

# Dell Networking Small Business Reference Architecture

A Reference Architecture for Small Businesses using Dell Networking X-Series Switches

Dell Networking Solutions Engineering  
July 2016

## Revisions

Date	Revision	Description	Authors
July 2016	1.2	Updated product information	Colin King, Davis Smith
February 2016	1.1	Updates for new SonicWALL hardware and software. Updated links, revised wording throughout.	Jim Slaughter, Davis Smith
April 2015	1.0	Initial release	Neal Beard, Manjesh Siddamurthy, Ed Blazek, Colin King, Michael Matthews

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Copyright © 2015 – 2016 Dell Inc. or its subsidiaries. All Rights Reserved. Dell and the Dell EMC logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. Except as stated below, no part of this document may be reproduced, distributed or transmitted in any form or by any means, without express permission of Dell.

You may distribute this document within your company or organization only, without alteration of its contents.

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.

Trademarks used in this text: Dell™, the Dell logo, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™, SonicWall™ and Vostro™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. Broadcom® and NetXtreme® are registered trademarks of Broadcom Corporation. Qlogic is a registered trademark of QLogic Corporation. 3CX® is a registered trademark of 3CX Ltd in Europe, the United States and other countries. Apple® iOS and Mac OS® X are registered trademarks of Apple Inc. Kindle™ and Fire™ are trademarks of Amazon.com, Inc. Android™ is a trademark of Google, Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.

# Table of contents

Revisions.....	2
1 Introduction.....	5
2 Dell Networking X-Series Ethernet Switches .....	7
2.1 Dell Networking X4012 Switch .....	7
2.2 Dell Networking X1052/1052P Switches .....	8
3 Dell Networking W-Series Wireless Networking .....	9
3.1 Dell Networking W-IAP205 .....	9
4 Dell SonicWALL TZ Series .....	10
5 Dell PowerEdge VRTX Shared Infrastructure Chassis .....	11
6 Small Business Reference Architecture - Design .....	12
6.1 Example design .....	13
7 Small Business Reference Architecture - Switching .....	15
7.1 Dell Networking X-Series Switches .....	15
7.2 Important X-Series Features .....	15
7.2.1 Power over Ethernet (PoE).....	15
7.2.2 VLANs and Virtual LAN Routing.....	17
7.2.3 LAG.....	19
7.2.4 Voice VLAN .....	21
7.2.5 LLDP-MED.....	22
7.2.6 VoIP Digital PBX.....	24
8 Small Business Reference Architecture - Mobility .....	25
8.1 Important W-Series Features .....	26
8.1.1 W-Series Instant Access Points .....	26
8.1.2 W-Series Instant Access Point Virtual Controller .....	27
8.1.3 WLAN Employee and Guest Network Settings .....	29
8.1.4 Wireless Intrusion Detection and Protection .....	31
9 Small Business Reference Architecture - Firewall .....	33
9.1 Important SonicWALL TZ400 Features.....	33
9.1.1 Security Services Licenses.....	33
9.1.2 NAT Policies .....	34
9.1.3 Zones.....	35

9.1.4 Firewall .....	36
10 Small Business Reference Architecture - Compute .....	37
10.1 Important Dell PowerEdge VRTX features .....	37
10.2 Dell PowerEdge VRTX R1-2210 10GbE Ethernet I/O Module .....	37
11 Summary .....	38
A Resources and References .....	39
B Attachments .....	40
C Support and Feedback .....	41

# 1 Introduction

Today's small businesses increasingly rely on Voice over IP (VoIP), instant messaging, streaming video, and larger files and attachments. This has driven the need for enterprise-level feature sets in a small-business-centric product class. The emergence of virtual machines, virtual desktop infrastructure and very large databases (VLDB) has driven the need for increased bandwidth, lower latency and converged infrastructure in today's networks.

At the same time, small businesses face the challenge of keeping pace with the changing networking landscape. With limited resources, they must support a variety of connected devices that support key business functions. The Dell Networking Small Business Reference Architecture (SBRA) uses proven network design principles and best practices to create a framework for stable performance.

Dell Networking supports modern networks as depicted in Figure 1, providing customers with the most efficient use of current networking equipment at the lowest cost, while still providing today's great new technologies focused around the explosive data growth in the industry.

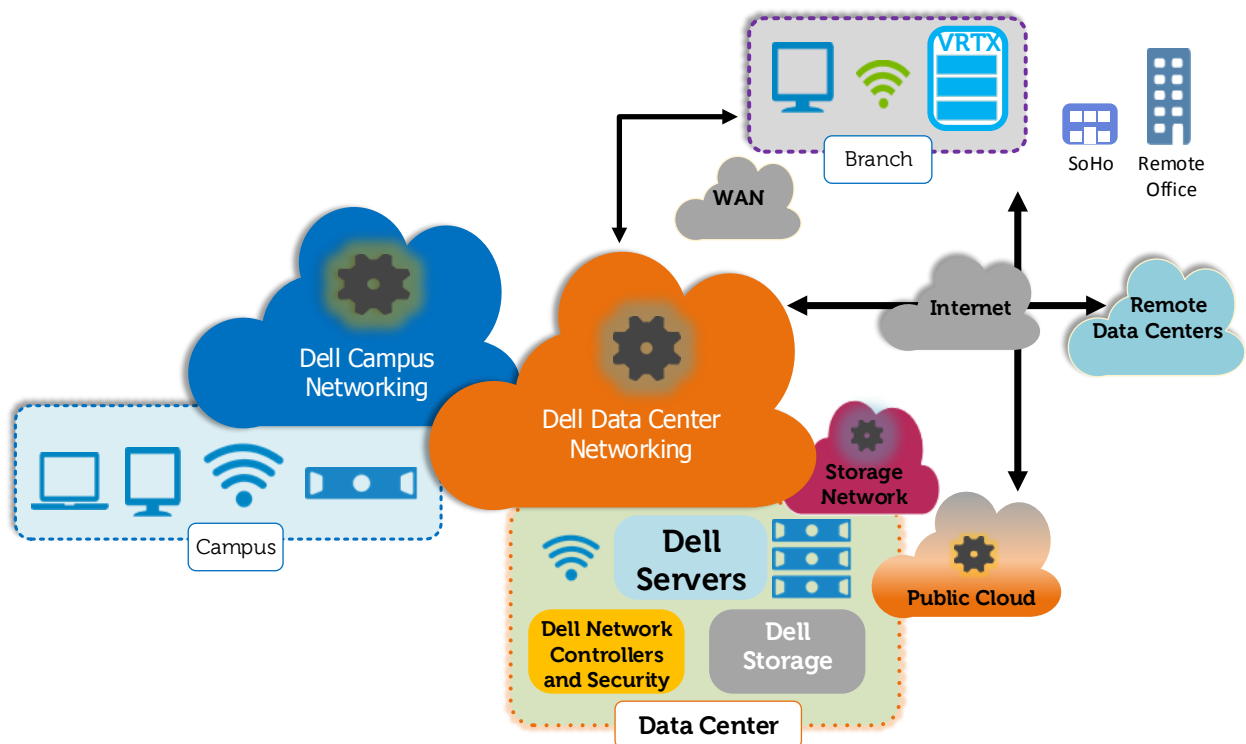


Figure 1 Modern Network Architecture

The Dell Small Business Reference Architecture (SBRA) focuses on the branch office, Small office/Home office (SoHo) and remote office portion of the Networking Architecture. Along with limited IT budgets, IT resources at these offices are often restricted to a single IT person. This person must support all infrastructure aspects of the office (servers, networks, backup, devices, applications, etc.) With this in mind, the solution must be simple with straightforward configuration and management. The Dell SBRA meets these needs and provides a template for wired and wireless technology, security, compute and storage.

The Dell SBRA highlights the ease-of-use and scalability of the Dell Networking X-Series smart-managed, GUI-based switches. These switches in conjunction with Dell EMC's W-Series Wireless Instant Access Points (W-IAPs) and SonicWALL TZ Series firewalls bring small businesses previously unattainable performance and security. The Dell PowerEdge VRTX chassis integrates servers, storage, networking and management into a single, compact form-factor with office-optimized dimensions, acoustics and security.

## 2 Dell Networking X-Series Ethernet Switches

Figure 2 shows the Dell X-Series smart-managed 1GbE and 10GbE Ethernet switches. These switches are designed for small and medium-sized businesses that require enterprise-class network control combined with the ease-of-use of a consumer device. These switches form a secure, energy-efficient switching environment designed to meet the needs of today's wired and wireless office environments. The Dell Networking X-Series switches, with step-by-step wizards and streamlined dashboard reporting tools, greatly assist in deployment speed and ease-of-management.



Figure 2 Dell Networking X-Series Switches

### 2.1 Dell Networking X4012 Switch

Figure 3 shows the Dell Networking X4012 switch, which forms the heart of a modern small business network, serving as its core or distribution layer. Today's small businesses need speed for bandwidth-intensive environments, such as virtualization or shared storage. This 10GbE Smart Managed Layer2+ switch is an ideal choice to meet this need. These switches provide power-efficient, enterprise-level technology with end-user-centric, step-by-step wizards for easy customization.



Figure 3 Dell Networking X4012 Series

The X4012 series features:

- Twelve 10GbE SFP+ ports
- Redundant variable-speed fans
- IPv4 and IPv6 Layer 2+ routing

## 2.2 Dell Networking X1052/1052P Switches

Figure 4 shows the Dell Networking X1052P which is used at the Access layer of the network. The X1052/1052P series of 52-port switches enables network designs with high-density connections in a limited space. The ability to connect [Power over Ethernet \(PoE\)](#) wireless access points, phones, cameras and network devices, such as the compact X1008 switches, directly to the 1052P allows any small business to create a best-of-breed network.



Figure 4 Dell Networking X1052P Series

The Dell Networking X1052 series features include:

- Forty-eight 10/100/1000Mbps RJ45 Ethernet ports
- Four 10GbE SFP+ ports
- Ready Rail kit for fast and easy rack installation
- IPv4 and IPv6 Layer 2+ routing



## 3 Dell Networking W-Series Wireless Networking

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

Dell Networking's W-Series WLAN products offer both centralized, controller-based and distributed, controller-less solutions. Along with this architectural flexibility, the product line offers a wide variety of capacity and performance options, which fit any branch, remote office or SoHo deployment.

### 3.1 Dell Networking W-IAP205

The W-IAP205 Instant Access Point (Figure 5) is a dual-radio access point with 802.11ac technology with data rates up to 867 Mbps. These Instant Access Points (IAPs) feature a virtual controller for a distributed, controller-less solution with access point clusters. The simplicity of configuration and deployment makes the W-IAP205 a perfect solution for small business sites with limited IT expertise or resources.

W-IAP205s offer many enterprise-class networking services without enterprise-size complexity.



#### W-IAP205 Features

- **Over-the-air provisioning**
- **Rogue detection**
- **Specialized Adaptive Radio Management functions for optimized Wi-Fi client behavior**
- **Auto-configuration for added IAPs**
- **802.11ac technology for maximum mobile device performance**

Figure 5 Dell Networking W-Series W-IAP205

## 4 Dell SonicWALL TZ Series

The Dell SonicWALL TZ series firewalls are the most secure Unified Threat Management (UTM) firewalls for small businesses. TZ series firewalls include the following features:

- Intrusion prevention
- Content/URL filtering
- Broad mobile platform support
- Deep packet inspection technology
- Network-based anti-malware and anti-spam services
- Multiple zones of controlled access
- GUI interface with easy-to-use wizards



Figure 6 Dell SonicWALL TZ400

Dell SonicWALL TZ400 firewalls provide industry-leading protection, performance and scalability.

The TZ400 has been developed with the needs of small businesses in mind, from its native remote VPN support for Apple iOS, Google Android, Windows 8.1, Mac OS X, Kindle Fire and Linux, to its ability to adapt as organizations and threats evolve. The TZ400 is an elegant integration of multiple products combined into a single solution providing value while reducing complexity.

## 5 Dell PowerEdge VRTX Shared Infrastructure Chassis

Figure 7 shows the Dell PowerEdge VRTX chassis, which combines blade servers, storage and networking into a compact tower chassis that can be rack-mounted into a 5U space. This award-winning Dell PowerEdge chassis is a purpose-built IT solution for small business environments. Its modular, flexible design delivers extensive capacity and performance scalability that ensures a future-proof investment. VRTX features include the following:

- Office-level acoustics
- Fresh-air validated configurations, which eliminate the need for special cooling
- Standard power requirements found in most offices (110-220V)
- Versatile internal shared storage



Figure 7 Dell PowerEdge VRTX Chassis

In the Small Business Reference Architecture, a Dell PowerEdge VRTX R1-2210 10GbE switch module resides in the Dell PowerEdge VRTX chassis.

The VRTX R1-2210 eliminates the need to cable and power an external networking switch. This industry-leading 10GbE switch module includes 16 internal server-facing ports and six external network ports (four 10GbE and two 1GbE) that can be used as uplinks.

## 6 Small Business Reference Architecture - Design

The Dell SBRA assists small business IT stakeholders in evaluating and planning robust, easy-to-deploy and easy-to-operate networks that grow with the needs of the business. It shows how wired and wireless network access and network intrusion prevention can work together with compute, storage, and a multitude of device types.

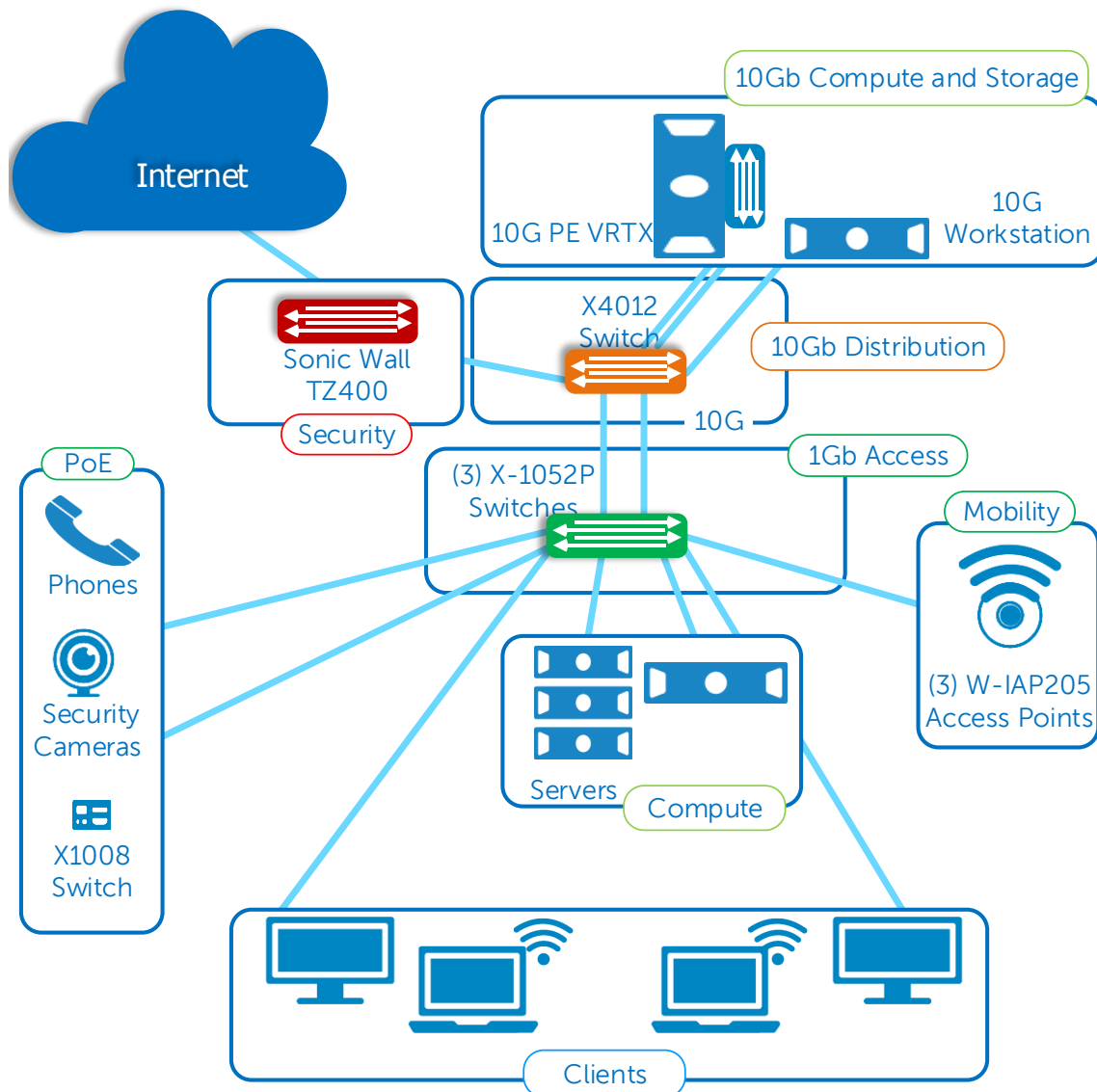


Figure 8 Small Business Reference Architecture Topology

This document presents a network topology, as shown in Figure 8, which represents a best-in-class design. The network uses a 10GbE X4012 switch as the distribution layer and three 1/10GbE X1052P switches for the access layer. W-IAP205 access points and a SonicWALL TZ400 firewall address the mobility and threat management aspects of the design. The Dell PowerEdge VRTX shared-infrastructure chassis contains M630

blade servers for compute, up to 25 hot-plug hard drives for shared storage, and an R1-2210 10GbE switch module for network connectivity.

The design of the SBRA scales around the number and type of users, as well as the device types that they use. The network is built around 50 users in a modern office setting who connect using both wired and wireless devices. The solution design scales from 25 to 75 users. Smaller deployments remove one X1052P, while larger deployments add more X1052Ps. For larger campus deployments, Dell EMC recommends reviewing the [Dell Networking Campus Switching and Mobility Reference Architecture 3.0](#).

## 6.1 Example design

The ability to allow for growth is an important consideration when entering into any network design project. A best practice is to design a base topology that meets the needs of the business with 10% to 20% headroom for port expansion. The following lists show a breakdown of the components in the featured network and include extra ports for future expansion.

### Distribution Layer

The distribution layer consists of a single Dell Networking X4012 switch with twelve 10GbE ports. The following list shows the port allocation:

- Link Aggregation Groups (LAG) to X1052Ps - six ports
- LAG to VRTX R1-2210 - two ports
- SonicWALL TZ400 Firewall - one port
- Future growth - three ports

### Access Layer

Three Dell Networking X1052P switches with 156 ports comprise the Access layer. The 156 ports include 144 1GbE RJ45 ports and twelve 10GbE SFP+ ports (non-shared), allocated as follows:

- LAGs to X4012 - six 10GbE ports
- W-IAP205 instant access points - three PoE ports
- Security cameras - four PoE ports
- Wired clients - 50 ports
- IP Phones - 50 PoE ports
- Future growth - 43 ports

**Note:** The X1052P switches connect in a simple LAG format for High Availability (HA). The switches can be located in close proximity to the devices that require connectivity.

## Wireless Network

The wireless network consists of three W-IAP205 Instant Access Points that provide the following data rates:

- 867 Mbps at 5GHz (802.11ac)
- 450 Mbps at 2.4GHz (802.11n)

**Note:** Typical deployments allocate 10-20 devices per access point depending on the physical environment and applications. This Small Business Reference Architecture uses three W-IAP205s in a 50-person office; however, it is easy to scale for density by adding more IAP's

## Firewall:

The SonicWALL TZ400 firewall includes:

- Support for up to 500 single-sign-on users
- Inspection throughput of 1300 Mbps

## VRTX R1-2210 10GbE I/O Module

The VRTX R1-2210 10GbE I/O Module includes the following ports:

- External, network uplink ports – six (four 10GbE and two 1GbE)
- Internal, server-facing, 10GbE ports - 16

The following sections provide details on each of the major areas of the SBRA.

[7 Small Business Reference Architecture - Switching](#)

[8 Small Business Reference Architecture - Mobility](#)

[9 Small Business Reference Architecture - Firewall](#)

[10 Small Business Reference Architecture - Compute](#)

## 7 Small Business Reference Architecture - Switching

### 7.1 Dell Networking X-Series Switches

The Dell Networking X-Series-based switching architecture modernizes the SoHo, branch and remote office (Figure 9):

- Easy, wizard-based deployment
- Optimized solutions
- Unified communications prioritization
- Energy-efficient design for low Total Cost of Ownership (TCO)

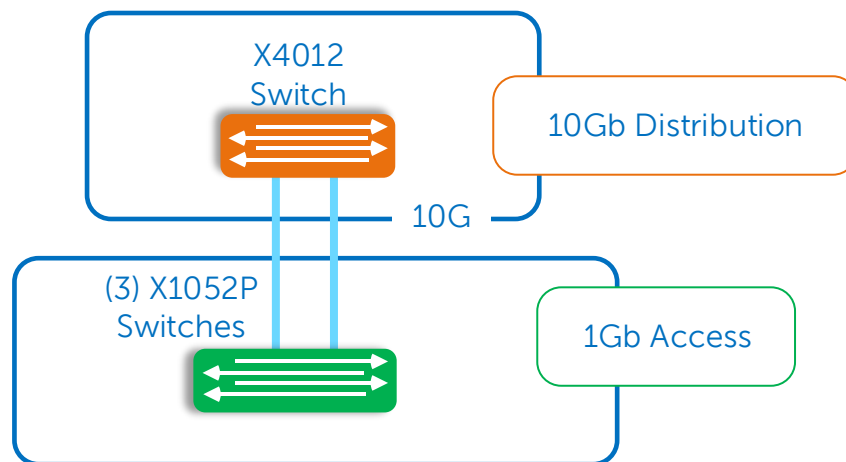


Figure 9 X-Series Switch Topology

### 7.2 Important X-Series Features

The following sections outline some of the features and guidelines to consider while designing a network using X-Series switches:

- [PoE](#) - Provides Power over Ethernet for security cameras and IP phones
- [VLANs](#) - Divides a physical network into multiple virtual networks
- [Virtual LAN Routing](#) – Forwards traffic across VLANs
- [LAG](#) - Creates a single logical link between switches for HA
- [Voice VLAN](#) - Ensures Quality of Service for Voice over IP
- [LLDP-MED](#) - Sets Voice VLAN Quality of Service parameters
- [VoIP Digital PBX](#) - Software package that's used as a digital PBX

#### 7.2.1 Power over Ethernet (PoE)

Power over Ethernet (PoE) allows a single Ethernet cable to provide both data and electrical power to PoE devices, which can include wireless access points, phones and cameras.

Figure 10 illustrates the broad support that X-Series switches have for PoE (15.4 watts) and PoE+ (30 watts) devices on the market today. The PoE characteristics of these switches (Table 1) should satisfy the needs of most small businesses.

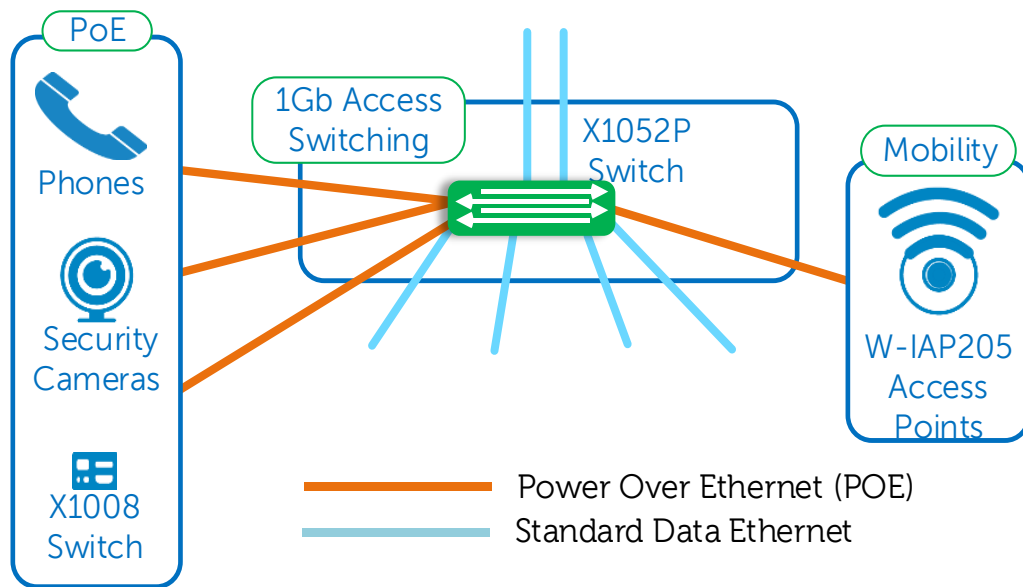


Figure 10 Power Over Ethernet

Table 1 Dell Networking X-Series Switches PoE Characteristics

Model	PoE/PoE+ Ports	Power Budget
X1008P	8 PoE ports	120W
X1018P	16 PoE ports	240W
X1026P	Up to 24 PoE ports or 12 PoE+ ports	360W
X1052P	Up to 24 PoE ports or 12 PoE+ ports	360W

Review the PoE/PoE+ devices that are connected to the switch using the Dell Networking Administrator Dashboard page shown in Figure 11. The Power over Ethernet dial shows PoE information as follows:

- Wattage used
- Overall Power Budget
- Total number of connected devices



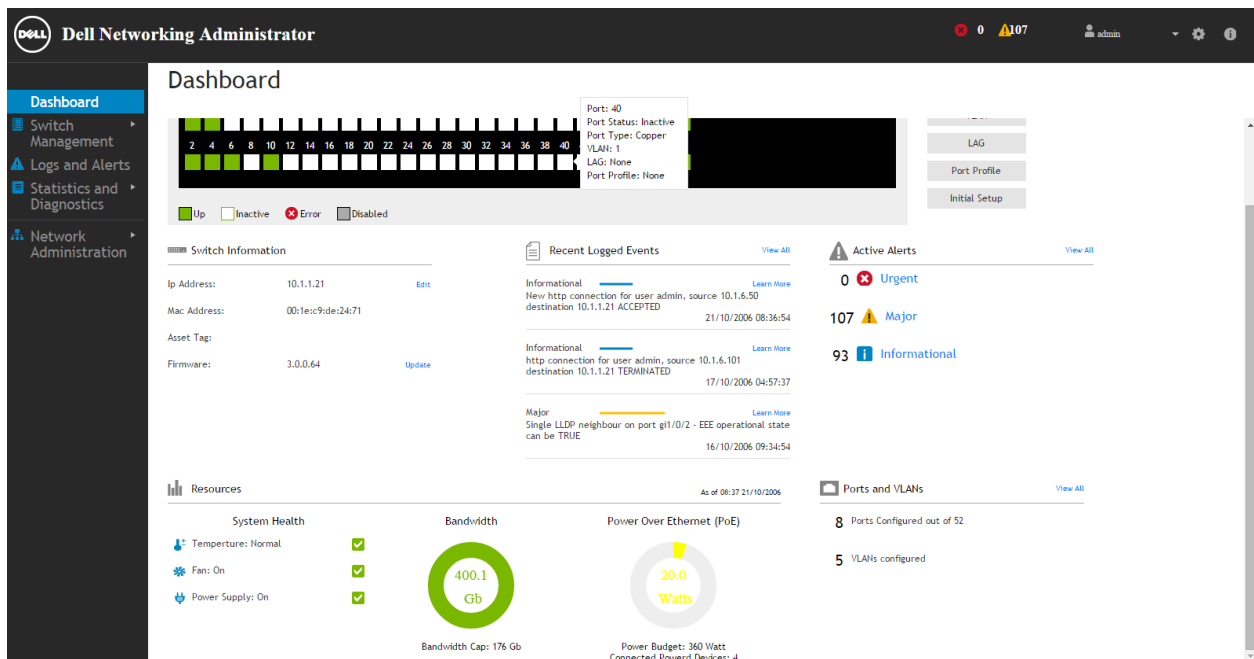


Figure 11 Power over Ethernet (PoE) on the Dashboard of the Dell Networking Administrator

The X-Series PoE switches have a Power over Ethernet network administration page that allows an administrator to set critical aspects of PoE functionality on a per-port basis or an overall (global) switch basis. This bi-level configuration granularity ensures successful management as well as greater control of all PoE device attributes.

## 7.2.2 VLANs and Virtual LAN Routing

Virtual LANs (VLANs) allow administrators to divide a physical network into multiple virtual networks or broadcast domains. Other benefits include the following:

- VLANs allow workstations in different buildings to belong to the same LAN.
- VLANs can increase performance on certain LAN segments by limiting broadcast traffic.
- VLANs can simplify administration tasks.
- VLANs can enhance existing security methods for sensitive data being sent on a network.

When IT administrators need to forward traffic across VLANs, the X-Series switches have a Layer 2+ mode that allows inter-VLAN routing. The Small Business Reference Architecture utilizes the X4012 switch, which defaults to Layer 2+ mode, to handle all VLAN-to-VLAN communications. Several VLANs have been configured to provide what a typical branch, remote office or SoHo might need. Figure 12 shows an example of a VLAN configuration. To see the full configuration of the Dell Networking X4012 used in this example, refer to the **X4012 Distribution switch.pdf** attachment.

**Note:** Administrators configure the Dell Networking X-Series line of switches from a GUI interface. The command line examples in this SBRA are for explanation purposes only.

```

interface vlan 1
  name Default_Vlan
  ip address 10.1.1.20 255.255.255.0
  no ip address dhcp
  ip dhcp relay enable
!
interface vlan 5
  name Security_Vlan
  ip address 10.1.5.20 255.255.255.0
!
interface vlan 6
  name Employee_Vlan
  ip address 10.1.6.20 255.255.255.0
  ip dhcp relay enable
!
interface vlan 7
  name Guest_Vlan
  ip address 10.1.7.20 255.255.255.0
  ip dhcp relay enable
!
interface vlan 10
  name VoIP
  ip address 10.1.10.20 255.255.255.0
  ip dhcp relay enable
!
interface vlan 15
  name Security_Camera
  ip address 10.1.15.20 255.255.255.0
!
interface vlan 100
  name "DHCP Relay"
  ip address 172.25.169.20 255.255.0.0
  ip dhcp relay enable

```

Figure 12 X4012 VLAN Configuration

**Note:** Initial VLAN provisioning for this SBRA was performed through the wizard-based VLAN configuration tool, accessible from the Dell Networking Administrator Dashboard. VLAN routing was configured from the Network Administration section.

## 7.2.3 LAG

A Link Aggregation Group (LAG) or port channel is an Ethernet protocol that combines multiple LAN cables between switches into a single logical link. This protocol provides a number of advantages pertaining to high availability in an Ethernet network, including the following:

- Load balancing – Allows data to be distributed across the multiple links.
- Failover – Allows data to keep flowing between switches as long as one physical link exists.
- Bandwidth – As network bandwidth needs grow, administrators may add LAN connections to an existing LAG through a non-disruptive process.
- Spanning Tree – The Spanning Tree Protocol (STP) sees the LAG as a single logical link and puts all the LAN connections into a forwarding state. When multiple LAN connections link two switches that are not running the link aggregation protocol, STP puts all but one LAN interface into a blocked state to ensure that no loops exist in the network.

The Small Business Reference Architecture has dual 10GbE link LAGs between the R1-2210 and X4012 and the X4012 and X1052P. In an office of 50 people or fewer, 20GbE generally provides enough bandwidth to satisfy the needs of most businesses. If an office has a need for higher bandwidth, the X-Series line of switches support up to eight LAN interfaces between switches for a provisioned bandwidth of 80GbE.

When setting up LAGs on X-Series switches, administrators set up the LAGs first and then add their interfaces via the wizard. The LAG wizard is accessed from the Dashboard page, shown in Figure 13, of the Dell Networking Administrator. After configuration, subsequent changes are made via the LAG page in the Network Administration section.

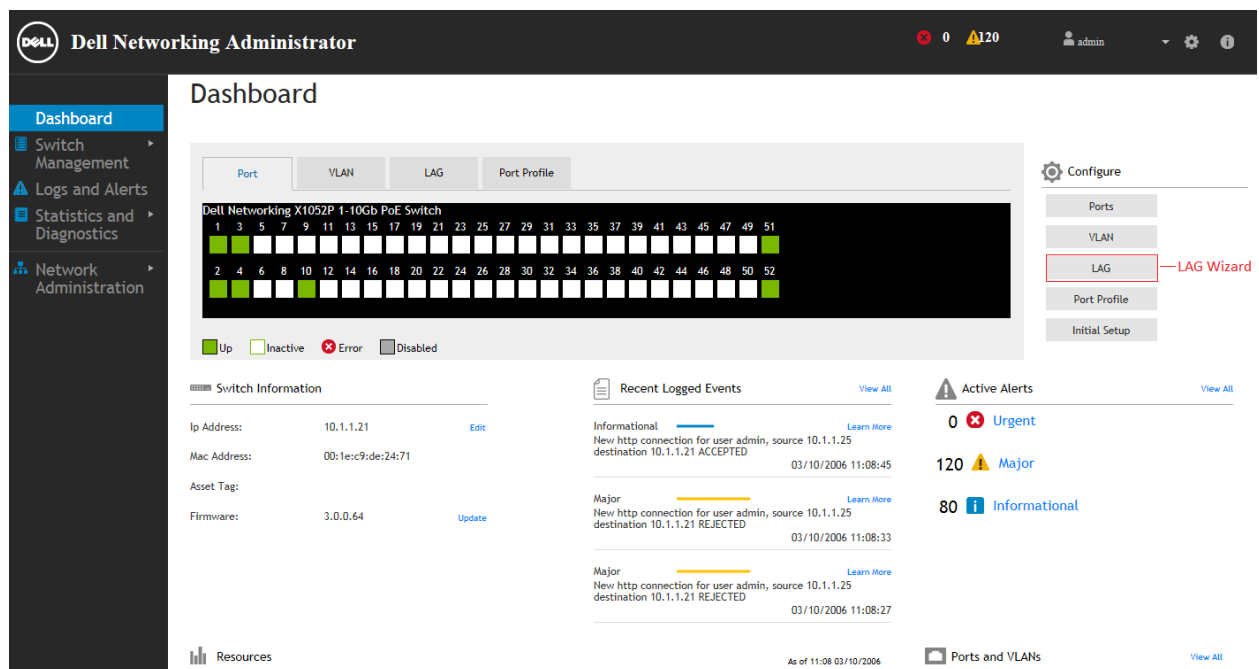


Figure 13 X-Series LAG Wizard

Figure 14 shows the LAG configurations for the X1052P Ethernet switch. Figure 15 shows the Dell PowerEdge R1-2210 10GbE Network I/O module. Figure 16 shows the X4012 Ethernet switch and X1052P Ethernet switch. Please refer to the attachments to view the full switch configurations.

```
interface tengigabitethernet1/0/3
description LAG11_to_Port11_X4012
channel-group 11 mode auto
switchport mode trunk
!
interface tengigabitethernet1/0/4
description LAG11_to_Port12_X4012
channel-group 11 mode auto
switchport mode trunk
!
interface Port-channel11
flowcontrol on
description X1052_ports5152_X4012_ports1112
switchport mode trunk
```

Figure 14 Dell Networking X1052P LAG Configuration

```
interface tengigabitethernet0/1
channel-group 1 mode auto
!
interface tengigabitethernet0/2
channel-group 1 mode auto
!
interface tengigabitethernet1/1
switchport access vlan 6
!
interface Port-channel1
description LAG_to_X4012
switchport mode trunk
```

Figure 15 Dell PowerEdge R1-2210 10GbE Network I/O module LAG Configuration

```
interface tengigabitethernet1/0/1
no eee enable
description LAG12_to_Port1_R1_2210
channel-group 12 mode auto
switchport mode trunk
no eee lldp enable
!
interface tengigabitethernet1/0/2
no eee enable
description LAG12_to_Port2_R1_2210
channel-group 12 mode auto
switchport mode trunk
no eee lldp enable
!
interface tengigabitethernet1/0/11
description LAG11_to_Port51_X1052
channel-group 11 mode auto
switchport mode trunk
!
```

```

interface tengigabitethernet1/0/12
description LAG11_to_Port52_X1052
channel-group 11 mode auto
switchport mode trunk
!
interface Port-channel11
description X4012_ports1112_X1052_ports5152
switchport mode trunk
!
interface Port-channel12
flowcontrol on
description R1_2210_Ports1_2_X4012_Ports1_2
switchport mode trunk

```

Figure 16 Dell Networking X4012 LAG Configuration

## 7.2.4 Voice VLAN

The X-Series Voice VLAN feature enables switch ports to carry voice traffic with a defined Quality of Service (QoS). This defined priority enables the separation of voice and data traffic coming into the port. The primary benefit of using the Voice VLAN feature is ensuring that the sound quality of an IP phone is safeguarded from deteriorating when data traffic on the port is high.

Voice over IP (VoIP) phones transmit IP traffic with a pre-configured Organizational Unique Identifier (OUI) prefix in the source MAC address of the Ethernet header. The OUI enables the switch to dynamically identify ports connected to VoIP equipment and automatically add these ports to the Voice VLAN. For the Voice VLAN to be operational on a port, it needs to be configured in conjunction with the Link Layer Discovery Protocol-Media Endpoint Device protocol ([LLDP-MED](#)). This combination of features ensures that IP phone voice traffic receives the correct Class of Service (CoS) prioritization.

Figure 17 shows the configuration of VoIP. Figure 18 shows the Voice VLAN Parameters on the Voice VLAN page from the Dell Networking Administrator.

```

voice vlan id 10
voice vlan state oui-enabled
voice vlan cos 6 remark
voice vlan oui-table add 000181 Nortel_____
voice vlan oui-table add 0001e3 Siemens_AG_phone_____
voice vlan oui-table add 00036b Cisco_phone_____
voice vlan oui-table add 0004f2 Polycom_____
voice vlan oui-table add 00096e Avaya_____
voice vlan oui-table add 000fe2 H3C_Aolynk_____
voice vlan oui-table add 001049 Shoretel_____
voice vlan oui-table add 0060b9 Philips_and_NEC_AG_phone_____
voice vlan oui-table add 00907a Polycom/Veritel_phone_____
voice vlan oui-table add 00e0bb 3Com_phone_____
lldp med network-policy 1 voice vlan 10 vlan-type tagged up 6 dscp 46
!
interface vlan 10
name VoIP
dot1x auth-not-req
!

```

```

interface gigabitethernet1/0/2
description VoIP Phone 1
spanning-tree portfast
switchport mode trunk
switchport access vlan none
switchport trunk allowed vlan remove 10
lldp optional-tlv port-desc sys-name sys-desc sys-cap
lldp med enable network-policy
lldp med network-policy add 1
voice vlan enable
!
interface gigabitethernet1/0/3
description VoIP Phone 2
spanning-tree portfast
switchport mode trunk
switchport access vlan none
switchport trunk allowed vlan remove 10
lldp optional-tlv port-desc sys-name sys-desc sys-cap
lldp med enable network-policy
lldp med network-policy add 1
voice vlan enable

```

Figure 17 X-Series VoIP Parameters

The screenshot shows the Dell Networking Administrator web interface. The left sidebar has a menu with 'Standard VLAN' and 'Voice VLAN' (selected). The main content area is titled 'Voice VLAN' and shows the following configuration:

- Properties:**
  - Voice VLAN State: Enabled
  - Voice VLAN ID: 10
  - Class Of Service: 6
  - Remark CoS: Enabled
  - Voice VLAN Aging Time: 1 Day 0 Hour 0 Min
- Port Setting:**
  - View By: Ports

Port	Voice VLAN Mode	Voice VLAN Security	Membership
gi1/0/1	Disabled	Unsecured	Excluded
gi1/0/2	Enabled	Unsecured	Included
gi1/0/3	Enabled	Unsecured	Included

  - 52 Item(s) Found.

Figure 18 X-Series Voice VLAN Parameters

## 7.2.5 LLDP-MED

The Link Layer Discover Protocol-Media Endpoint Discovery (LLDP-MED) protocol, in conjunction with the Voice VLAN feature, is used to set the QoS parameters. These parameters include the following:

- Voice VLAN ID
- Class of Service (CoS)
- Presence or absence of a VoIP phone on the port or network
- Phone Vendor information

Figure 19 shows the Dell Networking Administrator's Link Layer Discovery Protocol (LLDP) page for managing LLDP-MED. To enable this protocol, first create an LLDP-MED network policy and then assign the policy to individual ports connected to IP phones. The LLDP-MED network policy instructs the connected phones on how to send traffic. The policy created for the reference architecture instructs the phones to do the following:

- Send voice traffic on VLAN 10
- Tag voice traffic with CoS=6

These QoS parameters ensure that all voice traffic receives higher priority than regular data traffic when processed by the X-Series switches.

The screenshot shows the Dell Networking Administrator interface. The left sidebar contains a menu with options like VLAN, Port Settings, Spanning Tree and LAG, Link Layer Discovery Protocol (LLDP), Route Settings, Quality of Service, Security, SNMP, Monitoring, Multicast, DHCP Snooping and Relay, DHCP Server, Power Management, and sFlow. The main content area is titled 'Link Layer Discovery Protocol (LLDP)' and includes the following sections:

- LLDP Properties:** A table showing LLDP Status (Enabled), Updates Interval (Sec) (30), Hold Multiplier (Sec) (4), Reinitializing Delay (Sec) (2), and Transmit Delay (Sec) (2).
- LLDP Port Settings:** A section with an 'Edit' link.
- MED Network Policy:** A table showing Network Policy Number (1), Application (Voice), VLAN ID (10), VLAN Type (Tagged), User Priority (6), and DSCP Value (46). Below the table, it says '1 Item(s) Found.'.
- MED Port Settings:** A table showing Port (g1/0/1, g1/0/2, g1/0/3), LLDP MED Status (Disabled, Enabled, Enabled), Network Policy (No, Yes, Yes), Location (No, No, No), and Details (links to Details). Below the table, it says '52 Item(s) Found.'.
- Neighbors Information:** A section with an 'Edit' link.

Figure 19 X-Series LLDP-MED Parameters

## 7.2.6 VoIP Digital PBX

The SBRA VoIP solution uses a Windows-based software PBX system by 3CX. This open-standard unified communications VoIP platform works with standard SIP phones and can replace any proprietary PBX. Please refer to the [Voice Vlan section \(7.2.4\)](#) and the [LLDP MED section \(7.2.5\)](#) on the X-Series VoIP optimization features that are enabled for the SBRA.

**Note:** Locate a free version of the 3CX VoIP Phone System for Windows at the following web address:  
<http://www.3cx.com/phone-system/download-phone-system>.

Locate configuration guides at the following web address: <http://www.3cx.com/support>.



## 8 Small Business Reference Architecture - Mobility

Small businesses require the same high quality, reliable wireless networks that larger enterprises deploy. Dell Networking provides an extensive selection of enterprise-class WLAN solutions designed for the specific needs of small businesses. Figure 20 shows the W-Series Instant Access Points (W-IAPs) that this reference architecture uses to deliver enterprise capabilities with the simplicity of an entry-level deployment:

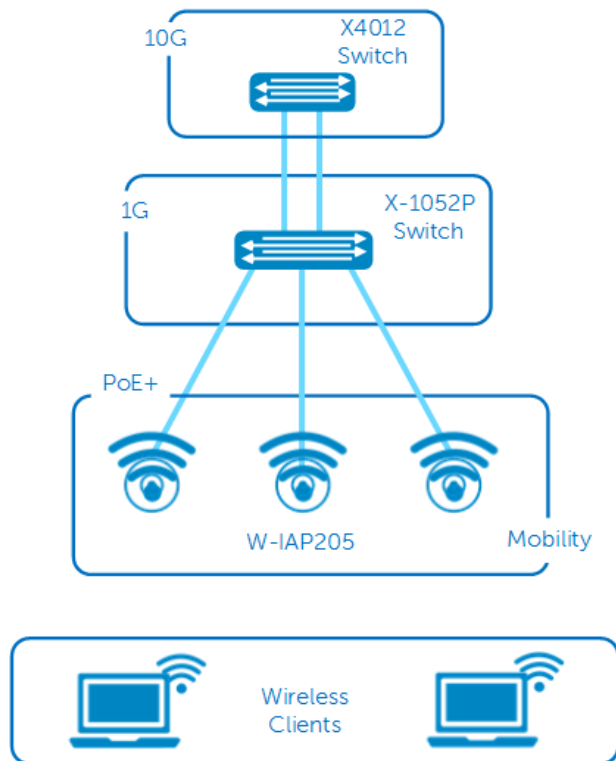


Figure 20 W-Series Instant Access Point Topology

**Note:** For more information on Dell W-Series Wireless Networking, see the Wireless Networking page at <http://www.dell.com/wireless>.

## 8.1 Important W-Series Features

The following sections outline some of the features and guidelines to consider while designing a wireless network using W-Series mobility products:

- **W-Series Instant Access Points** - Wireless access devices
- **W-Series Instant Access Point Virtual Controller** - Wireless controller used to configure wireless access points
- **WLAN Employee and Guest Network Settings** - Wireless networks for employees and guests
- **Wireless Intrusion Detection and Protection** - Component to identify and protect from wireless threats

### 8.1.1 W-Series Instant Access Points

The design of W-Series Instant Access Points (W-IAPs) equips them to provide enterprise-class networking services without enterprise-class complexity. Easy configuration means W-IAPs can be up and running in no time. As access and security requirements increase, administrators can add more features to their network.

W-IAPs allow small businesses to choose between quick and simple deployments and enabling a large variety of enterprise-grade features through an easy-to-use graphical user interface (GUI). W-IAPs also offer a level of high availability and uptime not provided by consumer-level products.

This SBRA uses the most basic settings for providing an employee and guest network. Configuration time, excluding physical installation, can be expected to take less than 10 minutes.

## 8.1.2 W-Series Instant Access Point Virtual Controller

W-IAPs feature a built-in virtual controller. As W-IAPs join the network, the virtual controller automatically configures them, enabling easy expansion without the requisite licenses or strict AP limitation concerns.

Figure 21 shows the main dashboard of the Dell Virtual Controller GUI administrators access to configure the W-IAPs and virtual controllers.

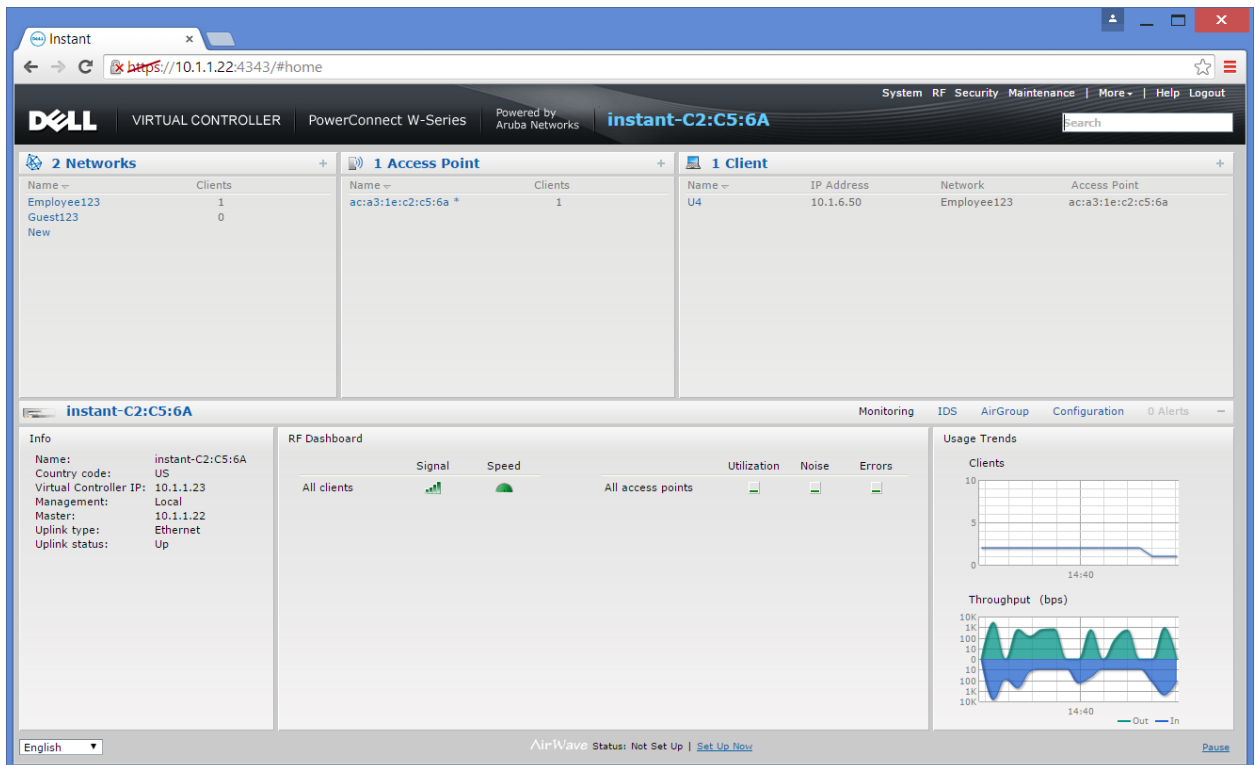


Figure 21 W-IAP Main Dashboard

Administrators can use DHCP to enable the IP assignment for the virtual controller and individual W-IAPs. Figure 22 shows the Virtual Controller System window, accessible through the System settings. In this example, the virtual controller is configured with a static IP address

**System** [Help](#)

General Admin Uplink L3 Mobility Enterprise Domains Monitoring WISPr Proxy

Name: instant-C2:C5:6A

System location:

Virtual Controller IP: 10.1.1.23

Dynamic RADIUS proxy: Disabled ▼

MAS integration: Disabled ▼

NTP server:

Timezone: International-Date-Lin ▼

Preferred band: All ▼

AppRF visibility: Disabled ▼

Virtual Controller Netmask: 255.255.255.0

Virtual Controller Gateway: 10.1.1.20

Virtual Controller VLAN: 1

Auto join mode: Enabled ▼

Terminal access: Enabled ▼

Console access: Enabled ▼

Telnet server: Disabled ▼

LED display: Enabled ▼

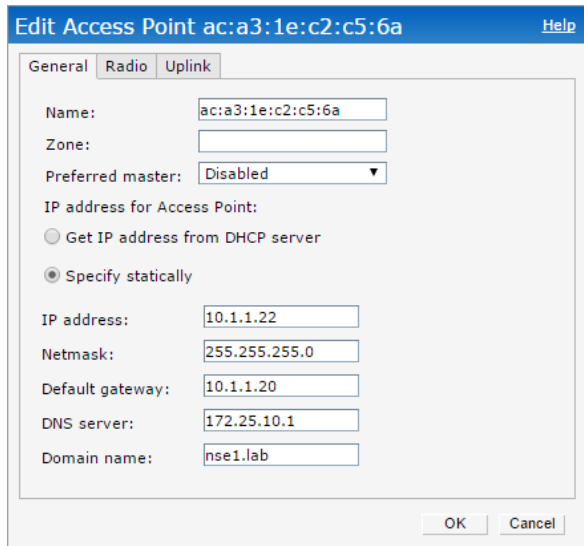
Extended SSID: Enabled ▼

Deny inter user bridging: Disabled ▼

[Hide advanced options](#) OK Cancel

Figure 22 Virtual Controller System Settings

Figure 23 shows the W-IAP settings, accessible through the Edit Access Point link window on the dashboard. In this example, the W-IAP IP address is set statically.



The screenshot shows a web interface titled "Edit Access Point ac:a3:1e:c2:c5:6a" with a "Help" link. It has three tabs: "General", "Radio", and "Uplink". The "General" tab is active. It contains the following fields and options:

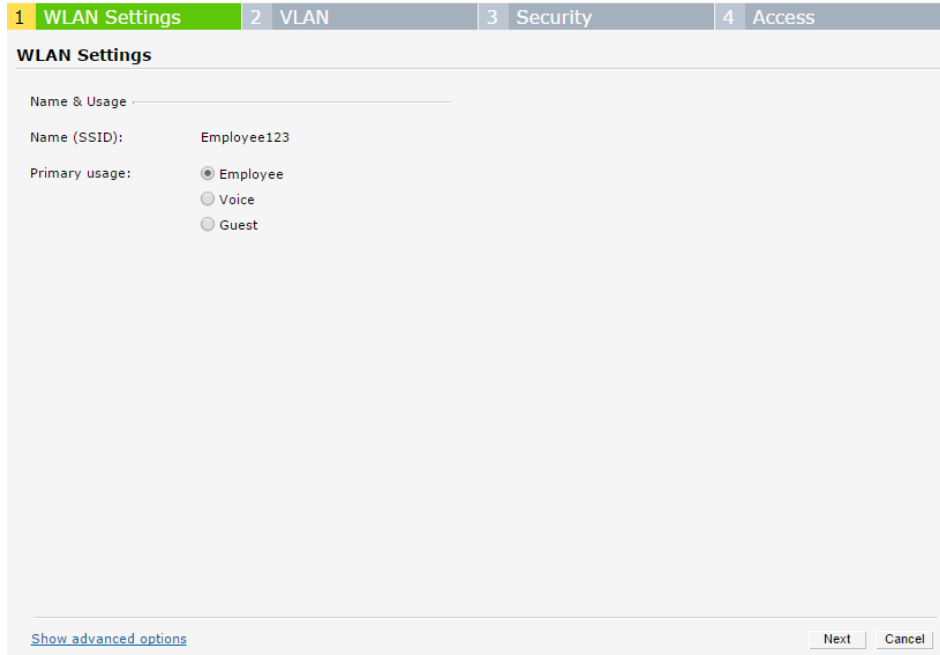
- Name: ac:a3:1e:c2:c5:6a
- Zone: (empty text box)
- Preferred master: Disabled (dropdown menu)
- IP address for Access Point:
  - ☐ Get IP address from DHCP server
  - ☒ Specify statically
- IP address: 10.1.1.22
- Netmask: 255.255.255.0
- Default gateway: 10.1.1.20
- DNS server: 172.25.10.1
- Domain name: nse1.lab

At the bottom right are "OK" and "Cancel" buttons.

Figure 23 Access Point General Settings

### 8.1.3 WLAN Employee and Guest Network Settings

Administrators can add WLAN Networks through the New Network wizard from the main dashboard. Figure 24 shows the WLAN Settings tab in the basic setup. This example shows an employee network.



The screenshot shows a wizard with four steps: 1. WLAN Settings (highlighted), 2. VLAN, 3. Security, and 4. Access. The "WLAN Settings" section is titled "Name & Usage". It contains the following fields and options:

- Name (SSID): Employee123
- Primary usage:
  - ☒ Employee
  - ☐ Voice
  - ☐ Guest

At the bottom left is a link "Show advanced options". At the bottom right are "Next" and "Cancel" buttons.

Figure 24 Employee WLAN Setting example

The remaining tabs allow the administrator to setup VLAN, security and access rules, which establish password and firewall rules. Some of the features in the basic setup include the following:

- Client IP assignment
- Client VLAN assignment
- Security settings (WPA2 Personal or Enterprise)
- Role and Network based access rules

For this reference architecture, client IP address assignment is implemented through a DHCP server located on the network. The W-IAP can also be used to manage the DHCP assignment of its wireless clients internally.

The W-IAPs' captive portal feature allows guest access. By using the captive portal, administrators can provide guests common or customized user accounts. Figure 25 shows the built-in Captive Portal page. Figure 26 shows the Security tab, which administrators use to configure the WLAN guest portal.

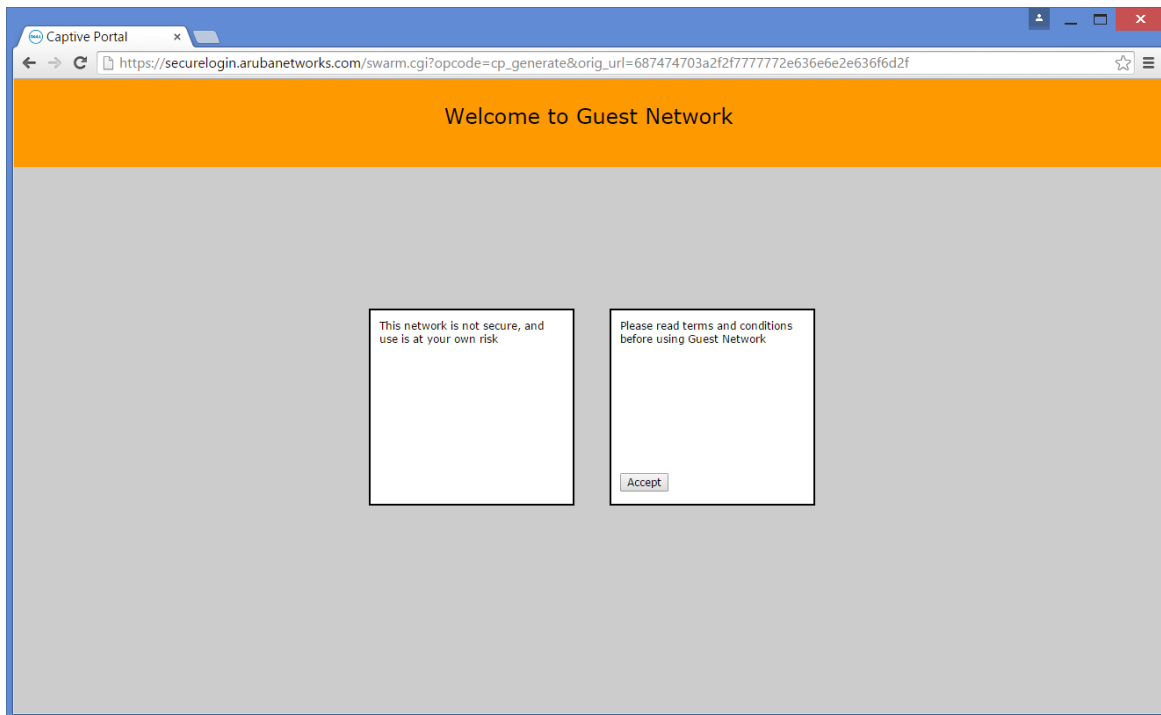


Figure 25 Captive Portal for an Open Network

Figure 26 Captive Portal WLAN Security Tab

Each area of the GUI has an advanced settings option, which provides additional settings for more complex features. This reference architecture highlights basic wireless network setup to show how easy it is to deploy a wireless network with minimal IT administrative expertise.

**Note:** For more information on basic and advanced setup of Dell Networking W-Series products, see the Instant User Guides at [Dell's Support Site](http://dell.com/support).

## 8.1.4 Wireless Intrusion Detection and Protection

Dell W-IAPs have Intrusion Detection System (IDS) and Wireless Intrusion Protection (WIP) features to identify and protect against wireless threats. Figure 27 shows some of the many types of intrusion threats these features can detect. Users can select sets of threats using a slider or the Custom Settings menu to customize detection for specific threats. Users also configure how IDS and WIP deal with identified threats. Users configure WIP settings through the More drop-down list in the upper right corner of the main dashboard. The IDS link on the main dashboard reveals the neighborhood and provides detailed monitoring information. Unknown access points and clients are classified as Interfering or Rogues.

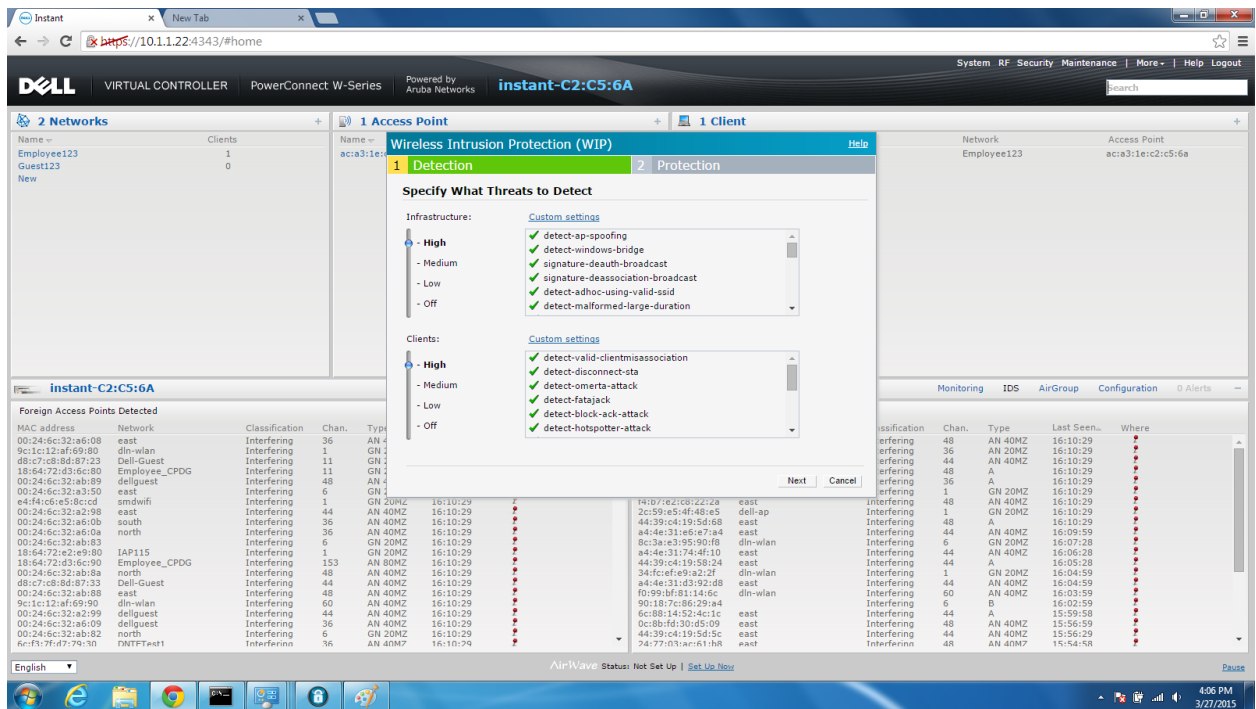


Figure 27 Wireless Intrusion Detection and Protection

The following lists provide details on some of the capabilities of the IDS and WIP features:

#### Detection Capabilities -

- AP Spoofing
- Windows Bridging
- Ad hoc networks
- AP Impersonation
- Flood Attack

#### Protection Capabilities -

- Wired containment
- Wireless containment
  - Deauthenticate
  - Tarpit



## 9 Small Business Reference Architecture - Firewall

The SBRA uses a SonicWALL TZ400 firewall as shown in Figure 28. This firewall solution from Dell EMC includes the ability to link the office LAN to as many as six Internet Service Providers (ISPs) using configurable WAN connections on the TZ400. Load balancing options include basic failover, round robin and spillover. The spillover method enables administrators to set a bandwidth threshold on a WAN interface and when that threshold is exceeded, new traffic flows are allocated to alternate WAN interfaces in a round robin manner.

**Note:** For more information, see the TZ400 and SonicOS manuals that are available on the [Dell SonicWALL TZ400 Product Support](#) website.

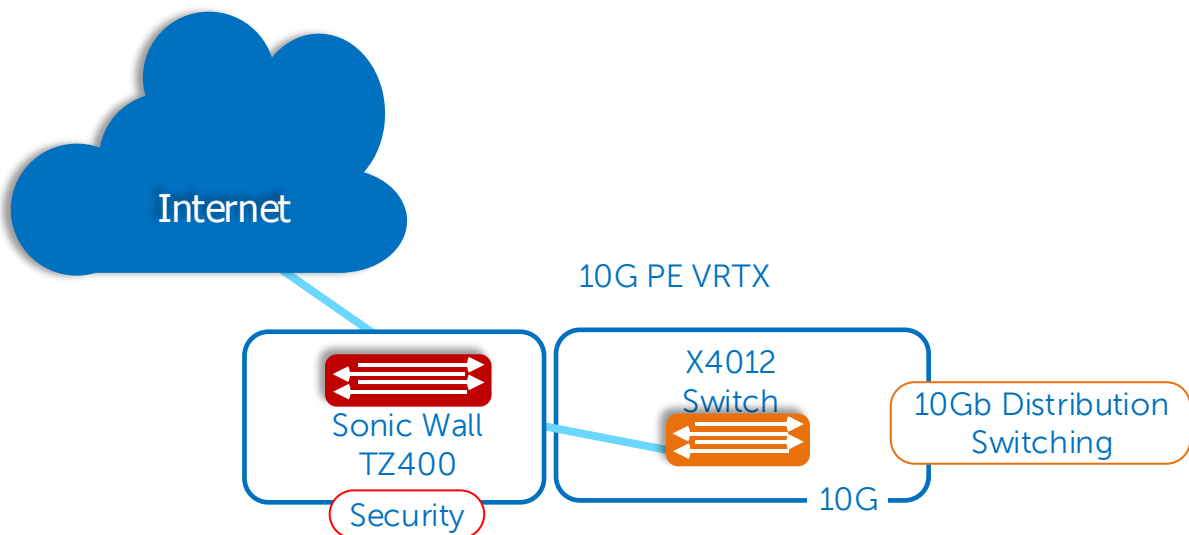


Figure 28 Small Business Reference Architecture firewall.

### 9.1 Important SonicWALL TZ400 Features

The following sections outline some of the features and guidelines to consider while implementing a firewall.

- **Security Services Licenses** – Licenses to activate TZ400 features
- **NAT Policies, Zones, and Firewall** – Policies for incoming and outgoing traffic

#### 9.1.1 Security Services Licenses

The Dell SonicWALL Unified Threat Management license integrates Gateway Anti-Virus, Anti-Spyware, Intrusion Protection and Application Intelligence as shown in Figure 29. Dell SonicWALL Unified Threat Management delivers real-time network security protection against sophisticated application layer and content-based attacks. These attacks can include viruses, spyware, worms, Trojans, software vulnerabilities and other malicious code. This heightened level of gateway protection addresses multiple threat access points and thoroughly scans all network layers.

**Note:** To view the Security Services Licenses, login to the SonicWALL TZ400, go to **System** and select **Status**.

Security Services	
Service Name	Status
Nodes/Users	Licensed - Unlimited Nodes
SSL VPN Nodes/Users	Licensed 2 Nodes (0 in use)
VPN	Licensed
Global VPN Client	Licensed - 2 Licenses (0 in use)
CFS (Content Filter)	Licensed
Expanded Feature Set	Not Licensed
McAfee AV Enforcement	Not Licensed
Client Content Filtering	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	Not Licensed
WXAC Acceleration	Licensed
Botnet	Licensed

Figure 29 SonicWALL UTM Licenses

### 9.1.2 NAT Policies

The Network Address Translation (NAT) engine in SonicOS allows users to define up to 512 granular NAT policies for incoming and outgoing traffic. By default, the Dell SonicWALL TZ400's preconfigured NAT policy allows all systems connected to the LAN interfaces to perform a many-to-one NAT. The NAT translates the interfaces' IP addresses into that of the default WAN interface on port X1. Therefore, the destination sees the request coming from the WAN port rather than from an internal private IP address.

The packets traversing the LAN and WAN interfaces contain (among other things) the requestor's IP address and protocol information, and the destination's IP address. The SonicOS's NAT Policies engine inspects the relevant portions of the packet and dynamically rewrites the information in specified fields for incoming and outgoing traffic.

To view the **NAT Policies** page, login to the SonicWALL TZ400. Expand **Network** in the left pane and choose **NAT Policies**.

Figure 30 shows the default SonicWALL NAT policies.

Network / **NAT Policies**

**NAT Policies**

Search:  Select: ☒ All Types ☐ Default ☐ Custom

#	Source Original	Source Translated	Destination Original	Destination Translated	Service Original	Service Translated	Interface Inbound	Interface Outbound	Priority
<input type="checkbox"/> 1	Any	Original	X0 IP	Original	Ping	Original	X0	X0	1
<input type="checkbox"/> 2	Any	Original	X0 IP	Original	SSH Management	Original	X0	X0	2
<input type="checkbox"/> 3	Any	Original	X0 IP	Original	HTTPS Management	Original	X0	X0	3
<input type="checkbox"/> 4	Any	Original	X0 IP	Original	HTTP Management	Original	X0	X0	4
<input type="checkbox"/> 5	All Interface IP	X1 IP	Any	Original	Any	Original	Any	X1	5
<input checked="" type="checkbox"/> 6	Any	X1 IP	Any	Original	Any	Original	X0	X1	6
<input type="checkbox"/> 7	Any	Original	Any	Original	Any	Original	Any	Any	7
<input type="checkbox"/> 8	Any	Original	X0 Management IPv6 Addresses	Original	Ping6	Original	X0	X0	8
<input type="checkbox"/> 9	Any	Original	X0 Management IPv6 Addresses	Original	HTTPS Management	Original	X0	X0	9
<input type="checkbox"/> 10	Any	Original	X0 Management IPv6 Addresses	Original	HTTP Management	Original	X0	X0	10
<input type="checkbox"/> 11	Any	Original	Any	Original	Any	Original	Any	Any	11

Figure 30 SonicWALL NAT Policies

### 9.1.3 Zones

A network security zone provides a logical method of grouping interfaces with user-configurable names, and applying security rules as traffic passes from one zone to another. Security zones provide an additional, more flexible, layer of security for the firewall. With zone-based security, an administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface. A best practice is to enable appropriate security services for each zone.

To view the **Zone Settings** page, login to the SonicWALL TZ400. Expand **Network** then select **Zones**.

Figure 31 shows the default security zones on the Dell SonicWALL TZ400:

The screenshot shows the 'Zones' configuration page in SonicWALL. It lists several default security zones with their respective settings.

Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Client AV	Client CF	Gateway AV	Anti-Spyware	IPS	App Control	SSL Control	SSLVPN Access	Configure
<input type="checkbox"/> DMZ	Public	N/A	✓	✓									[Edit] [Refresh]
<input type="checkbox"/> LAN	Trusted	X0 X2 X3 X4 X5 X6	✓	✓			✓	✓	✓	✓			[Edit] [Refresh]
<input type="checkbox"/> MULTICAST	Untrusted	N/A											[Edit] [Refresh]
<input type="checkbox"/> SSLVPN	SSLVPN	N/A									✓		[Edit] [Refresh]
<input type="checkbox"/> VPN	Encrypted	N/A											[Edit] [Refresh]
<input type="checkbox"/> WAN	Untrusted	X1					✓	✓	✓	✓			[Edit] [Refresh]
<input type="checkbox"/> WLAN	Wireless	N/A											[Edit] [Refresh]

Buttons: Add..., Delete

Figure 31 SonicWALL Zone Settings

## 9.1.4 Firewall

There are numerous firewall configuration options available in SonicOS under **Firewall** and **Firewall Settings** in the left pane of the GUI. Options include **Flood Protection**, **SSL Control**, **QoS Mapping** and **Access Rules**. Configure firewall access rules by zone or interface. Figure 32 shows a partial list of the SonicOS default access rules.

The screenshot shows the 'Access Rules' configuration page in SonicWALL. It displays a list of default access rules.

#	From	To	Priority	Source	Destination	Service	Action	Users Ind.	Users Excl.	Flow Report	Geo-IP Filter	Botnet Filter	Packet Monitor	Comment	Enable	Configure
<input type="checkbox"/> 1	LAN	> LAN	1	Any	All X0 Management IP	Ping	Allow	All	None						✓	[Edit] [Refresh]
<input type="checkbox"/> 2	LAN	> LAN	2	Any	All X0 Management IP	SSH Management	Allow	All	None						✓	[Edit] [Refresh]
<input type="checkbox"/> 3	LAN	> LAN	3	Any	All X0 Management IP	HTTPS Management	Allow	All	None						✓	[Edit] [Refresh]
<input type="checkbox"/> 4	LAN	> LAN	4	Any	All X0 Management IP	HTTP Management	Allow	All	None						✓	[Edit] [Refresh]

Figure 32 SonicWALL Firewall Access Rules

## 10 Small Business Reference Architecture - Compute

The Dell PowerEdge VRTX blade chassis provides is a preferred compute resource for a branch office, remote office or SoHo. The SBRA utilizes a Dell M630 half-height blade server for hosting the 3CX digital PBX VoIP solution for enabling the IP phones. The R1-2210 10GbE I/O Switching Module connects to the X4012 network-distribution layer switch via a two-cable 10GbE LAG. This high-bandwidth configuration ensures the availability of quality VoIP services when high bandwidth demand events occur, such as:

- Webinars
- Video conference calls
- Streaming media events

### 10.1 Important Dell PowerEdge VRTX features

The following section outlines some of the features and guidelines to consider while designing a network using the Dell PowerEdge VRTX R1-2210 I/O module.

- **Dell PowerEdge VRTX R1-2210 10GbE Ethernet I/O Module** – I/O module providing the uplink between internal, server-facing ports and external network resources

### 10.2 Dell PowerEdge VRTX R1-2210 10GbE Ethernet I/O Module

The R1-2210 I/O module is a 10GbE Ethernet switch with eight external-facing ports for uplinks and 16 internal, server-facing ports. The internal, server-facing ports support up to four Ethernet connections per blade server. The SBRA utilizes the R1-2210 to provide high-speed uplinks to the X4012 X-Series switch. These high-speed uplinks are configured as LAGs in order to allow enough bandwidth and high availability for all workloads on the VRTX M630 blade server.

Please refer to the [LAG section \(7.2.3\)](#), specifically Figure 15, for the R1-2210 LAG configuration.

**Note:** Please refer to the [Dell VRTX IO Module CLI and User Guides](#) for detailed configuration information.

## 11 Summary

The Dell Networking Small Business Reference Architecture showcases X-Series switches, W-Series mobility, SonicWALL security and VRTX compute product lines.

The SBRA provides guidance for modern offices and branches whose IT staff faces limited resources, but still must support all the office's IT needs (servers, networks, backup devices, applications etc.) while looking for simple, yet powerful, solutions. The Dell SBRA highlights a solution including both wired and wireless technology and combining the power of enterprise-level features with the ease-of-use and configuration usually reserved for consumer-level products.

## A Resources and References

### [Support.Dell.com](http://Support.Dell.com)

Dell EMC's Support Site – Manuals

### [DellTechCenter.com](http://DellTechCenter.com)

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

### [Dell Networking Guides](#)

Additional information on Dell Networking products

### [Wireless Networking page](#)

Additional information on Dell W-Series Wireless Networking

### [W-Series Whitepapers and Validated Reference Designs](#)

VRDs and Whitepapers

### [Dell Support Services for Network Security Products](#)

SonicWALL Support Site

### [Dell SonicWALL Security](#)

SonicWALL Products, Solutions and Whitepapers

### [Dell PowerEdge VRTX Page](#)

Specifications and White Papers

## B Attachments

This document includes the following attachments:

- X1052P Access switch.pdf
- X4012 Distribution switch.pdf
- R1\_2210 10GbE VRTX IO Module.pdf



## C 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](mailto:Dell_Networking_Solutions@Dell.com)