic does not require the complexities of DiffServ. Administrators can configure minimum guaranteed bandwidth and transmission rate shaping at the queue (or port) level.

Dell N-Series switches have a total of 7 queues numbered 0 thru 6. Network control traffic commonly receives the highest queue. Therefore, the first available queue for voice traffic is usually queue 5. Network administrators should evaluate all network traffic and assign the appropriate DSCP and queue priority to each traffic type. Figure 34 shows an example of N-series VoIP CoS:

```
configure
vlan 100,200
exit

voice vlan

classofservice trust ip-dscp
classofservice ip-dscp-mapping 46 5
cos-queue random-detect 0 1
cos-queue strict 5

interface Gi5/0/1
channel-group 2 mode active
exit

interface Gi5/0/2
channel-group 2 mode active
exit

interface Gi5/0/15
spanning-tree portfast
switchport mode general
switchport general pvid 100
switchport general allowed vlan add 100
switchport general allowed vlan add 200 tagged
voice vlan 200
exit

interface port-channel 2
switchport mode trunk
switchport mode trunk allowed vlan 100,200
exit
```

Figure 34 VoIP example configuration

Note: For more information on configuring VoIP refer to the following:

Reliable Skype for Business Voice with Dell Networking Switches and Wireless

Quality of Service for Voice on Dell Networking N-Series Switches and W-Series WLAN Controllers

4.2.2 Dell Networking OS 6.3 functionality enhancements

The Dell Networking OS has made several enhancements since the release of Dell Networking Campus Switching and Mobility Reference Architecture 2.0. These enhancements can be directly applied to campus networks to enable new features, topologies, or use cases.

Note: Customers can find details on new features within the Release Notes that are included in every firmware release package. Firmware releases can be downloaded from the Drivers and downloads section of the appropriate Product Support page at Dell EMC Support.

Key features in DNOS 6.2:

RADIUS Change of Authorization

DNOS 6.2 now supports a RADIUS CoA request for session termination. This reference architecture utilizes Dell Networking W-ClearPass to manage policy and access to the network for all clients. Administrators can now use the RADIUS CoA template to terminate sessions after a change of posture in the client. W-ClearPass Onboard application can be used to monitor the client's posture to provide greater security from unauthorized changes to client devices.

Note: Customers can find the Deployment Guide titled *ClearPass NAC and Posture Assessment for Campus Networks* at Dell TechCenter.

MLAG enhancements

DNOS 6.2 now supports topologies for mixed full-mesh LAG using MLAG and VLT. This allows for a pair of VLT peers to be connected with a full-mesh LAG to a second set of MLAG peers. Customer now have greater choice in implementing redundancy through this enhanced compatibility between VLT and MLAG protocols.

Single homed devices such as servers and appliances, which do not support multi-homing, were limited to connecting through a partner switch. Single homed devices can now attach directly to one of the MLAG peers when in an MSTP environment.

Note: Customers can find details in the Deployment Guide entitled Using MLAG in Dell Networks.

5 Campus mobility architecture

Dell Networking provides a variety of products to help businesses large and small address their mobile wireless infrastructure needs. This Reference Architecture shows how Dell Networking W-Series can be used to deliver feature-rich mobile connectivity to users on the main campus, at remote branches and teleworkers.

Note: For more information on Dell W-Series Wireless Networking, refer to the Business Solutions page at Dell Wireless Networking.

5.1 W-Series controller-based WLAN

At the heart of the mobile solution are Dell Networking W-Series mobility controllers and wireless access points (APs). The controller is the central point of all wireless traffic providing access, policy enforcement, security, and traffic monitoring for wireless users. The controller is also the key integration point for W-ClearPass to provide policy enforcement, guest access, BYOD and with W-Airwave for network management features of the WLAN.

5.1.1 W-Series controller topology

The medium-to-large campus uses the tiered architecture with a core/aggregation layer and access layer as described in Chapter 3, Campus Reference Design, and Chapter 4, Campus Switching Architecture. The W-Series controllers reside on the core/aggregation layer to provide the most effective communication to the entire network.Figure 35 shows the controllers.

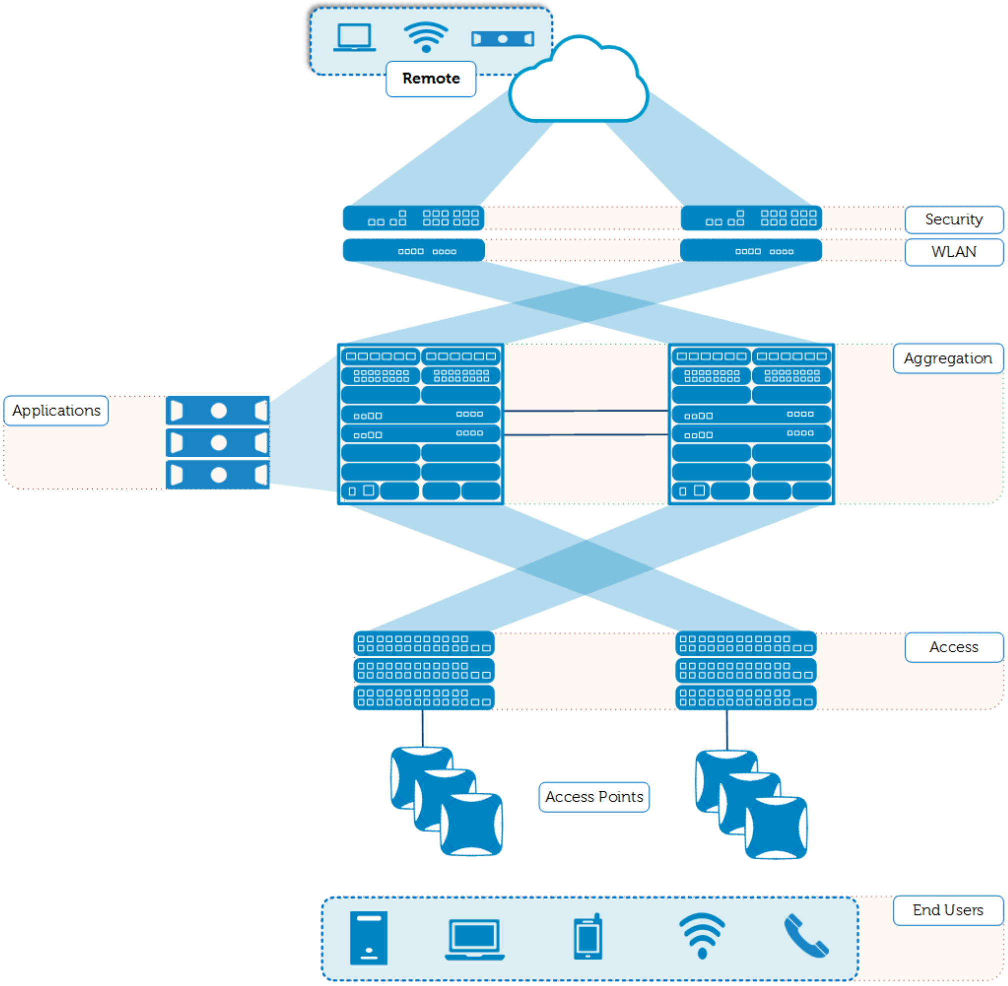


Figure 35 CRA 2.0 WLAN topology

Active LACP lags each controller to the peered Aggregation Switches using 10 GbE ports. This arrangement provides the optimal resiliency and bandwidth for the wireless traffic.

The APs placed throughout a campus building connect to (and obtain power from) the N3000 stacked switches, which typically reside in wiring closets. The PoE+ access switches included in each access stack accommodate the APs located near wiring closets on each floor. The W-Series W-AP225 802.11ac Access Points distributed on each floor of the building provide a high capacity wireless network.

5.1.2 WLAN main campus configuration

5.1.2.1 WLAN design and controller configuration

The design and configuration of the WLAN falls into two major categories: access and security. Users expect reliable access to the applications and resources needed to do their jobs. IT managers require that their networks be secure and easy to maintain. The following basic example applies key features of both areas to show how Dell Networking can satisfy campus-networking deployments.

Notes:
The configurations in the following sections are from the W-Series controllers running configuration, which is also included as an attachment to this document. This section is not intended as a step-by-step guide for configuring the W-Series controller. This document does not provide all settings.
Many of the configurations from the Standby controller are synchronized to those of the Master controller. Some of the following configurations only show the configuration from the Master controller, as the Standby configuration is identical. Those features that have significant differences show both configurations.

5.1.2.2 Master VRRP-based redundancy

WLAN networks are critical systems in today's work environment. One of the main objectives of this Reference Architecture is to provide reliable connectivity through failure-resistant features and topologies.

W-Series Controllers accomplish redundancy through High Availability and VRRP-based redundancy. Each type of failover has its advantages, but this Reference Architecture uses VRRP-based redundancy to support remote APs. Figure 36 shows the controllers and a representation of VRRP IP configuration.

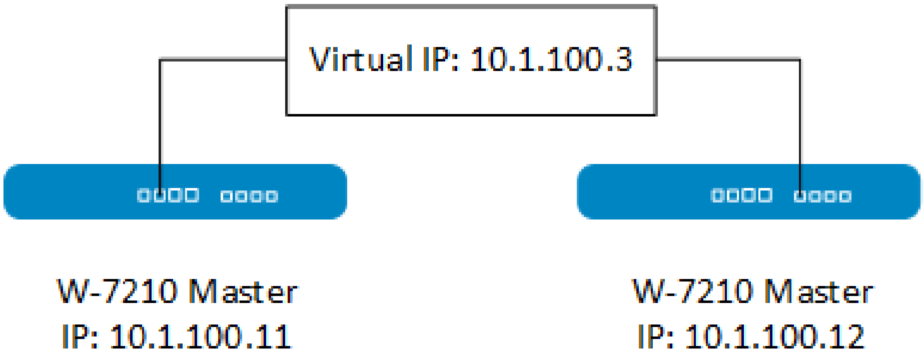


Figure 36 VRRP IP configuration

The Reference Architecture utilizes two Master controllers, one active and one standby. Figure 37 shows the CLI commands to configure the preferred Master for VRRP-based redundancy.

```
master-redundancy
  master-vrrp 99
  peer-ip-address 10.1.100.12 ipsec
04e416a543f7b1018c15f886a0b3d54cd9898e4ed7932291

vrrp 99
  priority 120
  authentication password
  ip address 10.1.100.3
  description "Preferred-Master"
  vlan 100
  no shutdown
```

Figure 37 Configuring preferred master for VRRP

Figure 38 shows the CLI commands to configure the Standby for VRRP-based redundancy.

```
master-redundancy
  master-vrrp 99
  peer-ip-address 10.1.100.11 ipsec
9231d00edf8b5207e5b982f3ce710c3f4b9a2c0a1080e496
!
vrrp 99
  authentication password
  ip address 10.1.100.3
  description "Backup-Master"
  vlan 100
  no shutdown
```

Figure 38 Configuring standby for VRRP

5.1.2.3 Centralized licensing

W-Series controllers feature the ability to use centralized licensing. This enables controllers to share a pool of licenses installed on each controller in the network. This Reference Architecture only shows a single active controller in operation at any given time. If a failure occurs, the standby controller uses the licenses installed on the preferred Master. This feature reduces the cost of having to install licenses on the standby. Figure 39 shows the command to enable centralize licensing:

```
license profile
   centralized-licensing-enable
```

Figure 39 Centralized licensing

Note: Refer to the AOS 6.3 User Guide at the Dell Networking Support Site for more information on centralized licensing.

Topologies consisting of dedicated active and redundant standby controllers automatically set the primary and backup licensing servers.

5.1.2.4 LACP and port channels

W-Series controllers connect to the Core/Aggregation Layer through 10 GbE DAC or Optical cable. Each controller connects to both Dell Networking N4000 switch MLAG peers or to C-Series VLT peers. The MLAG configuration of the two Aggregation Switches presents the switches to the controller as a single switch. Refer to the Campus Switching Architecture section for more information on how MLAG enables reliable data traffic in the presence of multiple failures.

Figure 40 shows the CLI configuration for the connections to the aggregation layer. The Master and Standby controllers' configurations are similar to each other.

```
interface gigabitethernet 0/0/2
      description "GE0/0/2"
      trusted
      trusted vlan 1-4094
      switchport mode trunk
      switchport trunk native vlan 100
      switchport trunk allowed vlan 1,5-7,57,100
      lacp group 2 mode active

interface gigabitethernet 0/0/3
      description "GE0/0/3"
      trusted
      trusted vlan 1-4094
      switchport mode trunk
      switchport trunk native vlan 100
      switchport trunk allowed vlan 1,5-7,57,100
      lacp group 2 mode active

interface port-channel 2
      trusted
      trusted vlan 1-4094
      switchport mode trunk
      switchport access vlan 99
      switchport trunk native vlan 100
      switchport trunk allowed vlan 1-172,174-4094
```

Figure 40 Configuration of controller-to-aggregation switches connection

5.1.2.5 VLAN assignments

VLAN configuration and assignment is identical to that for wired switches in Chapter 4, Campus Switching Architecture. As users connect to the network, policy enforcement applies their roles and assigns their VLANs. This reference architecture describes policy enforcement accomplished through W-ClearPass and the W-Series Controllers.

CRA VLANs separate traffic into the following pre-defined categories:

- VLAN 5 – Engineering VLAN
- VLAN 6 – Finance VLAN
- VLAN 7 – Guest VLAN
- VLAN 57 – Network Management and Windows Server VLAN
- VLAN 100 – Native VLAN and W-ClearPass

Figure 41 shows the commands to configure and assign the VLANs:

```
vlan 5
vlan 6
vlan 7
vlan 57
vlan 100

interface vlan 100
      ip address 10.1.100.11 255.255.255.0

interface vlan 1
      ip address 10.1.1.3 255.255.255.0

interface vlan 57
      ip address 10.1.57.4 255.255.255.0

interface vlan 5
      ip address 10.1.5.4 255.255.255.0

interface vlan 6
      ip address 10.1.6.4 255.255.255.0

interface vlan 7
      ip address 10.1.7.4 255.255.255.0
```

Figure 41 Wireless controller VLAN configuration

5.1.2.6 DHCP

This design configures the DHCP server within the W-Series controller. Figure 42 shows the DHCP configurations for each subnet.

> **Note:** The configuration and location of the DHCP server in this reference architecture supports the validation of the architecture. Best practice is to utilize an external DHCP server. IT managers can deploy their own DHCP server solution that satisfies their specific requirements and preferences.

```
ip dhcp pool Guest
 default-router 10.1.7.77
 dns-server 10.1.57.127
 domain-name cra.lab
 lease 1 0 0 0
 network 10.1.7.0 255.255.255.0
 authoritative
!
ip dhcp pool Eng
 default-router 10.1.5.10
 dns-server 10.1.57.127 172.25.10.1
 domain-name cra.lab
 lease 1 0 0 0
 network 10.1.5.0 255.255.255.0
 authoritative
!
ip dhcp pool Finance
 default-router 10.1.6.10
 dns-server 10.1.57.127 172.25.10.1
 domain-name cra.lab
 lease 1 0 0 0
 network 10.1.6.0 255.255.255.0
 authoritative
!
ip dhcp pool CRA
 default-router 10.1.100.3
 dns-server 10.1.57.127 172.25.10.1
 domain-name cra.lab
 lease 1 0 0 0
 network 10.1.100.0 255.255.255.0
 authoritative
!
service dhcp
```

Figure 42 DHCP configurations

5.1.2.7 WLAN access point groups

Deployed APs receive provisioning when included in AP Groups. An AP Group is a set of configurations that contain the profiles defining how each AP in the group operates. Each AP can only be assigned to one AP Group. This Reference Architecture contains a single AP Group named *CRA_Employee.*

Many of the settings within the AP Group in this Reference Architecture are kept as default. These include the RF Management, AP interface, Regulatory Domain, QOS, and IDS settings. You can change these default settings to suit your IT organization without affecting the interoperability of the features used in this reference architecture.

The AP Group *CRA_Employee* includes the following configurations:

- ap-group
- wlan virtual-ap
- wlan ssid profile

ap-group

Figure 43 shows the top level ap-group setting, which defines two virtual APs – one for employee access, *CRA_Employee,* and another for guest access, *CRA_Guest-vap_prof.*

```
ap-group "CRA_Employee"
   virtual-ap "CRA_Employee"
   virtual-ap "CRA_Guest-vap_prof"
```

Figure 43 AP group settings

Note: The “vap_prof” extension on the guest access virtual-ap variable is automatically appended when the administrator uses the AP wizard within the web GUI. The appended text identifies the type of setting and can be useful when reviewing the text-based configuration file.

wlan virtual-ap

Figure 44 shows the wlan virtual-ap settings, which associate the profiles defined for SSID, AAA, and define the VLAN assignment users receive when connecting to the virtual APs.

```
wlan virtual-ap "CRA_Employee"
   aaa-profile "CP_dot1x_profile"
   ssid-profile "CRA_Employee"
   vlan 100
!
wlan virtual-ap "CRA_Guest-vap_prof"
   aaa-profile "CP_Guest_profile"
   ssid-profile "CRA_Guest-ssid_prof"
   vlan 7
```

Figure 44 WLAN virtual AP settings

wlan ssid-profile

Figure 45 shows the wlan ssid-profile settings that define the ESSID and the authentication/encryption used for each WLAN. This architecture uses WPA2-AES for 802.1X on the Employee SSID, while the Guest SSID is open.

```
wlan ssid-profile "CRA_Employee"
   essid "CRA_Employee"
   opmode wpa2-aes
wlan ssid-profile "CRA_Guest-ssid_prof"
   essid "CRA_Guest"
```

Figure 45 WLAN SSID profile settings

5.1.2.8 WLAN security – AAA

W-Series controllers contain the profiles, user roles and authentication settings to enable the policy enforcement for all wireless users. In this reference architecture example, the W-Series controller utilizes W-ClearPass as its authentication server. A partial list of other acceptable sources of authentication servers includes RADIUS, AD (Active Directory), LDAP (Lightweight Directory Access Protocol), and TACACS.

User roles are groups of firewall policies that are assigned based on the status and attributes of the user and device accessing the network. The W-Series controller contains the user roles, while the W-ClearPass policy manager assigns them.

This section shows the configuration of the W-Series controller. To get the entire picture of user evaluation and user role assignment, refer to Section 5.3, W-ClearPass Access Management.

aaa server settings

The aaa server settings example in Figure 46 shows the profile and server configurations to set W-ClearPass as the 802.1X and RADIUS servers:

```
aaa authentication dot1x "cra-CRA_Employee"
   timer reauth-period 32400
   max-requests 2
   timer wpa-key-period 3000
   timer wpa2-key-delay 100
   timer wpa-groupkey-delay 100
   reauthentication
aaa authentication-server radius "cra-CRA_Employee"
   host "10.1.100.128"
   key 0a6efcd6079b7850ba2ea65c0a9ccff6c2ae8fa08960dae2
   nas-identifier "CRAcontroller"
   nas-ip 10.1.100.3
   mac-lowercase
```

Figure 46 aaa server settings

dot1x aaa profiles, user roles, and access lists

Figure 47 shows the assignment of the *CRA_Employee* SSID to the aaa profile *CP_dot1x_profile* described in the wlan virtual-ap section. Figure 47 also shows the profile. Note the initial-role setting under the aaa profile. When a user logs into the network, they receive their initial-role assignment, limiting their access until they are authenticated. In this example, the initial-role is *CRA_Employee-logon.*

```
aaa profile "CP_dot1x_profile"
   initial-role "CRA_Employee-logon"
   authentication-dot1x "cra-CRA_Employee"
   dot1x-server-group "clearpasscra"
   radius-accounting "clearpasscra"
   radius-interim-accounting
   rfc-3576-server "10.1.100.128"

user-role CRA_Employee-logon
 vlan 100
 captive-portal "CRA_Employee"
 access-list session ra-guard
 access-list session CRA_Employee-logon-control
 access-list session CRA_Employee-allow-external-captive-portal
 access-list session CRA_Employee-allow-google-play
 access-list session CRA_Employee-captiveportal

ip access-list session CRA_Employee-allow-external-captive-portal
  user host 10.1.100.128 svc-http  permit
  user host 10.1.100.128 svc-https  permit
  user   alias CRA_Employee-allow-external-captive-portal svc-http  permit
  user   alias CRA_Employee-allow-external-captive-portal svc-https  permit
```

Figure 47 Dot1x aaa profiles, user roles and access lists

Further examination of the *CRA_Employee-logon,* shows an access list for an external captive portal. This example is part of a BYOD configuration, where devices that have not been provisioned are directed to a portal that enables a certificate to be installed. The provisioning feature used is part of W-ClearPass Onboard, which will be discussed in a later section. Note that the access list for the external captive portal only allows specific traffic to the W-ClearPass server.

There are several profiles, user-roles, and firewall rules that enable the features discussed in this reference architecture. They can be seen in the controller configurations attached to this document.

5.1.2.9 Controller configuration for remote APs in a branch site

The objective is to have the Remote Branch site be an extension of the Main Campus; that is, providing the same type of access to Branch Office users as if they were in the Main Campus. This Reference Architecture contains a remote Instant Access Point solution. To enable the users at the remote site to access resources located at the corporate site, a VPN is established between the Instant AP and the W-Series controller. Figure 48 shows the VPN connection. The VPN tunnel is established across the WAN (Internet), through the firewall using NAT, and then routed by the Aggregation Layer to the controller. Depending on the size of the Remote Branch, one or more Instant Access Points and scalable number of wired ports will be required.

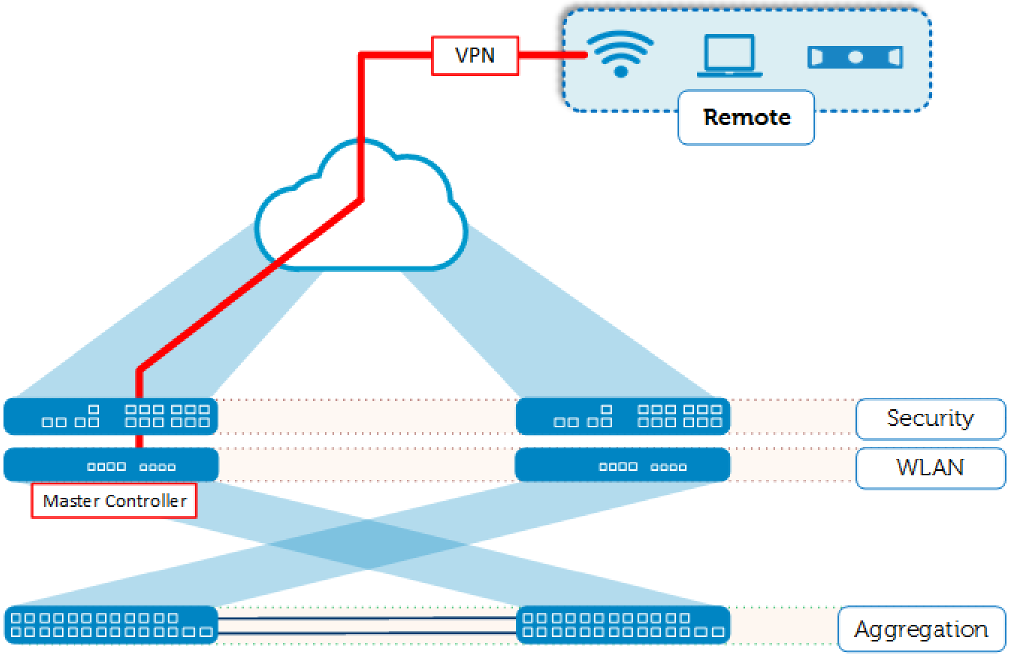
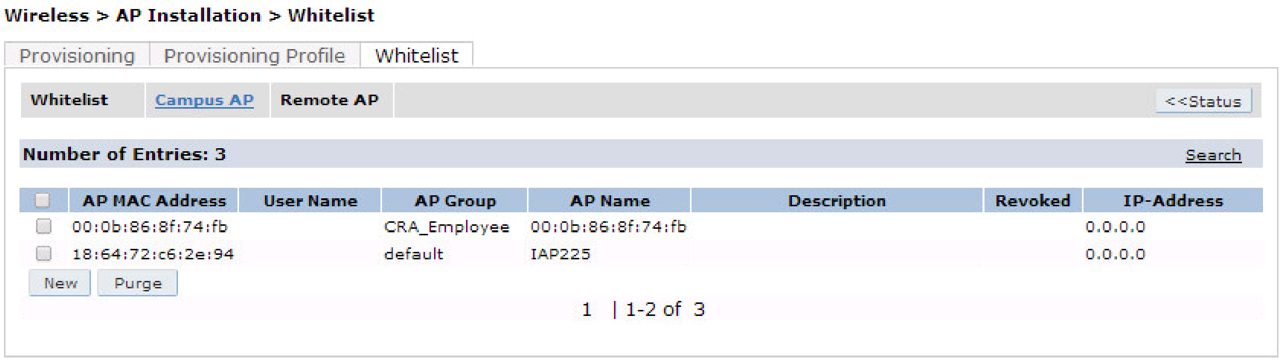


Figure 48 VPN connection from remote branch office to the main campus

In this example, the VPN IPsec parameters, roles, and profiles are all kept at the default settings. No explicit configuration is required except for the access points establishing a VPN connection to be added to the Remote AP Whitelist in the Mobility Controller on the Main Campus.

Figure 49 shows the AP's MAC addresses added to the Remote AP Whitelist**.** The IP address for the VPN termination is set to 0.0.0.0 to enable an address pool to be utilized instead of static addresses.



Number of Entries: 3

☐	AP MAC Address	User Name	AP Group	AP Name	Description	Revoked	IP-Address
☐	00:0b:86:8f:74:fb		CRA_Employee	00:0b:86:8f:74:fb			0.0.0.0
☐	18:64:72:c6:2e:94		default	IAP225			0.0.0.0

1 | 1-2 of 3

Figure 49 Remote AP whitelist

Figure 50 shows the configuration of the address pool.

```
ip local pool "rappool" 10.1.100.82 10.1.100.84
```

Figure 50 Address pool

5.1.2.10 Network management

Figure 51 shows setting up the SNMP community strings for both Open Manage Network Manager and W-Airwaves as required by the Network Management solution. Additionally, W-Airwave requires a specific server IP setting.

```
syslocation "austin-rr-campus"
syscontact "abc@dell.com"
snmp-server community "test123"

snmp-server enable trap
snmp-server host 10.1.57.100 version 2c test123 udp-port 162
```

Figure 51 SNMP community strings

5.2 W-Series Instant Access Point – remote deployments

W-Series Instant Access Points provide enterprise level features through a built-in virtual controller. W-Instant Access Points feature an easy to use interface with minimal IT deployment interaction. These products are able to fulfill many of the IT manager's requirements in any campus setting. This Reference Architecture focuses on using W-Instant at remote sites or with teleworkers.

Replicating corporate resources is cost prohibitive, or not feasible due to the nature of the data and services that need to be accessed. W-Instant can provide workers at these remote sites access to all the corporate resources at the main facility. The next two sections describe Dell Networking's two options to help solve the IT manager's requirements at remote sites.

5.2.1 W-Series Instant Access Point networks

In the case of a remote site, where maintaining a separate managed wireless network and a connection to the main corporate building is required, a W-Instant Access Point can be used. W-IAPs are full featured APs that contain virtual controller technology built into each AP. When W-IAPs are used together on the same subnet, they form clusters where a single IAP will assume control as the Master Virtual Controller. W-IAPs are an easy way to deploy and scale at such sites.

W-IAPs contain a VPN that can be terminated at a W-Series controller located within the main campus. The master virtual controller will establish a single VPN connection to the controller. This Reference Architecture uses this VPN mechanism to allow users at the remote site to access resources within the main corporate site. Key resources such as W-ClearPass and Active Directory can be used through the VPN connection.

Instant configuration examples can be seen by accessing the attachment titled, *Dell Networking W-Instant Configuration*.

5.2.2 W-Series Instant Access Points for teleworkers

Teleworkers require the same access to corporate resources that their co-workers have on the corporate campus or branch offices. The growing trend of employees or contractors working from their home offices makes this an important use case.

A historical solution was to install a VPN client on the user's PC and their mobile devices and maintain a VPN infrastructure at the offices. Dell Networking W-Series provides a solution that is easier to deploy and does not require finding VPN software for the different device types, while providing a full context-aware user policy managed solution.

W-Instant products provide an excellent solution to provide teleworkers with the same network access in their home or while traveling. IT managers can use W-Instant products to significantly simplify and reduce resources needed to manage and distribute access points to teleworkers.

W-Series controllers have an ability to manage APs at remote sites across the WAN. IPsec tunnels are used for control traffic and the remote APs act very similar to APs within the local campus. The same SSIDs and setting used for campus APs are available to the Remote APs.

Traditional APs and W-Instant APs have the ability to operate as controller based remote APs. However, the W-Instant APs have an advantage in the ease of setup and deployment at the remote site. Since the W-IAP can boot and become operational through its Instant Software without expert IT assistance, this enables teleworkers to deploy a remote AP without a physical IT presence.

When a W-IAP is taken from its box, all that is needed is an AC power connection, and a wired network connection to a cable/internet modem. Simple, easy to follow instructions are included in the box. With additional instructions from the teleworker’s IT department on converting the W-IAP to a remote AP, the teleworker can have corporate network access in no time.

In this Reference Architecture, the W-IAP155 is used as a teleworker solution, and it provides both wired and wireless connectivity at the teleworker's location, including PoE Sourcing ports if needed. For a travelling user, the IAP can be plugged into a hotel's Ethernet port and turn the hotel room into a fully policy managed office.

An example covering the Conversion of a W-IAP into a Remote AP can be seen by accessing the attachment titled, *Dell Networking W-Instant Configuration*.

5.3 W-ClearPass Access Management

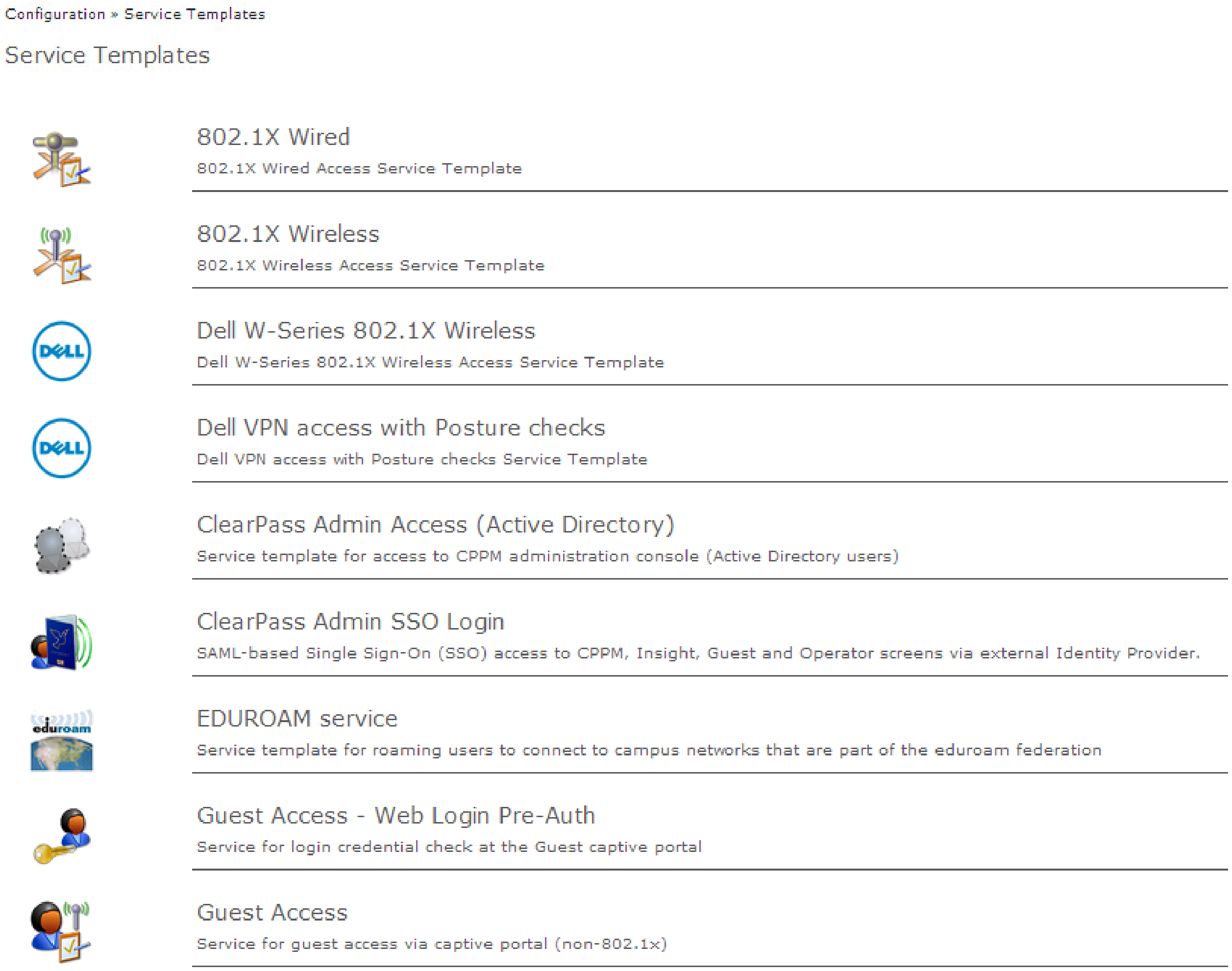
Dell Networking W-series ClearPass is a powerful solution for policy management, BYOD, and Guest access. It integrates seamlessly with the W-Series controller-based products and W-Instant Access Points. In this section, several examples are presented to show how W-ClearPass can be used to provide access to network resources, to the approved personnel, using IT approved devices.

5.3.1 W-ClearPass Policy Manager

Dell Networking W-ClearPass Access Management appliance is divisible into several modular pieces. The base of the system is the ClearPass Policy Manager (CPPM). This is the main module that holds the administrative server settings, RADIUS and other built-in databases, and the configured services.

W-ClearPass services are containers that hold the Identification, Authentication, Authorization, Role Mapping, and Enforcement policies to accomplish a policy management task. Some examples of services include 802.1X, MAC Authentication, and Web Authentication.

Figure 52 shows the templates that W-ClearPass provides for administrators for many of the most common service types. These templates include all the basic settings typically used for a particular service.



Configuration » Service Templates

Service Templates

802.1X Wired
802.1X Wired Access Service Template

802.1X Wireless
802.1X Wireless Access Service Template

Dell W-Series 802.1X Wireless
Dell W-Series 802.1X Wireless Access Service Template

Dell VPN access with Posture checks
Dell VPN access with Posture checks Service Template

ClearPass Admin Access (Active Directory)
Service template for access to CPPM administration console (Active Directory users)

ClearPass Admin SSO Login
SAML-based Single Sign-On (SSO) access to CPPM, Insight, Guest and Operator screens via external Identity Provider.

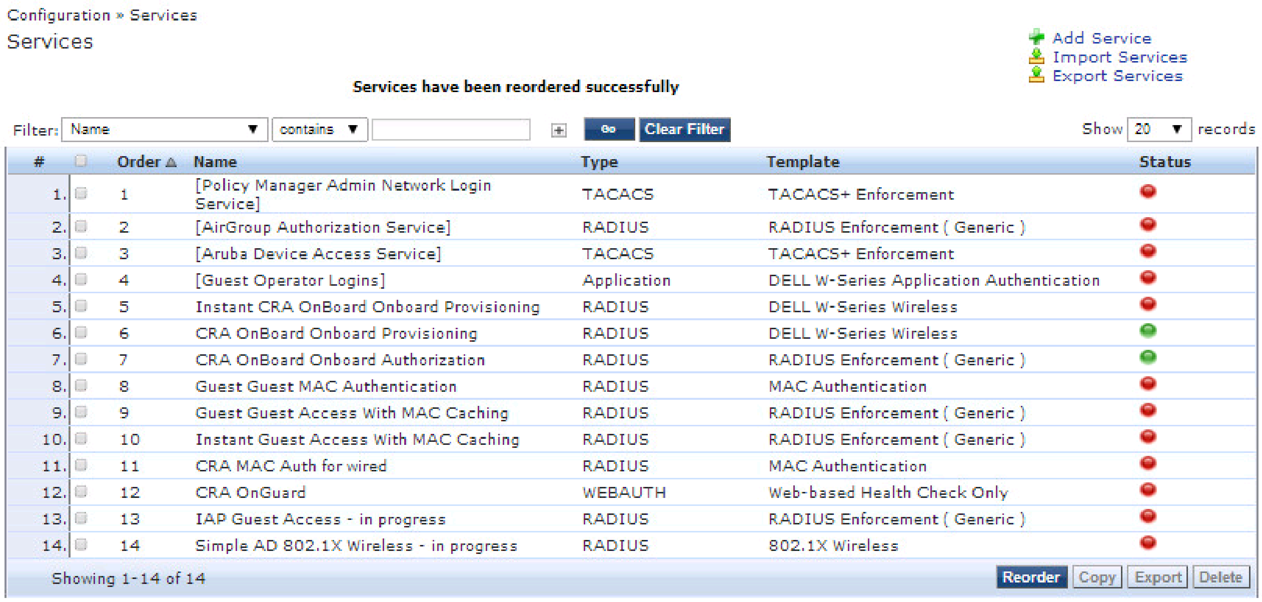
EDUROAM service
Service template for roaming users to connect to campus networks that are part of the eduroam federation

Guest Access - Web Login Pre-Auth
Service for login credential check at the Guest captive portal

Guest Access
Service for guest access via captive portal (non-802.1x)

Figure 52 W-ClearPass service templates

Once a service has been configured it is placed into an ordered list. Authentication requests from Network Authentication Devices are evaluated starting at the top of the Services list and moving to the bottom, as Figure 53 shows.



Configuration » Services

Services

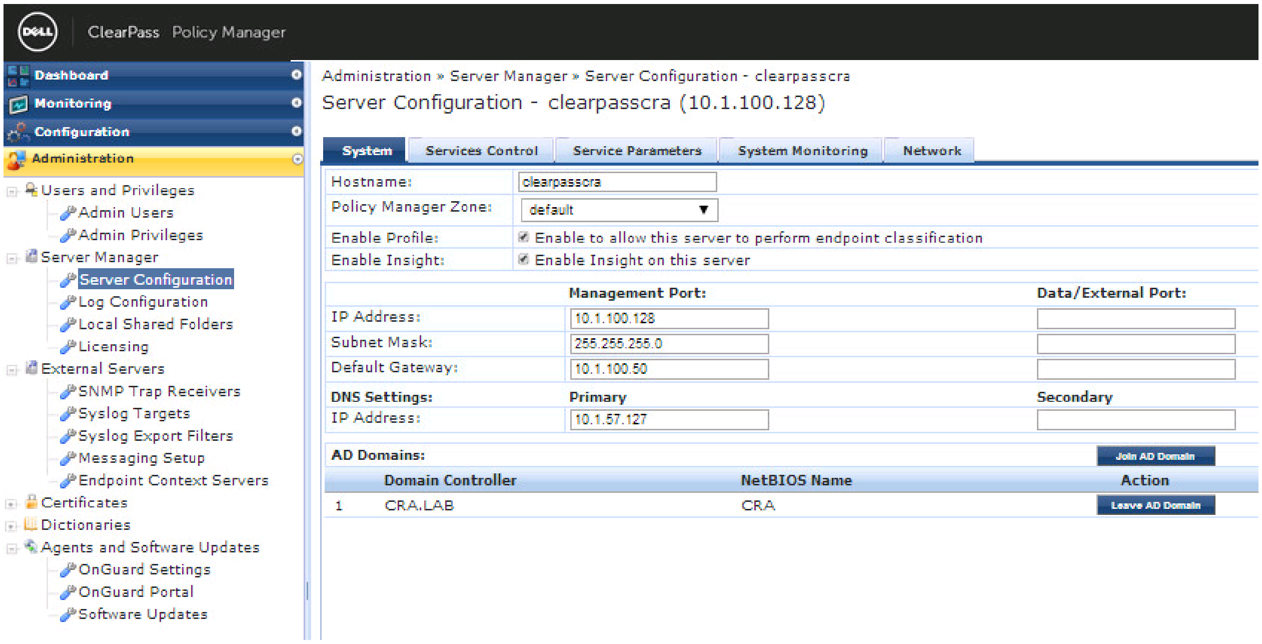
Services have been reordered successfully

#	□	Order ▲	Name	Type	Template	Status
1.	□	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	🔴
2.	□	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	🔴
3.	□	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	🔴
4.	□	4	[Guest Operator Logins]	Application	DELL W-Series Application Authentication	🔴
5.	□	5	Instant CRA OnBoard Onboard Provisioning	RADIUS	DELL W-Series Wireless	🔴
6.	□	6	CRA OnBoard Onboard Provisioning	RADIUS	DELL W-Series Wireless	🟢
7.	□	7	CRA OnBoard Onboard Authorization	RADIUS	RADIUS Enforcement (Generic)	🟢
8.	□	8	Guest Guest MAC Authentication	RADIUS	MAC Authentication	🔴
9.	□	9	Guest Guest Access With MAC Caching	RADIUS	RADIUS Enforcement (Generic)	🔴
10.	□	10	Instant Guest Access With MAC Caching	RADIUS	RADIUS Enforcement (Generic)	🔴
11.	□	11	CRA MAC Auth for wired	RADIUS	MAC Authentication	🔴
12.	□	12	CRA OnGuard	WEBAUTH	Web-based Health Check Only	🔴
13.	□	13	IAP Guest Access - in progress	RADIUS	RADIUS Enforcement (Generic)	🔴
14.	□	14	Simple AD 802.1X Wireless - in progress	RADIUS	802.1X Wireless	🔴

Showing 1-14 of 14

Figure 53 ClearPass services list

Figure 54 shows the first section of the server configuration screen. This section contains the basic settings for the W-ClearPass server, including network settings and joining a Windows Active Directory domain.



Administration » Server Manager » Server Configuration - clearpasscra

Server Configuration - clearpasscra (10.1.100.128)

Hostname: clearpasscra

Policy Manager Zone: default ▼

Enable Profile: ☑ Enable to allow this server to perform endpoint classification

Enable Insight: ☑ Enable Insight on this server

	Management Port:	Data/External Port:
IP Address:	10.1.100.128	
Subnet Mask:	255.255.255.0	
Default Gateway:	10.1.100.50	
DNS Settings:	**Primary**	**Secondary**
IP Address:	10.1.57.127	

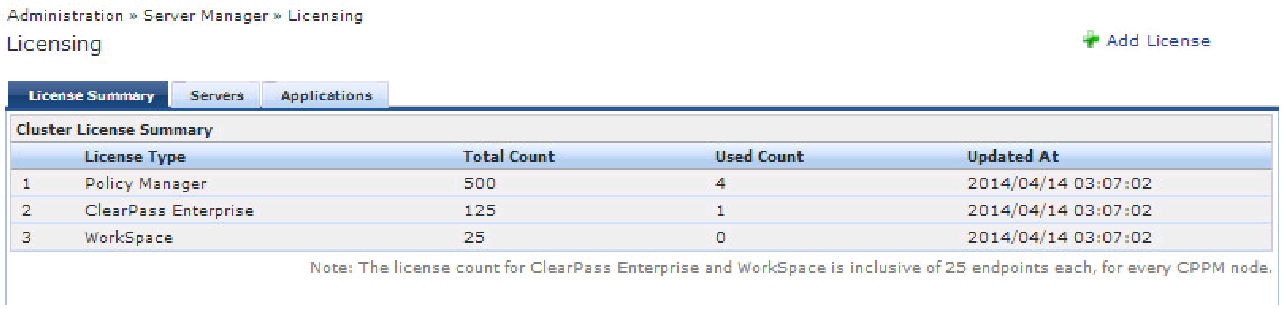
AD Domains:

	Domain Controller	NetBIOS Name	Action
1	CRA.LAB	CRA	Leave AD Domain

Figure 54 Server configuration screen

W-ClearPass Policy Manager licensing capacity varies according to the appliance model purchased. W-ClearPass (Onboard, OnGuard, and Guest) operation and client service requires licensing for those add-on features, as Figure 55 shows. Generally, the number of endpoints determines required licensing.

Note: For more information on W-ClearPass licensing refer to the W-ClearPass User's Guides at Dell EMC's Support Site



Administration » Server Manager » Licensing

Licensing

Add License

License Summary | Servers | Applications

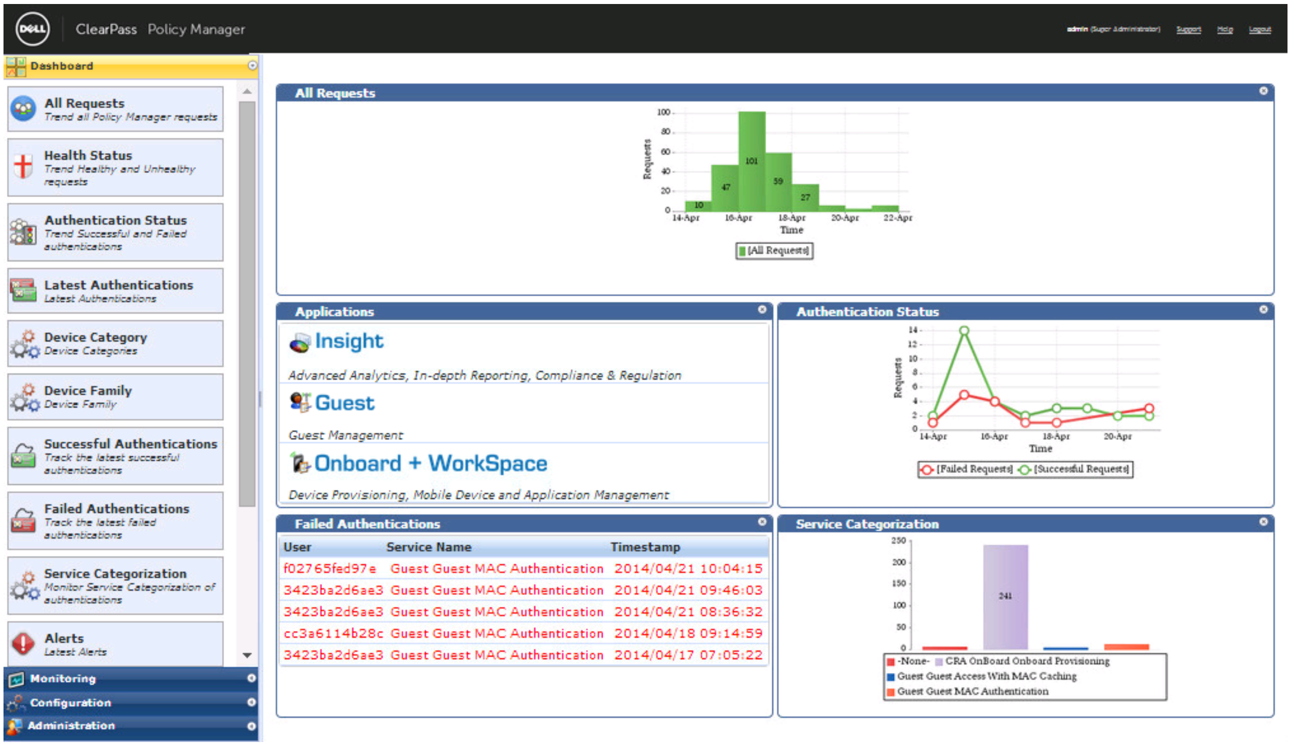
Cluster License Summary

	License Type	Total Count	Used Count	Updated At
1	Policy Manager	500	4	2014/04/14 03:07:02
2	ClearPass Enterprise	125	1	2014/04/14 03:07:02
3	WorkSpace	25	0	2014/04/14 03:07:02

Note: The license count for ClearPass Enterprise and WorkSpace is inclusive of 25 endpoints each, for every CPPM node.

Figure 55 W-ClearPass Licensing screen

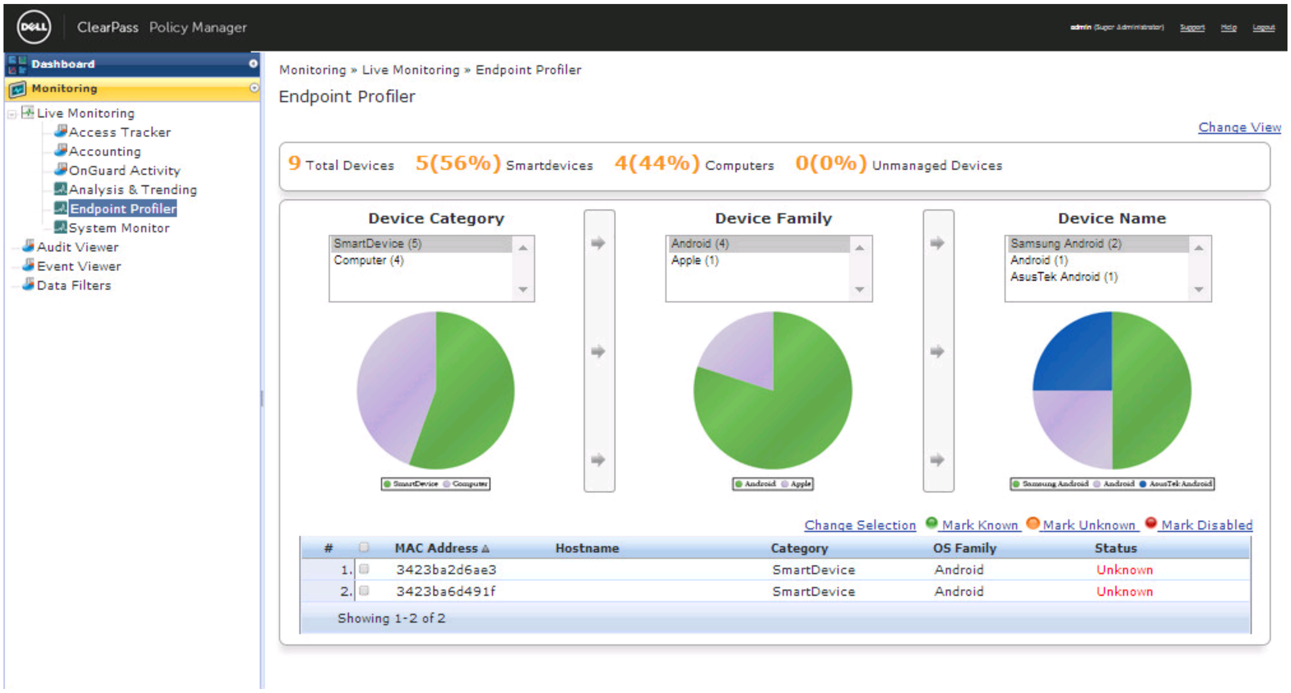
Monitor the network through the W-ClearPass Policy Manager, as Figure 56 shows. The W-ClearPass Policy Manager contains user-friendly interfaces to track the status of predefined categories. Change the Dashboard (located on the far left of Figure 56) using a simple drag and drop action.



User	Service Name	Timestamp
f02765fed97e	Guest Guest MAC Authentication	2014/04/21 10:04:15
3423ba2d6ae3	Guest Guest MAC Authentication	2014/04/21 09:46:03
3423ba2d6ae3	Guest Guest MAC Authentication	2014/04/21 08:36:32
cc3a6114b28c	Guest Guest MAC Authentication	2014/04/18 09:14:59
3423ba2d6ae3	Guest Guest MAC Authentication	2014/04/17 07:05:22

Figure 56 W-ClearPass Policy Manager window

W-ClearPass has extensive graphical and logging abilities to monitor every authentication request. Figure 57 shows the Endpoint Profiler.



Endpoint Profiler

9 Total Devices 5(56%) Smartdevices 4(44%) Computers 0(0%) Unmanaged Devices

Device Category	Device Family	Device Name
SmartDevice (5)	Android (4)	Samsung Android (2)
Computer (4)	Apple (1)	Android (1)
		AsusTek Android (1)

#	□	MAC Address ▲	Hostname	Category	OS Family	Status
1.	□	3423ba2d6ae3		SmartDevice	Android	Unknown
2.	□	3423ba6d491f		SmartDevice	Android	Unknown

Showing 1-2 of 2

Figure 57 Endpoint Profiler window

5.3.2 W-ClearPass applications

W-ClearPass Applications enable key features and policies of the Policy Manger. This reference architecture describes and validates Onboard, Guest, and OnGuard.

5.3.2.1 W-ClearPass Onboard for employee personal devices

The Onboard application within W-ClearPass enables IT managers to provide a BYOD service to their users. Onboard helps to configure and provision the most popular devices and operating systems on the market.

The key advantage to Onboard is the ability to use W-ClearPass and its built-in certificate authority. By providing a self-service portal and application to provision the device, users obtain network access without a complicated IT process.

This reference architecture validates Onboarding through both the W-Series controller based and Instant WLAN products. Users experience the same Onboarding process whether they are at the main campus or at a remote site. In addition, users who register their device at one site do not have to re-register it at another site.

The attachment entitled, *Dell Networking W-ClearPass Configuration* shows configuration examples for both W-ClearPass Policy Manager and Onboard.

5.3.2.2 W-ClearPass Guest

The Guest application within W-ClearPass enables IT managers to provide a Guest-access solution to visitors on their campus. W-ClearPass Guest allows for a safe and effective way for IT administrators to control network resources with minimal IT resources.

W-ClearPass Guest provides many options to the IT Manager. Guests' approval credentials come from a Guest Administrator, who is typically located at the front desk or reception. IT managers can also allow for a guest self-registration portal, with automatic or sponsor initiated approval.

This reference architecture validates guest access through both the W-Series controller based and Instant WLAN products. Users experience the same Guest access process whether they are at the main campus or at a remote site.

The attachment titled, *Dell Networking W-ClearPass Configuration* contains onboarding examples and shows configuration examples for both W-ClearPass Policy Manager and Guest.

5.3.2.3 W-ClearPass OnGuard

The OnGuard application within W-ClearPass enables advanced posture assessments and health checks of devices that are on the network, or requesting access to the network. OnGuard can be used as a persistent application or as a dissolvable agent used at the time of network access.

With the release of Dell Networking OS 6.2 on N-Series, RADIUS CoA can now be used with OnGuard to enable posture checks on wired clients. Any undesirable change to the health or posture on a client using the persistent application will trigger a re-authentication. The client can then be redirected to the appropriate quarantine VLAN until the issue is resolved.

Note: Additional content on OnGuard can be found in the Deployment Guide titled *ClearPass NAC and Posture Assessment for Campus Networks* at Dell TechCenter.

6 Campus Network Management System

6.1 OpenManage Network Manager

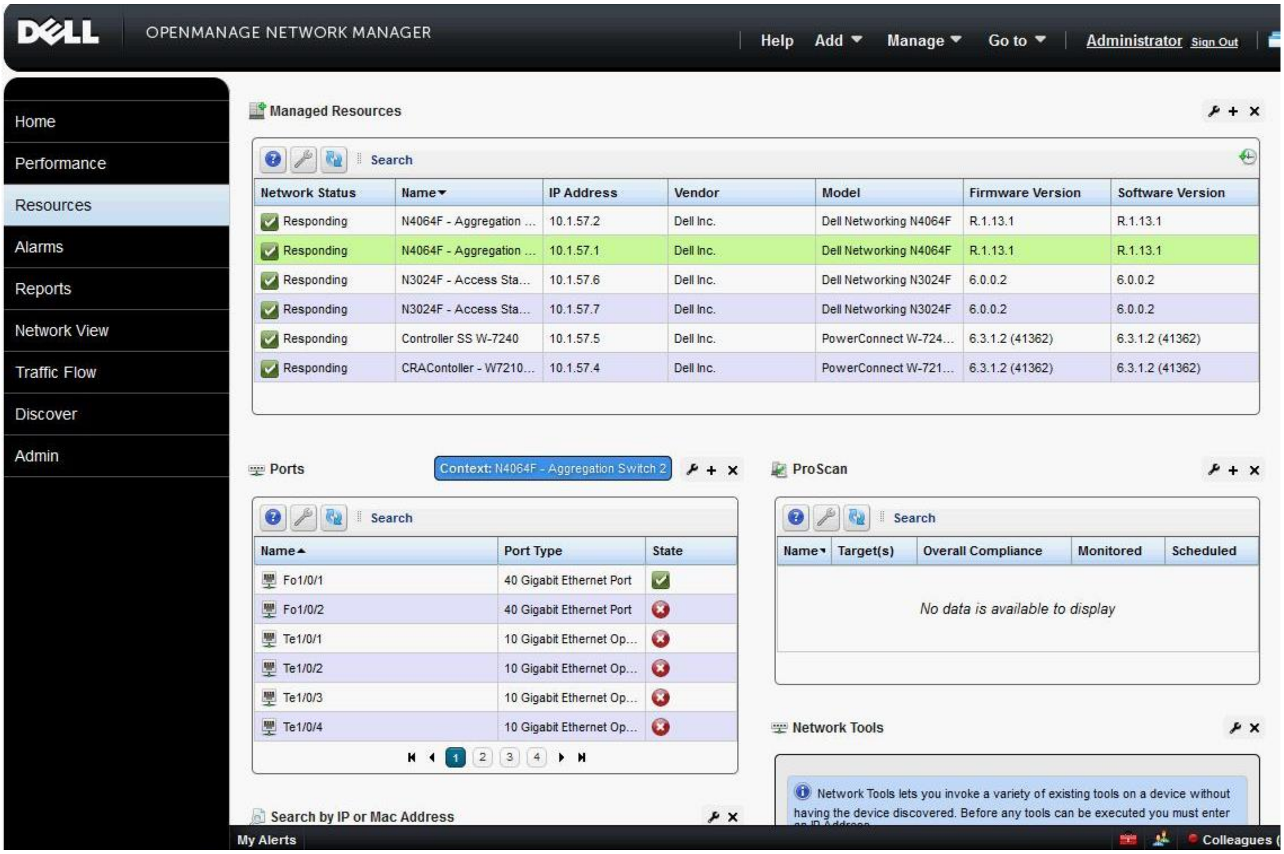
Dell Networking OpenManage Network Manager (OMNM) is Dell Networking's Tier 1 Network Management System (NMS) solution for all datacenter, campus and branch large-group switches. OMNM also provides seamless management for whole-campus networks. OMNM makes it easy to automate labor-intensive tasks while monitoring and managing the entire Dell Network-Switching infrastructure. A major benefit of OMNM is that it also has the capability to manage 3rd party network devices from Cisco, HP, Juniper, Aruba, Brocade and hundreds of other devices.

OMNM centralizes management for Dell Networking environments by providing discovery, monitoring, reporting and configuration management for the entire Dell Networking family of products.

OMNM provides the following advantages:

- Automates the discovery of network devices, and provides detailed information on the devices and their connectivity, including the ability to draw physical and logical topology maps.
- Provides the ability to easily configure and manage groups of Dell Network devices. OMNM can make configuration changes and firmware deployments to multiple devices in one operation as well as schedule many network operations ahead of time.
- Enables the network administrator to monitor the health and performance of their Dell Network, allowing the creation of dashboards to capture important events and trends, displaying them over time.
- Helps reduce Total Cost of Ownership by proactively monitoring for network problems, automating common configuration actions and enabling easy firmware deployment, thus allowing network administrators to focus on more critical activities.

Dell OpenManage Network Manager automates a wide range of tasks and takes the complexity out of many administrative activities. First, a resource discovery wizard helps simplify discovery of IP-based network elements and presents them in the Managed Resources pane, as Figure 58 shows. Wizards also automate discovery of network devices, providing detailed device information and customized reports, as Figure 58 shows. Administrators can use these reports to create network topology maps.



Network Status	Name	IP Address	Vendor	Model	Firmware Version	Software Version
✓ Responding	N4064F - Aggregation ...	10.1.57.2	Dell Inc.	Dell Networking N4064F	R.1.13.1	R.1.13.1
✓ Responding	N4064F - Aggregation ...	10.1.57.1	Dell Inc.	Dell Networking N4064F	R.1.13.1	R.1.13.1
✓ Responding	N3024F - Access Sta...	10.1.57.6	Dell Inc.	Dell Networking N3024F	6.0.0.2	6.0.0.2
✓ Responding	N3024F - Access Sta...	10.1.57.7	Dell Inc.	Dell Networking N3024F	6.0.0.2	6.0.0.2
✓ Responding	Controller SS W-7240	10.1.57.5	Dell Inc.	PowerConnect W-724...	6.3.1.2 (41362)	6.3.1.2 (41362)
✓ Responding	CRAContoller - W7210...	10.1.57.4	Dell Inc.	PowerConnect W-721...	6.3.1.2 (41362)	6.3.1.2 (41362)

Name	Port Type	State
Fo1/0/1	40 Gigabit Ethernet Port	✓
Fo1/0/2	40 Gigabit Ethernet Port	☒
Te1/0/1	10 Gigabit Ethernet Op...	☒
Te1/0/2	10 Gigabit Ethernet Op...	☒
Te1/0/3	10 Gigabit Ethernet Op...	☒
Te1/0/4	10 Gigabit Ethernet Op...	☒

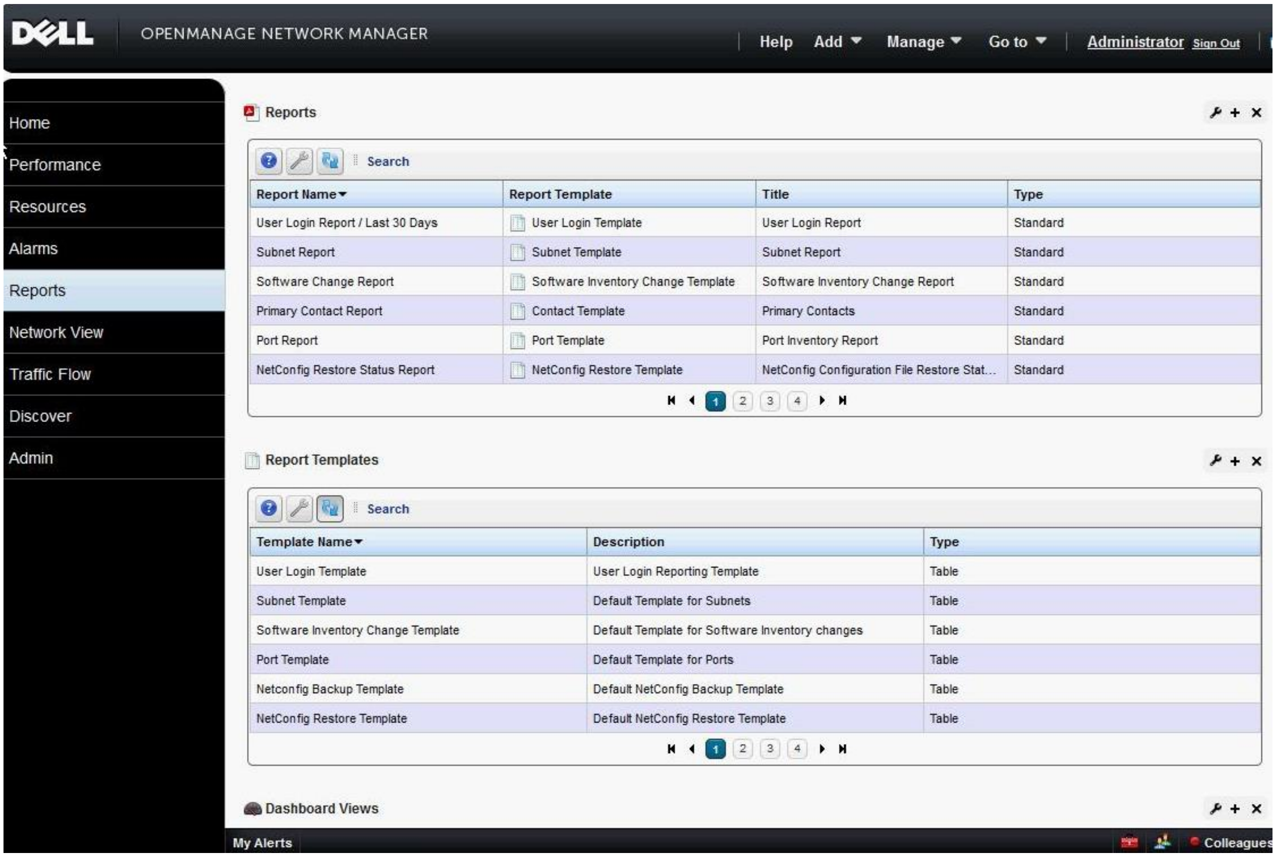
1 2 3 4

Name	Target(s)	Overall Compliance	Monitored	Scheduled

No data is available to display

Network Tools lets you invoke a variety of existing tools on a device without having the device discovered. Before any tools can be executed you must enter

Figure 58 OPNM Managed resources and Ports window



Reports

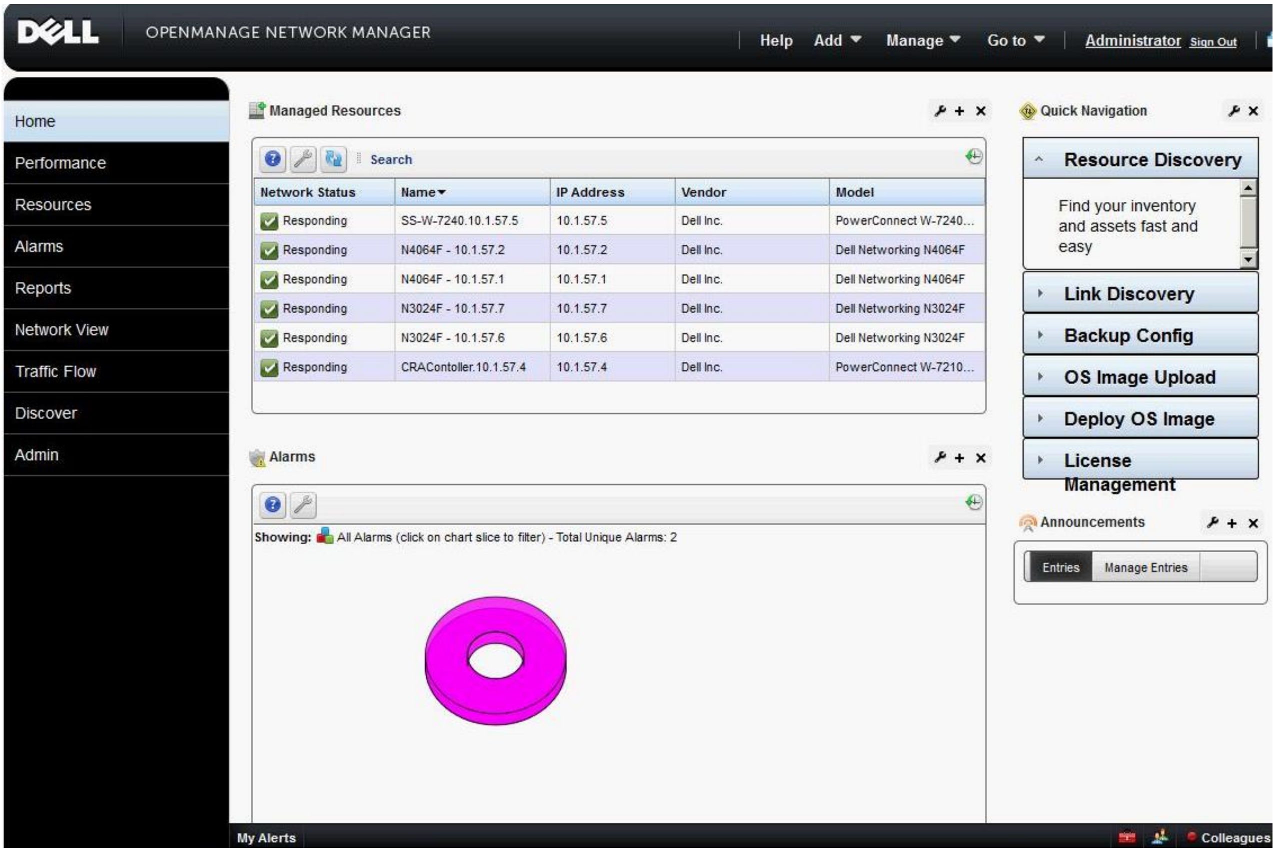
Report Name	Report Template	Title	Type
User Login Report / Last 30 Days	User Login Template	User Login Report	Standard
Subnet Report	Subnet Template	Subnet Report	Standard
Software Change Report	Software Inventory Change Template	Software Inventory Change Report	Standard
Primary Contact Report	Contact Template	Primary Contacts	Standard
Port Report	Port Template	Port Inventory Report	Standard
NetConfig Restore Status Report	NetConfig Restore Template	NetConfig Configuration File Restore Stat...	Standard

Report Templates

Template Name	Description	Type
User Login Template	User Login Reporting Template	Table
Subnet Template	Default Template for Subnets	Table
Software Inventory Change Template	Default Template for Software Inventory changes	Table
Port Template	Default Template for Ports	Table
Netconfig Backup Template	Default NetConfig Backup Template	Table
NetConfig Restore Template	Default NetConfig Restore Template	Table

Figure 59 OPNM Customized reports window

After device discovery, administrators can view the managed resources and alarms, as Figure 60 shows. These are available at a glance from the OpenManage Network Manager console providing quick access to a menu of management actions. By clicking on a network switch, administrators can easily view details such as performance alarms, processor and memory utilization, and learned Media Access Control (MAC) addresses. These details also include an audit trail of configuration changes. Active performance monitors enable network administrators to track network health and performance of their network. The monitors allow for the creation of dashboards to capture important events and trends over time, as Figure 60 shows. A traffic-flow analysis feature enables administrators to get detailed information on the bandwidth consumption of key users, applications and devices.



Network Status	Name	IP Address	Vendor	Model
✓ Responding	SS-W-7240.10.1.57.5	10.1.57.5	Dell Inc.	PowerConnect W-7240...
✓ Responding	N4064F - 10.1.57.2	10.1.57.2	Dell Inc.	Dell Networking N4064F
✓ Responding	N4064F - 10.1.57.1	10.1.57.1	Dell Inc.	Dell Networking N4064F
✓ Responding	N3024F - 10.1.57.7	10.1.57.7	Dell Inc.	Dell Networking N3024F
✓ Responding	N3024F - 10.1.57.6	10.1.57.6	Dell Inc.	Dell Networking N3024F
✓ Responding	CRAContoller.10.1.57.4	10.1.57.4	Dell Inc.	PowerConnect W-7210...

Showing: All Alarms (click on chart slice to filter) - Total Unique Alarms: 2

Find your inventory and assets fast and easy

Figure 60 OPNM Managed Resources and Alarms window

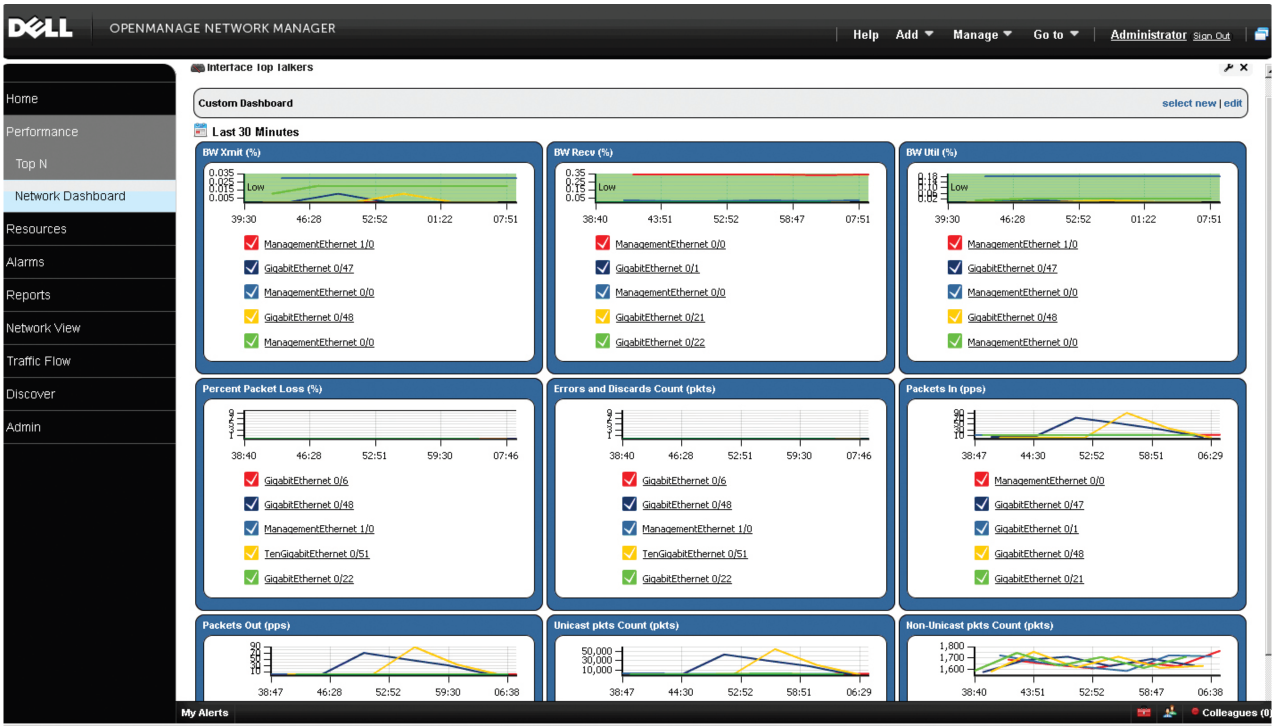


Figure 61 OPNM performance monitoring window

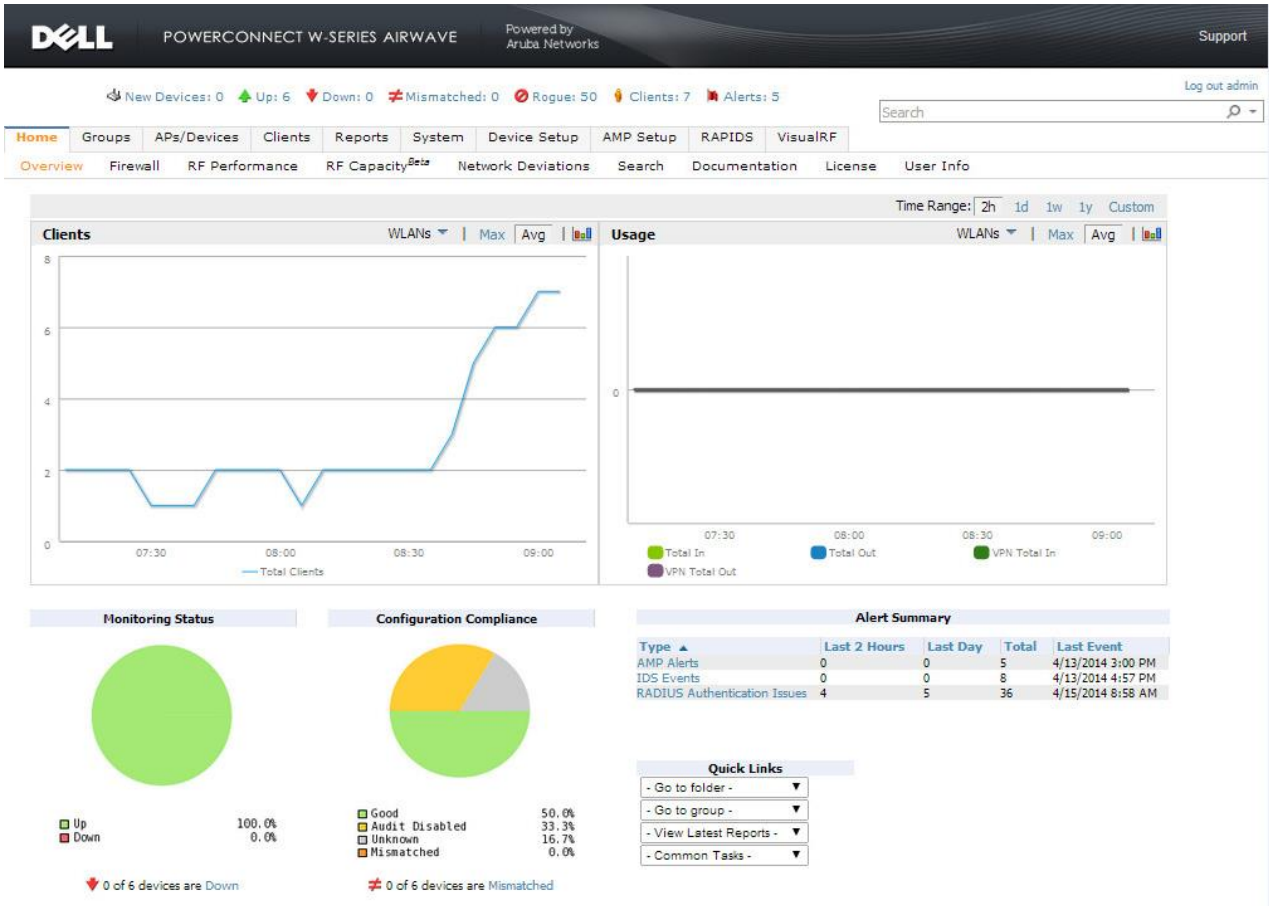
Note: For additional information on OMNM refer to the following publications -
OpenManage Network Manager WIKI
Dell OpenManage Network Manager User Guide 6.1
Dell OpenManage Network Manager Installation Guide 6.1
Dell OpenManage Network Manager Release Notes 6.1
Dell OpenManage Network Manager Quick Start Guide 6.1

6.2 W-Airwave

Dell Network W-Series Airwave is a network management product designed to provide deep visibility and configuration for the entire Dell W-Series WLAN portfolio. W-Airwave is a powerful tool to enable both device management and network monitoring of traffic and clients. This section shows many of the features and benefits W-Airwave provides in the campus environment.

6.2.1 W-Airwave interface

Administrators access and configure W-Airwave through the web GUI. Administrators can see an overview of the network from the home page of W-Airwave, as Figure 62 shows.

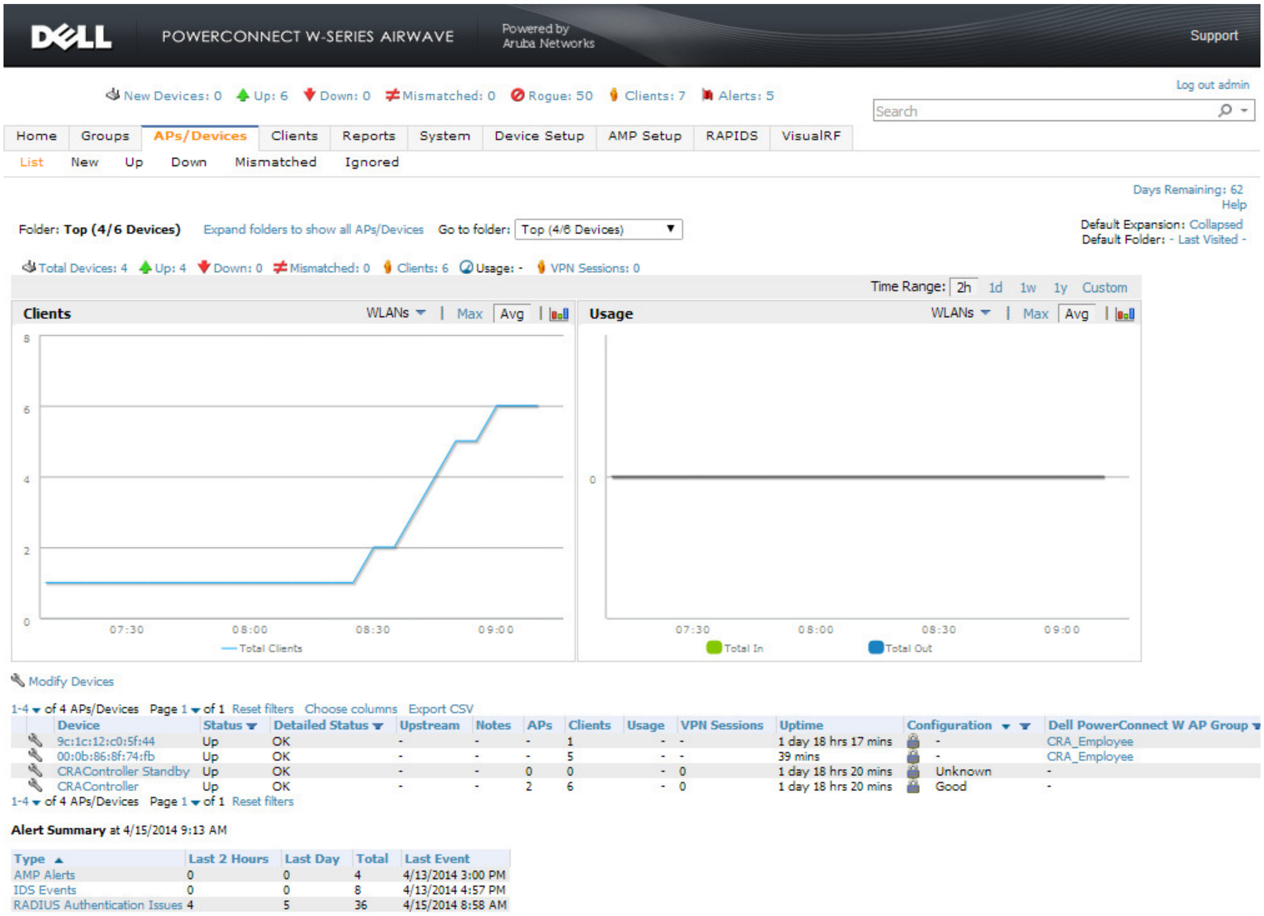


Alert Summary

Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	0	5	4/13/2014 3:00 PM
IDS Events	0	0	8	4/13/2014 4:57 PM
RADIUS Authentication Issues	4	5	36	4/15/2014 8:58 AM

Figure 62 W-Airwave home page

Administrators group network devices into any category that they prefer. Folders enable administrators to separate devices into groups to better monitor specific portions of the network. Figure 63 shows the status view for a group of controllers and APs:



New Devices: 0 Up: 6 Down: 0 Mismatched: 0 Rogue: 50 Clients: 7 Alerts: 5

Folder: **Top (4/6 Devices)** Expand folders to show all APs/Devices Go to folder: Top (4/6 Devices)

Default Expansion: Collapsed
Default Folder: - Last Visited -

Total Devices: 4 Up: 4 Down: 0 Mismatched: 0 Clients: 6 Usage: - VPN Sessions: 0

1-4 of 4 APs/Devices Page 1 of 1 Reset filters Choose columns Export CSV

Device	Status	Detailed Status	Upstream	Notes	APs	Clients	Usage	VPN Sessions	Uptime	Configuration	Dell PowerConnect W AP Group
9c:1c:12:c0:5f:44	Up	OK	-	-	-	1	-	-	1 day 18 hrs 17 mins	-	CRA_Employee
00:0b:86:8f:74:fb	Up	OK	-	-	-	5	-	-	39 mins	-	CRA_Employee
CRAController Standby	Up	OK	-	-	0	0	-	0	1 day 18 hrs 20 mins	Unknown	-
CRAController	Up	OK	-	-	2	6	-	0	1 day 18 hrs 20 mins	Good	-

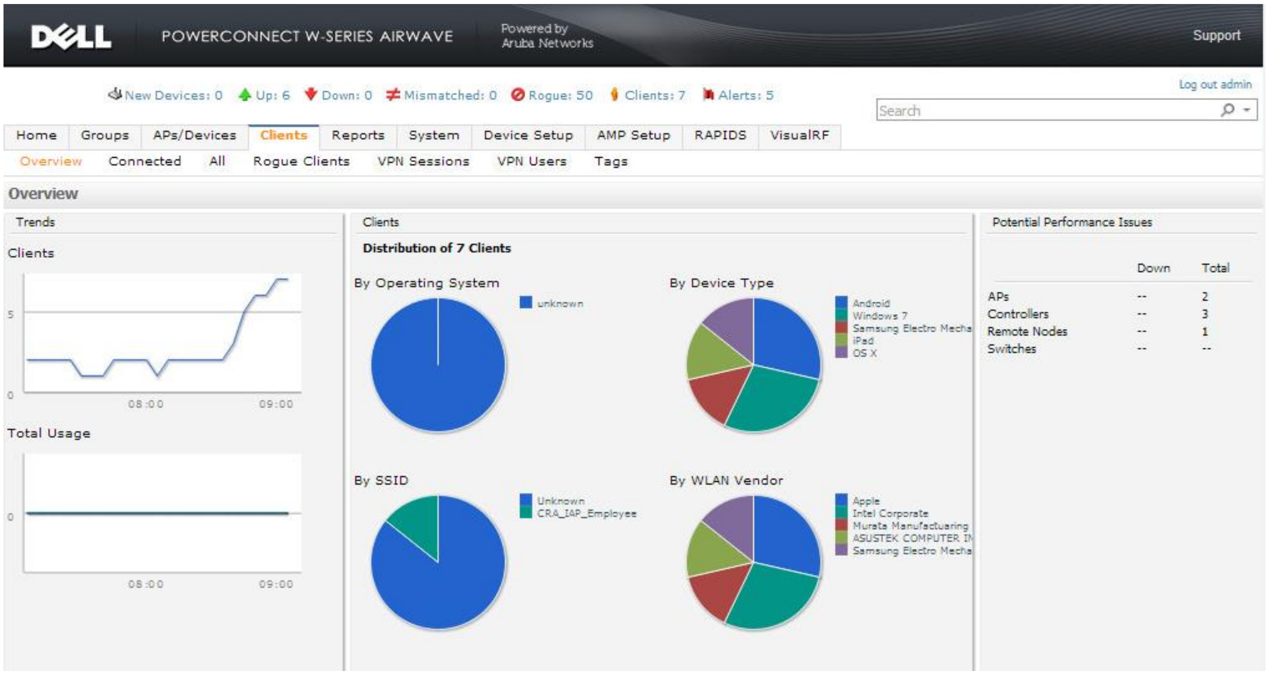
1-4 of 4 APs/Devices Page 1 of 1 Reset filters

Alert Summary at 4/15/2014 9:13 AM

Type	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	0	4	4/13/2014 3:00 PM
IDS Events	0	0	8	4/13/2014 4:57 PM
RADIUS Authentication Issues	4	5	36	4/15/2014 8:58 AM

Figure 63 W-Airwave status view

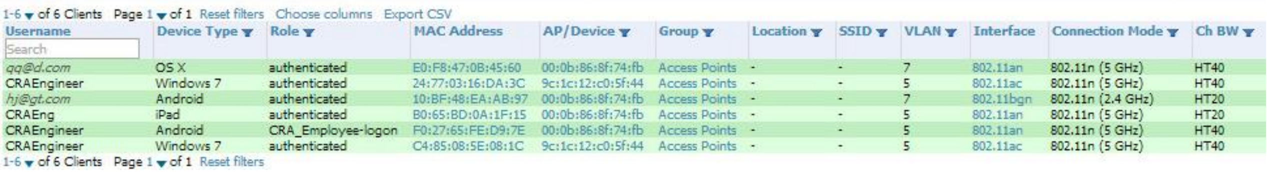
A client’s status is also a key feature of W-Airwave. Administrators track and monitor clients based on several factors including device type, access method, connection state, user name and user role. Figure 64 shows the W-Airwave Client Overview page:



	Down	Total
APs	--	2
Controllers	--	3
Remote Nodes	--	1
Switches	--	--

Figure 64 Client overview page

Figure 65 shows a detailed list of the client attributes displayed in table form:


1-6 of 6 Clients Page 1 of 1 Reset filters Choose columns Export CSV

Username	Device Type	Role	MAC Address	AP/Device	Group	Location	SSID	VLAN	Interface	Connection Mode	Ch BW
Search											
qq@d.com	OS X	authenticated	E0:F8:47:0B:45:60	00:0b:86:8f:74:fb	Access Points	-	-	7	802.11an	802.11n (5 GHz)	HT40
CRAEngineer	Windows 7	authenticated	24:77:03:16:DA:3C	9c:1c:12:c0:5f:44	Access Points	-	-	5	802.11ac	802.11n (5 GHz)	HT40
hj@gt.com	Android	authenticated	10:BF:48:EA:AB:97	00:0b:86:8f:74:fb	Access Points	-	-	7	802.11bgn	802.11n (2.4 GHz)	HT20
CRAEng	iPad	authenticated	B0:65:BD:0A:1F:15	00:0b:86:8f:74:fb	Access Points	-	-	5	802.11an	802.11n (5 GHz)	HT20
CRAEngineer	Android	CRA_Employee-logon	F0:27:65:FE:D9:7E	00:0b:86:8f:74:fb	Access Points	-	-	5	802.11an	802.11n (5 GHz)	HT40
CRAEngineer	Windows 7	authenticated	C4:85:08:5E:08:1C	9c:1c:12:c0:5f:44	Access Points	-	-	5	802.11ac	802.11n (5 GHz)	HT40

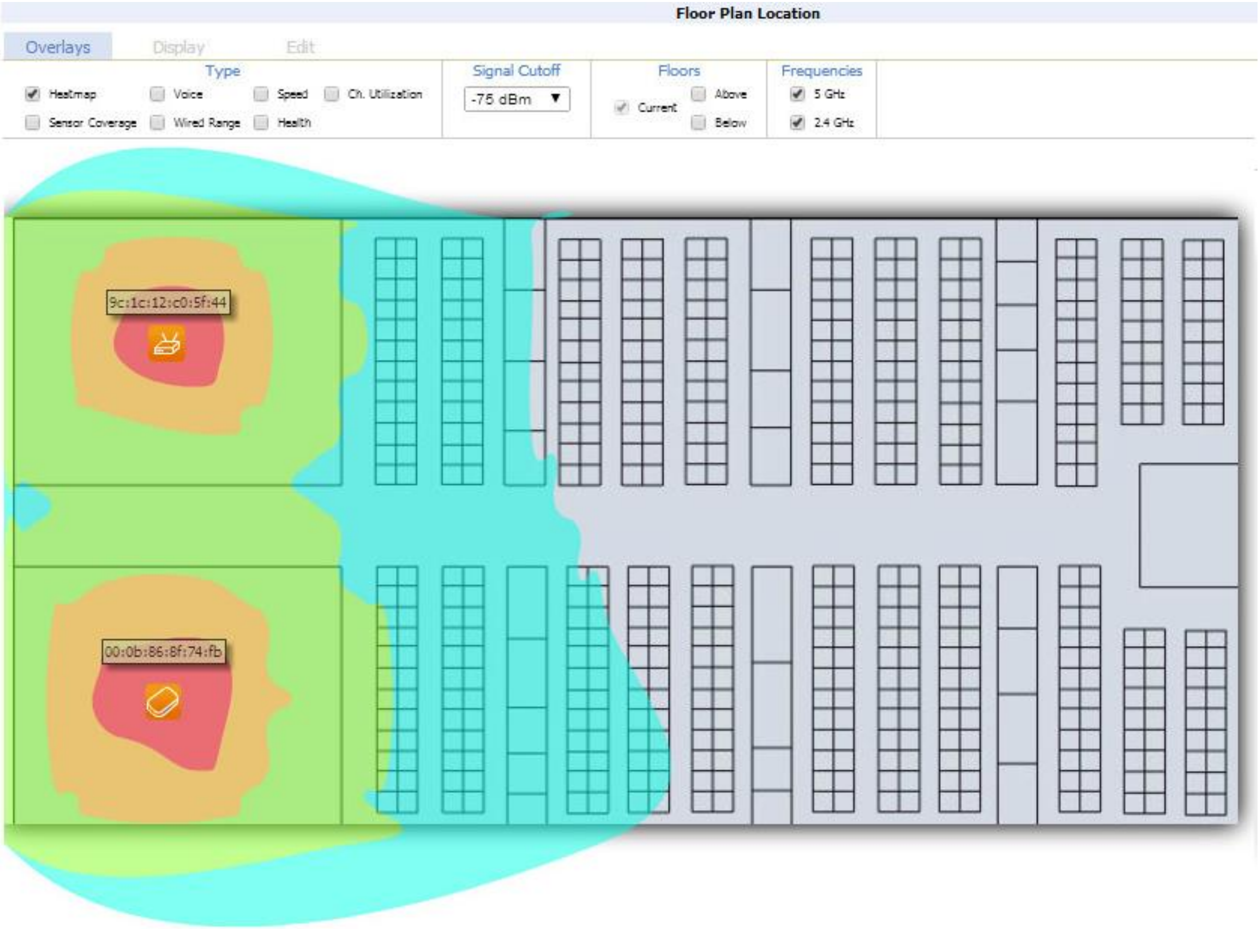
1-6 of 6 Clients Page 1 of 1 Reset filters

Figure 65 Client attributes list

6.2.2 W-Airwave features

W-Airwave includes all the standard features you would expect in a Network Management System. These features include device configuration, monitoring, firmware updates, alerts, and logging. W-Airwave also includes tools to help businesses plan, secure, and maintain regulatory controls.

Planning for and maintaining network performance of wireless networks is a difficult task. W-Airwave includes a powerful tool, VisualRF, to help with planning and maintenance. By uploading a floor plan into W-Airwave, VisualRF can overlay RF performance data to visually represent the RF environment. Figure 66 shows two deployed access points on a floor plan. The heat map produced shows the RF signal strength.



Type: ☑ Heatmap □ Voice □ Speed □ Ch. Utilization □ Sensor Coverage □ Wired Range □ Health

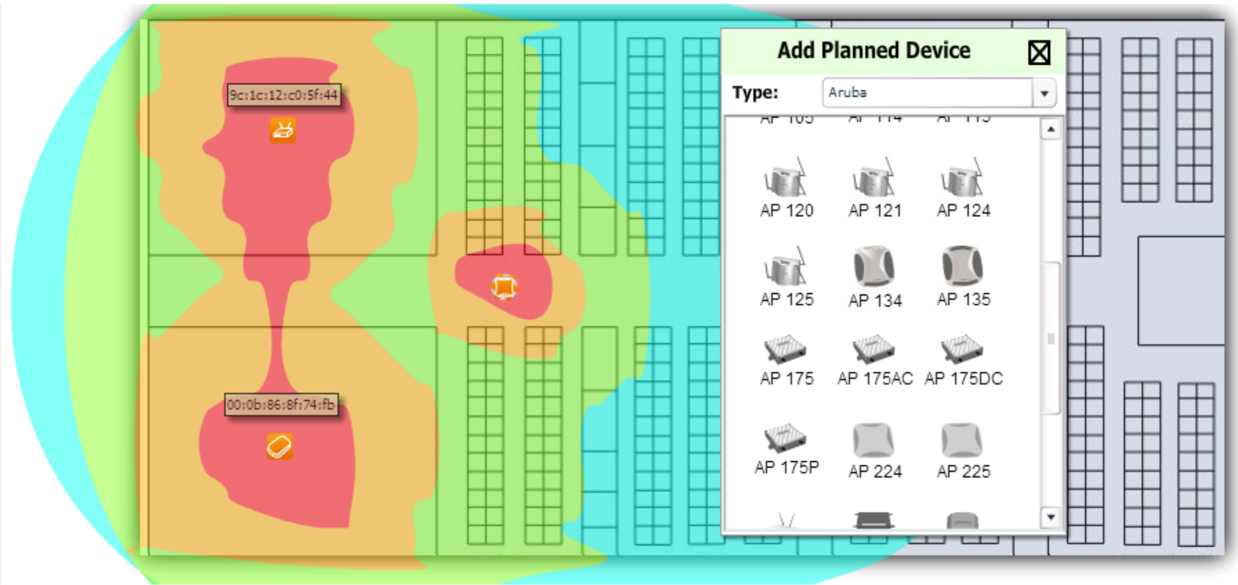
Signal Cutoff: -75 dBm ▼

Floors: ☑ Current □ Above □ Below

Frequencies: ☑ 5 GHz ☑ 2.4 GHz

Figure 66 W-Airwave, VisualRF floor plan with Heatmap overlay

The planning tools within VisualRF allow the user to place simulated APs on the building's floor plan. The user can improve the simulation by entering specific building materials and objects that can affect RF propagation. This tool is an excellent way to plan prior to an expensive and time consuming site survey. Figure 67 shows a simulated AP being added to the heat map shown in Figure 66. Simulated APs can be used by themselves or intermixed with active deployed APs.

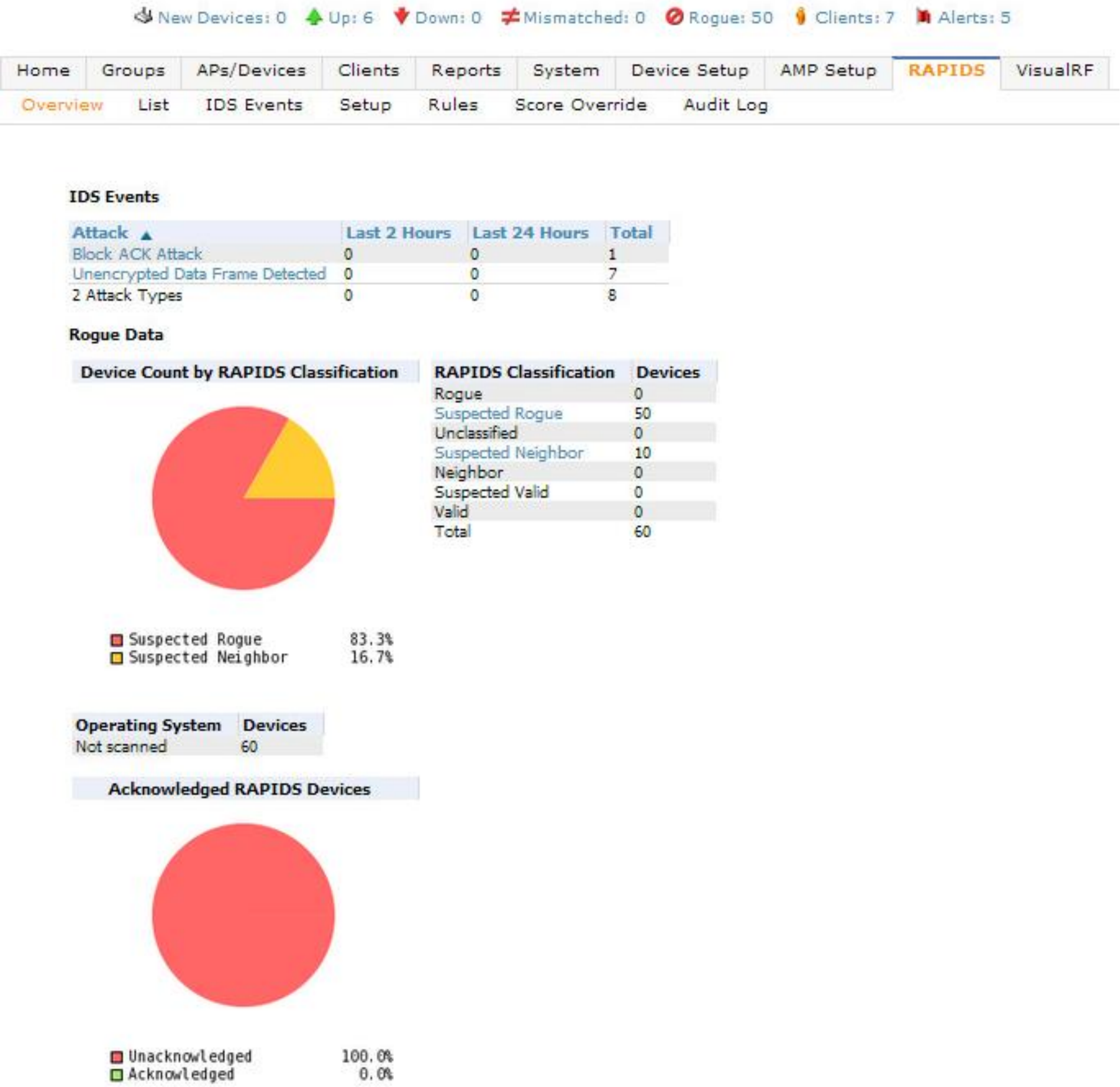


Type: Aruba

Figure 67 Simulated addition of an AP to the heat map

Another important feature of W-Airwave is security. W-Airwave includes Rogue Detection and IDS (RAPIDS). W-Airwave uses existing AP data to secure the network from rogue and intrusion threats. The RAPIDS tab provides access to monitored events through the tab and related status pages. RAPIDS also displays rogue devices within VisualRF to give an estimated location of the threat.

Figure 68 shows the RAPIDS overview pages.



IDS Events

Attack ▲	Last 2 Hours	Last 24 Hours	Total
Block ACK Attack	0	0	1
Unencrypted Data Frame Detected	0	0	7
2 Attack Types	0	0	8

Rogue Data

Device Count by RAPIDS Classification

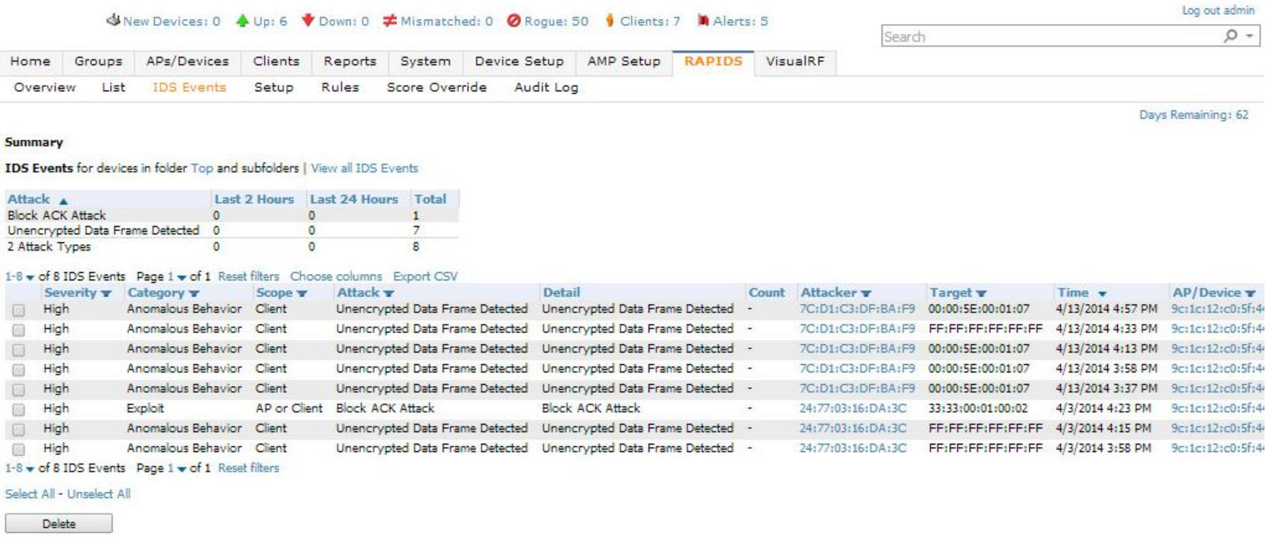
RAPIDS Classification	Devices
Rogue	0
Suspected Rogue	50
Unclassified	0
Suspected Neighbor	10
Neighbor	0
Suspected Valid	0
Valid	0
Total	60

Operating System	Devices
Not scanned	60

Acknowledged RAPIDS Devices

Figure 68 RAPIDS overview page

Figure 69 shows IDS events in a table format:



Summary

IDS Events for devices in folder Top and subfolders | View all IDS Events

Attack ▲	Last 2 Hours	Last 24 Hours	Total
Block ACK Attack	0	0	1
Unencrypted Data Frame Detected	0	0	7
2 Attack Types	0	0	8

1-8 ▾ of 8 IDS Events Page 1 ▾ of 1 Reset filters Choose columns Export CSV

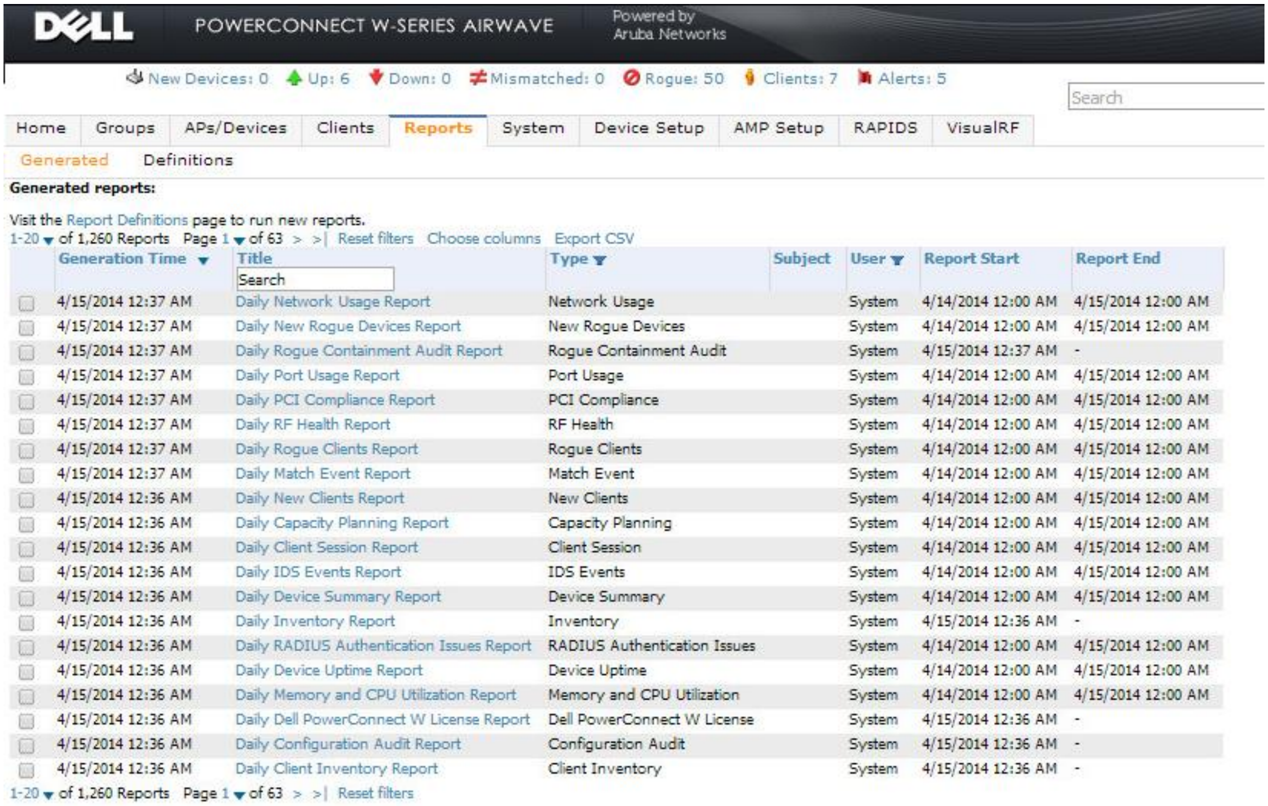
	Severity ▾	Category ▾	Scope ▾	Attack ▾	Detail	Count	Attacker ▾	Target ▾	Time ▾	AP/Device ▾
□	High	Anomalous Behavior	Client	Unencrypted Data Frame Detected	Unencrypted Data Frame Detected	-	7C:D1:C3:DF:BA:F9	00:00:5E:00:01:07	4/13/2014 4:57 PM	9c:1c:12:c0:5f:4
□	High	Anomalous Behavior	Client	Unencrypted Data Frame Detected	Unencrypted Data Frame Detected	-	7C:D1:C3:DF:BA:F9	FF:FF:FF:FF:FF:FF	4/13/2014 4:33 PM	9c:1c:12:c0:5f:4
□	High	Anomalous Behavior	Client	Unencrypted Data Frame Detected	Unencrypted Data Frame Detected	-	7C:D1:C3:DF:BA:F9	00:00:5E:00:01:07	4/13/2014 4:13 PM	9c:1c:12:c0:5f:4
□	High	Anomalous Behavior	Client	Unencrypted Data Frame Detected	Unencrypted Data Frame Detected	-	7C:D1:C3:DF:BA:F9	00:00:5E:00:01:07	4/13/2014 3:58 PM	9c:1c:12:c0:5f:4
□	High	Anomalous Behavior	Client	Unencrypted Data Frame Detected	Unencrypted Data Frame Detected	-	7C:D1:C3:DF:BA:F9	00:00:5E:00:01:07	4/13/2014 3:37 PM	9c:1c:12:c0:5f:4
□	High	Exploit	AP or Client	Block ACK Attack	Block ACK Attack	-	24:77:03:16:DA:3C	33:33:00:01:00:02	4/3/2014 4:23 PM	9c:1c:12:c0:5f:4
□	High	Anomalous Behavior	Client	Unencrypted Data Frame Detected	Unencrypted Data Frame Detected	-	24:77:03:16:DA:3C	FF:FF:FF:FF:FF:FF	4/3/2014 4:15 PM	9c:1c:12:c0:5f:4
□	High	Anomalous Behavior	Client	Unencrypted Data Frame Detected	Unencrypted Data Frame Detected	-	24:77:03:16:DA:3C	FF:FF:FF:FF:FF:FF	4/3/2014 3:58 PM	9c:1c:12:c0:5f:4

1-8 ▾ of 8 IDS Events Page 1 ▾ of 1 Reset filters

Select All - Unselect All

Figure 69 IDS events

Legal and Regulatory compliance from industry standards is an important and necessary part of maintaining a network. W-Airwave provides reporting functions to assist with compliance and provide evidence that the standards are being met. Figure 70 shows a list of common built-in reports generated by W-Airwave. New reports can also be generated by specifying definitions within W-Airwave. Note the PCI Compliance Report in the list, as Figure 70 shows:



Generated reports:

Visit the Report Definitions page to run new reports.

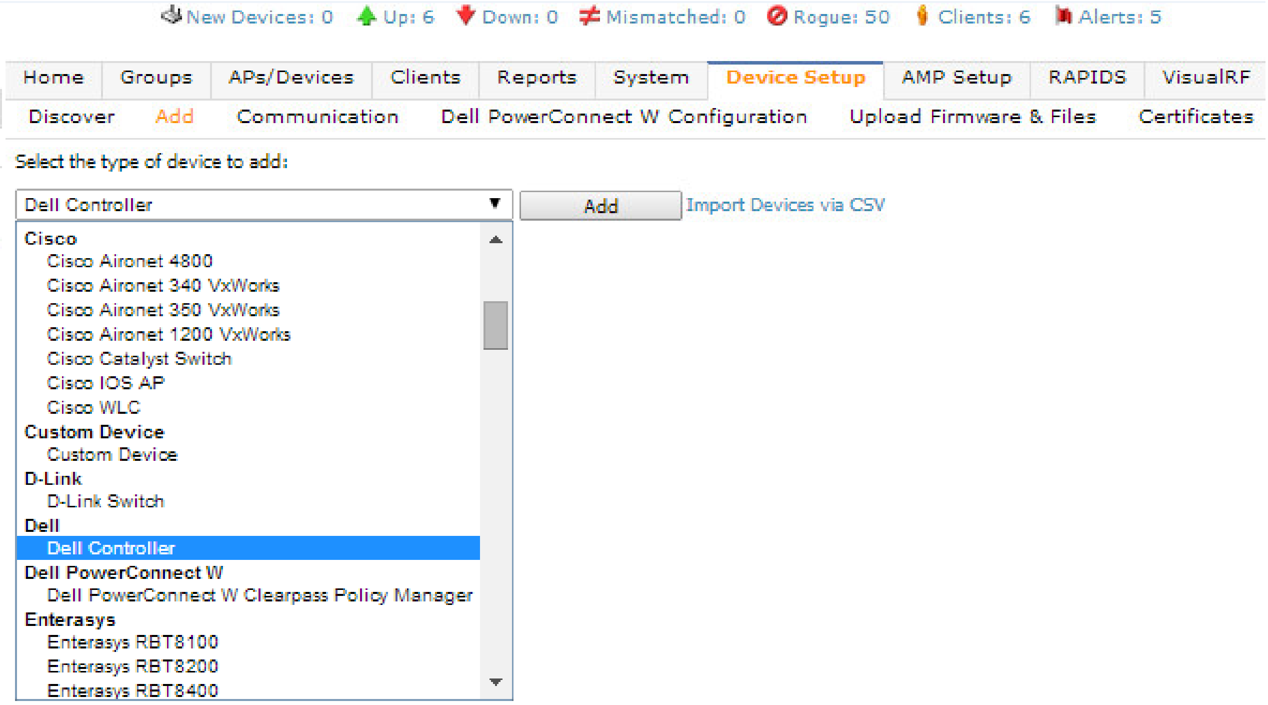
1-20 ▾ of 1,260 Reports Page 1 ▾ of 63 > >| Reset filters Choose columns Export CSV

	Generation Time ▾	Title Search	Type	Subject	User	Report Start	Report End
□	4/15/2014 12:37 AM	Daily Network Usage Report	Network Usage		System	4/14/2014 12:00 AM	4/15/2014 12:00 AM
□	4/15/2014 12:37 AM	Daily New Rogue Devices Report	New Rogue Devices		System	4/14/2014 12:00 AM	4/15/2014 12:00 AM
□	4/15/2014 12:37 AM	Daily Rogue Containment Audit Report	Rogue Containment Audit		System	4/15/2014 12:37 AM	-
□	4/15/2014 12:37 AM	Daily Port Usage Report	Port Usage		System	4/14/2014 12:00 AM	4/15/2014 12:00 AM
□	4/15/2014 12:37 AM	Daily PCI Compliance Report	PCI Compliance		System	4/14/2014 12:00 AM	4/15/2014 12:00 AM
□	4/15/2014 12:37 AM	Daily RF Health Report	RF Health		System	4/14/2014 12:00 AM	4/15/2014 12:00 AM
□	4/15/2014 12:37 AM	Daily Rogue Clients Report	Rogue Clients		System	4/14/2014 12:00 AM	4/15/2014 12:00 AM
□	4/15/2014 12:37 AM	Daily Match Event Report	Match Event		System	4/14/2014 12:00 AM	4/15/2014 12:00 AM
□	4/15/2014 12:36 AM	Daily New Clients Report	New Clients		System	4/14/2014 12:00 AM	4/15/2014 12:00 AM
□	4/15/2014 12:36 AM	Daily Capacity Planning Report	Capacity Planning		System	4/14/2014 12:00 AM	4/15/2014 12:00 AM
□	4/15/2014 12:36 AM	Daily Client Session Report	Client Session		System	4/14/2014 12:00 AM	4/15/2014 12:00 AM
□	4/15/2014 12:36 AM	Daily IDS Events Report	IDS Events		System	4/14/2014 12:00 AM	4/15/2014 12:00 AM
□	4/15/2014 12:36 AM	Daily Device Summary Report	Device Summary		System	4/14/2014 12:00 AM	4/15/2014 12:00 AM
□	4/15/2014 12:36 AM	Daily Inventory Report	Inventory		System	4/15/2014 12:36 AM	-
□	4/15/2014 12:36 AM	Daily RADIUS Authentication Issues Report	RADIUS Authentication Issues		System	4/14/2014 12:00 AM	4/15/2014 12:00 AM
□	4/15/2014 12:36 AM	Daily Device Uptime Report	Device Uptime		System	4/14/2014 12:00 AM	4/15/2014 12:00 AM
□	4/15/2014 12:36 AM	Daily Memory and CPU Utilization Report	Memory and CPU Utilization		System	4/14/2014 12:00 AM	4/15/2014 12:00 AM
□	4/15/2014 12:36 AM	Daily Dell PowerConnect W License Report	Dell PowerConnect W License		System	4/15/2014 12:36 AM	-
□	4/15/2014 12:36 AM	Daily Configuration Audit Report	Configuration Audit		System	4/15/2014 12:36 AM	-
□	4/15/2014 12:36 AM	Daily Client Inventory Report	Client Inventory		System	4/15/2014 12:36 AM	-

1-20 ▾ of 1,260 Reports Page 1 ▾ of 63 > >| Reset filters

Figure 70 W-Airwave reporting

In addition to W-Series WLAN products, W-Airwave also supports a wide variety of third party wired switches and WLAN devices. Figure 71 shows the drop-down list used when adding new devices to W-Airwave.



Select the type of device to add: Dell Controller

Figure 71 W-Airwave- adding new devices

7 Campus firewall

For this CRA, the Dell SonicWALL Network Security Appliance (NSA) 6600 delivers security and performance without compromise, as outlined in Figure 72. The NSA 6600 Appliance offers an extensive array of advanced security and networking features in an accessible and affordable platform that is easy to deploy and manage in a wide variety of environments.

NSA 6600 comes with 4x10G ports and supports up to 4000 single-sign-on users. NSA6600 fully supports high availability including active-active clustering. NSA6600 supports up to 90,000 connections per second and about 6000 site-to-site VPN connections. All these factors make NSA6600 a good match for large campus architectures.

7.1 Best practices and important features

The following sections outline some of the features and guidelines to consider while designing a network.

7.1.1 Active/standby high availability

This architecture shows NSA6600s used as highly available devices providing seamless connectivity to the outside world. Two NSA6600s are configured as an Active/Standby High Availability (HA) pair to support the requirements of the CRA. One firewall is the Active (Primary) device, processing and handling all traffic. The other firewall is in Standby mode until a keep-alive between the Primary and Standby expires, or a monitored link goes down. The NSA6600 comes with 4x10GbE and 8x1GbE interfaces. The 2x10GbE ports from each device are statically lagged to two N4064Fs. Administrators monitor these interfaces for any link failure or link down. As Figure 72 shows, 10GbE ports provide the data link and 1GbE links provide the control link.

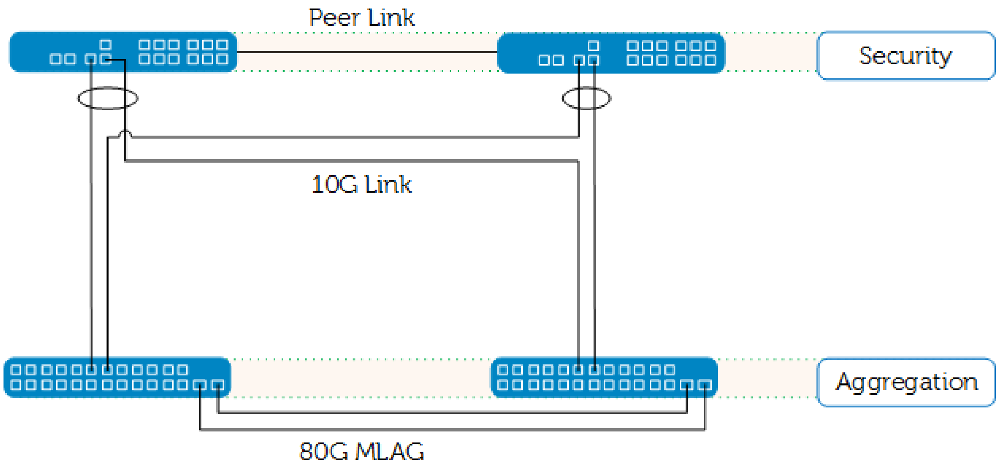


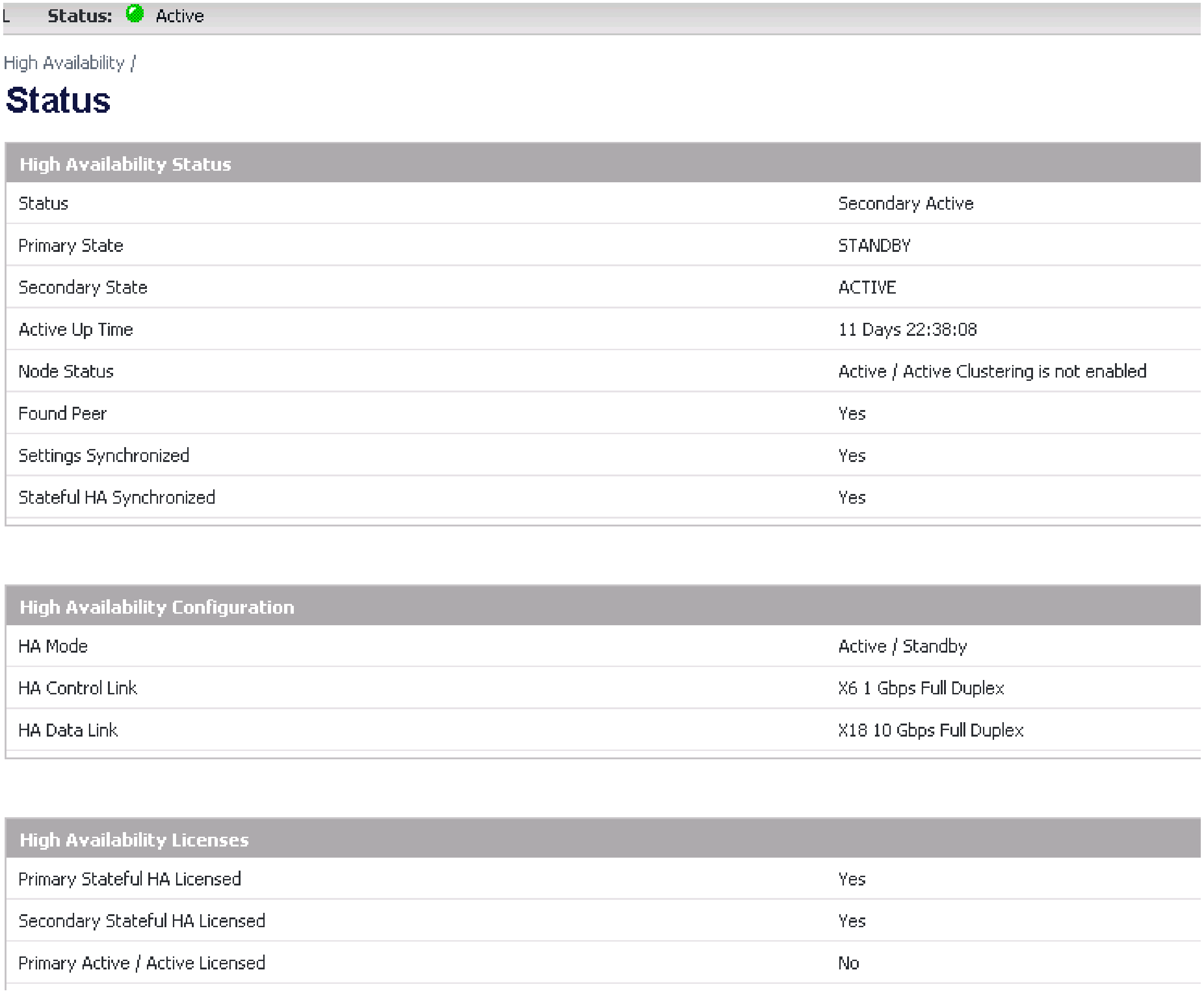
Figure 72 Firewall aggregation layer

The NSA 6600 supports the following four operation modes in high availability:

- Active/Standby
- Active/Active Deep Packet Inspection (DPI)
- Active/Active Clustering
- Active/Active DPI Clustering

The configuration includes NSA devices in Active/Standby mode based on the requirements of the Campus Architecture. Figure 73 provides a snapshot of the HA status:

Notes:
The HA feature needs a single license to operate. Both devices share a single license once configured as the HA pair in Active/Standby mode.
SonicWALL devices support static lag. Future plans include support for dynamic lag (LACP).



L Status: ● Active

High Availability /

Status

High Availability Status	
Status	Secondary Active
Primary State	STANDBY
Secondary State	ACTIVE
Active Up Time	11 Days 22:38:08
Node Status	Active / Active Clustering is not enabled
Found Peer	Yes
Settings Synchronized	Yes
Stateful HA Synchronized	Yes

High Availability Configuration	
HA Mode	Active / Standby
HA Control Link	X6 1 Gbps Full Duplex
HA Data Link	X18 10 Gbps Full Duplex

High Availability Licenses	
Primary Stateful HA Licensed	Yes
Secondary Stateful HA Licensed	Yes
Primary Active / Active Licensed	No

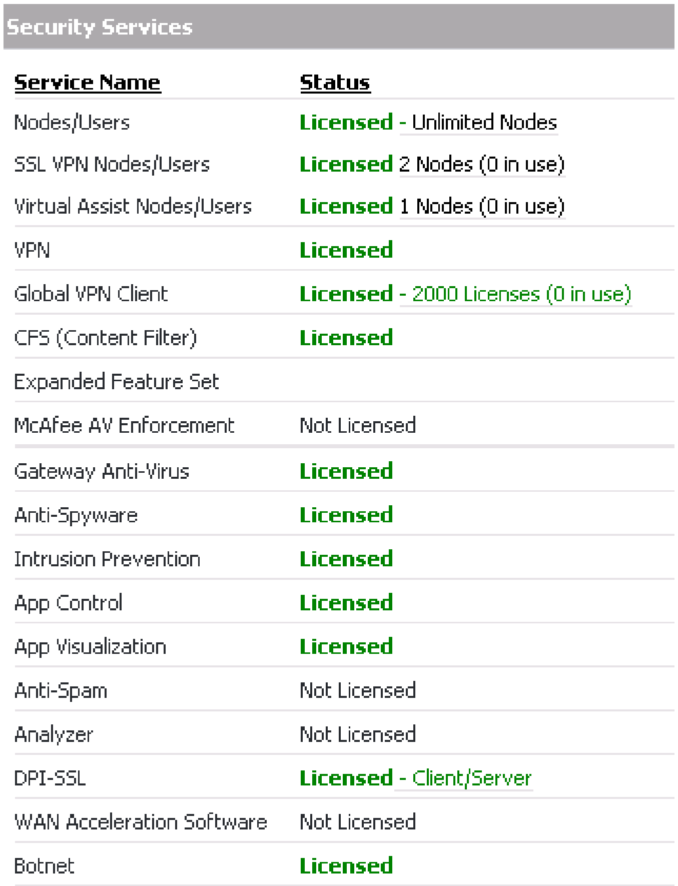
Figure 73 Snapshot of high availability status window

7.1.2 Security services licenses

The Dell SonicWALL Comprehensive Gateway Security Suite is a powerful security solution for businesses of all sizes, as it includes Gateway anti-virus, anti-spyware, Intrusion Prevention, application intelligence, control services, content filtering services, and 24x7 technical support.

Dell SonicWALL Gateway Security Suite delivers intelligent, real-time network security protection against sophisticated Application Layer and content-based attacks, including viruses, spyware and worms. Configurable tools prevent data leakage and enable visualization of network traffic.

Dell SonicWALL Content Filtering Service provides granular controls and unequalled content filtering to enforce Internet use policies and block access to websites containing information or images that are objectionable or unproductive. Figure 74 provides a snapshot of an enabled license:



Security Services

Service Name	Status
Nodes/Users	Licensed - Unlimited Nodes
SSL VPN Nodes/Users	Licensed 2 Nodes (0 in use)
Virtual Assist Nodes/Users	Licensed 1 Nodes (0 in use)
VPN	Licensed
Global VPN Client	Licensed - 2000 Licenses (0 in use)
CFS (Content Filter)	Licensed
Expanded Feature Set	
McAfee AV Enforcement	Not Licensed
Gateway Anti-Virus	Licensed
Anti-Spyware	Licensed
Intrusion Prevention	Licensed
App Control	Licensed
App Visualization	Licensed
Anti-Spam	Not Licensed
Analyzer	Not Licensed
DPI-SSL	Licensed - Client/Server
WAN Acceleration Software	Not Licensed
Botnet	Licensed

Figure 74 Snapshot of an enabled license

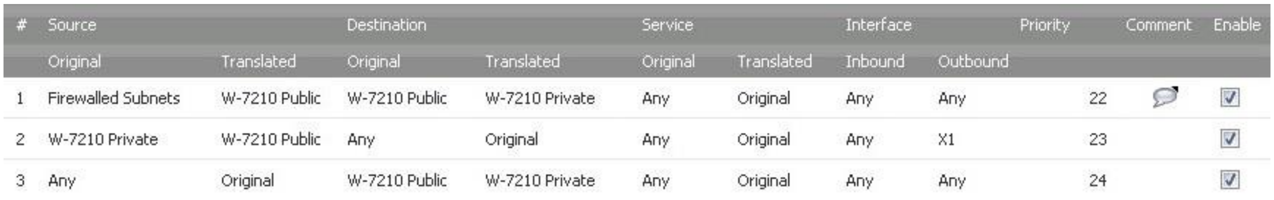
7.1.3 NAT policies, zones and firewall

The Network Address Translation (NAT) engine in SonicOS allows users to define granular NAT polices for their incoming and outgoing traffic. By default, the Dell SonicWALL Security Appliance has a preconfigured NAT policy to allow all systems connected to the LAN (X0**)** interface to perform Many-to-One NAT. This uses the IP address of the WAN (X1) interface. The appliance also has a policy to not perform NAT when traffic crosses between the other interfaces.

A packet contains (among other things) the requester’s IP address, the protocol information of the requestor, and the destination’s IP address. The NAT Policies engine in SonicOS can inspect the relevant portions of a packet and can dynamically rewrite the information in specified fields for incoming, as well as outgoing traffic.

This Reference Architecture topology has remote APs deployed across the WAN. These remote APs and networks utilize a VPN connection terminating on the W-Series controller within the campus network. To support this communication between the remote APs and the controller, the SonicWALL must have appropriate NAT policies to convert a public address to a private address. Figure 75 shows the NAT policy table.

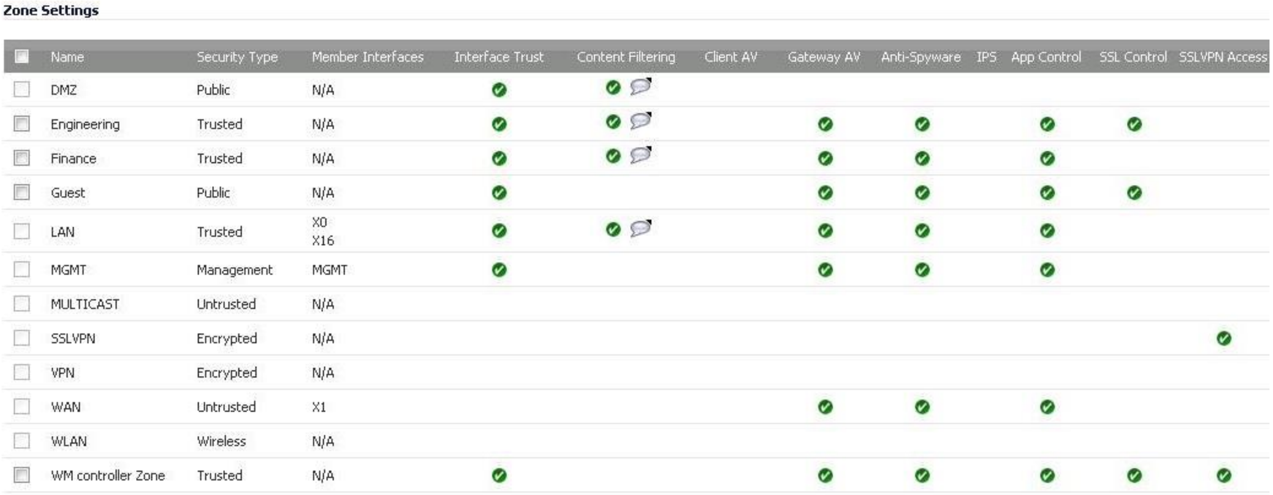
This topology includes an IAP located somewhere outside network, connected and managed from a controller within the network. To make this communication between IAP and controller, as Figure 75 shows, the SonicWALL must have appropriate NAT policies to convert the public address to private address and vice versa.



#	Source		Destination		Service		Interface		Priority	Comment	Enable
	Original	Translated	Original	Translated	Original	Translated	Inbound	Outbound			
1	Firewalled Subnets	W-7210 Public	W-7210 Public	W-7210 Private	Any	Original	Any	Any	22	💬	☑
2	W-7210 Private	W-7210 Public	Any	Original	Any	Original	Any	X1	23		☑
3	Any	Original	W-7210 Public	W-7210 Private	Any	Original	Any	Any	24		☑

Figure 75 Capture of zones enabled with proper security services

Figure 76 shows a Network Security Zone, It is simply a logical method of grouping one or more interfaces with friendly, user-configurable names and applying security rules as traffic passes between zones. Security zones provide an additional, more flexible layer of security for the firewall. With zone-based security, the administrator groups similar interfaces and applies the same policies to the groups. Otherwise, the administrator must write the same policy for each interface. Best practice is to enable appropriate security services for each zone.



Zone Settings

□	Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Client AV	Gateway AV	Anti-Spyware	IPS	App Control	SSL Control	SSLVPN Access
□	DMZ	Public	N/A	✓	✓ 💬							
□	Engineering	Trusted	N/A	✓	✓ 💬		✓	✓		✓	✓	
□	Finance	Trusted	N/A	✓	✓ 💬		✓	✓		✓		
□	Guest	Public	N/A	✓			✓	✓		✓	✓	
□	LAN	Trusted	X0 X16	✓	✓ 💬		✓	✓		✓		
□	MGMT	Management	MGMT	✓			✓	✓		✓		
□	MULTICAST	Untrusted	N/A									
□	SSLVPN	Encrypted	N/A									✓
□	VPN	Encrypted	N/A									
□	WAN	Untrusted	X1				✓	✓		✓		
□	WLAN	Wireless	N/A									
□	WM controller Zone	Trusted	N/A	✓			✓	✓		✓	✓	✓

Figure 76 Capture of zones enabled with proper security services

A Resources and references

Support.Dell.com
Dell EMC's Support Site – Manuals

DellTechCenter.com
Dell EMC IT Community for sharing knowledge, best practices, and information about Dell EMC products and installations

Dell Networking Hardware and Devices
Additional information on all Dell Networking products

Dell Wireless Networking
Additional information on Dell W-Series Wireless Networking

W-Series Whitepapers and Validated Reference Designs
VRDs and Whitepapers

Stacking Dell Networking Switches
Document detailing stacking on Dell Networking N4000 series switches

OpenManage Network Manager WIKI
Videos and documentation

Dell Force 10 VLT (Virtual Link Trunking) Overview and Optimization
VLT documentation

Using MLAG in Dell Networking N-Series Switches
MLAG documentation

Reliable Skype for Business Voice with Dell Networking Switches and Wireless

Skype for Business documentation

Quality of Service for Voice on Dell Networking N-Series Switches and W-Series WLAN Controllers

Document describing use of voice QoS with Dell N-Series and W-WLAN equipment

B Attachments

This document includes the following attachments:

- C-Series Topology Files.pdf
  - C-Series Aggregation Switch1
  - C-Series Aggregation Switch2
  - N-Series Access Switch1
  - N-Series Access Switch2
  - Master Controller.txt
  - Standby Controller.txt
  - Instant AP225 Remote Site.txt
  - New Dell Networking W-ClearPass Configuration.pdf
  - New Dell Networking W-Instant Configuration.pdf
- N-Series Topology Files.pdf
  - N- Series Aggregation Switch 1
  - N- Series Aggregation Switch 2
  - N- Series Access Switch Stack1
  - N- Series Access Switch Stack 2
  - Master Controller.txt
  - Standby Controller.txt
  - Instant AP225 Remote Site.txt
  - New Dell Networking W-ClearPass Configuration.pdf
  - New Dell Networking W-Instant Configuration.pdf

C Firmware versions in this document

The following tables present the versions of the hardware and software components used to configure and validate the solutions that this guide provides:

Component	Description/Firmware version
C9010 Network Director and C1048P Rapid Access Node	9-10(0-29)
N-Series switches	6.2.6.6
SonicWALL NSA 6600	SonicOS Enhanced 6.1.1.5-19
W-Series controller	ArubaOS 6.3.x (and later)
W-Instant Access Point	Aruba InstantOS 4.0.x (and later)
W-Clearpass	6.2.x (and later)
W-Airwave	8.0.9.2
OpenManage Network Manager	6.1 SP1

D Support and feedback

Contacting Technical Support

Support Contact Information	Web: http://Support.Dell.com/ Telephone: USA: 1-800-945-3355

Feedback for this document

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.

About Dell EMC

Dell EMC is a worldwide leader in data center and campus solutions, which includes the manufacturing and distribution of servers, network switches, storage devices, personal computers, and related hardware and software. For more information on these and other products, please visit the Dell EMC website at http://www.dell.com.