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

A Dell Deployment Guide

Dell Networking Solutions Engineering
July 2015

A Dell Deployment and Configuration Guide

Revisions

Date	Description	Authors
July 2015	Version 2.0 – Added wireless, removed 3CX CM	Colin King and Jeff Miller
May 2015	Version 1.1.1 – Added N1500 switches	Jeff Miller
March 2015	Version 1.1 – Added Cisco Unified CM, Cisco IP phones using DSCP and DNOS 6.2	Jeff Miller, Hemalatha Ganesan, Michael Mathews
May 2014	Version 1.0	Victor Teeter

Table of Contents

1 Introduction

Dell Networking provides customers with the most efficient use of modern networking equipment at the lowest cost for Data Center, Campus, and Remote networks. Dell Servers, Storage, and Networking products with Dell Solutions and Services enable organizations to achieve unique business goals, improve competitiveness and better serve their customers.

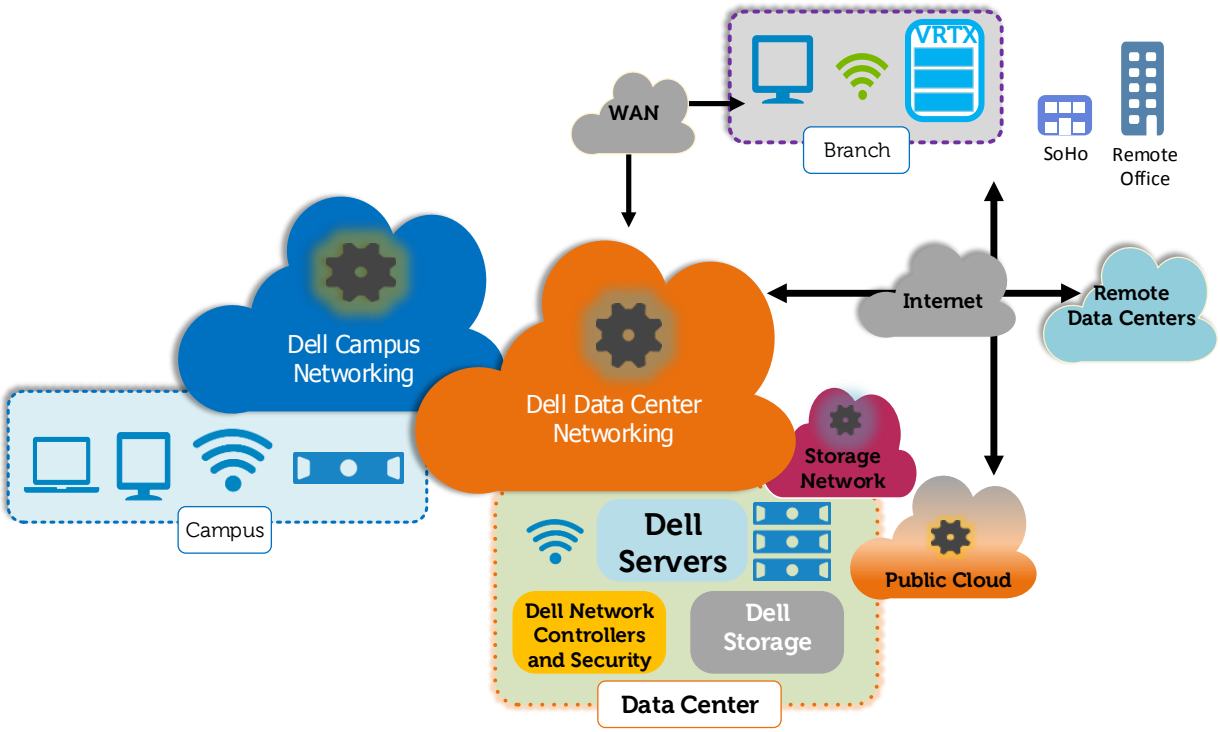

Figure 1 Comprehensive Modern Network

Dell Networking N-Series switches provide Quality of Service (QoS) features that ensure VoIP traffic is delivered with the high quality and low latency required to provide exceptional phone service to the user. This deployment guide provides information on QoS to help users set up and configure Dell Networking N-Series switches and W-Series WLAN controllers.

This paper can be used as a guide for any VoIP deployment regardless of the network topology, call manager or phone model used. The examples and information on QoS provide a foundation to enable any administrator to deploy high quality voice networks.

Dell Networking N-Series Wired Switches

Dell Networking N3000 switches are used in the examples in this document; however, any of the N-Series switches listed in Table 1 will accept the configurations used in this paper.

Table 1 N-Series Switches Validated for this Guide

N1524	N2024	N3024	N4032
N1524P	N2024P	N3024P	N4032F
N1548	N2048	N3024F	N4064
N1548P	N2048P	N3048	N4064F
		N3048P	

Dell Networking W-Series WLAN Controllers

Dell Networking W-7000 controllers are used in the examples in this document; however, any of the W-Series controllers listed in Table 2 will accept the configurations used in this paper.

Table 2 W-Series Controllers Validated for this Guide

W-7240	W-7030	W-3600
W-7220	W-7024	W-3400
W-7210	W-7010	W-3200
W-7205	W-7005	

VoIP Phone Models

The phones listed in Table 3 are the models used to validate the examples in this document. QoS settings on the wired and wireless networking equipment do not change when changing the model or phone equipment vendor.

Table 3 VoIP phones Validated for this Guide

Wired	Wireless
Cisco 9971	Cisco CP-7926G

VoIP Call Manager

The call manager used to validate the examples in this document is listed in Table 4.

Table 4 Call Manager Validated for this Guide

Cisco Unified Communications Manager v10.5

2 QoS for VoIP Deployments

Quality of Service (QoS) protocols provide reliable voice calls in the presence of data traffic on a network. Dell Networking N-Series switches and W-Series controllers support industry standard QoS protocols to classify and prioritize voice traffic. This section explains QoS methodology and features for both wired and wireless networks.

Quality of Service is used by networked devices to influence how traffic is delivered. QoS can be used to reduce latency in the delivery of traffic and/or ensure a particular traffic type is allocated a minimum or maximum amount of bandwidth. Reduced latency and jitter is critical in delay-sensitive applications such as VoIP. Several QoS mechanisms are used to accomplish these results, including classification, marking, policing, shaping, mapping and queuing.

2.1 QoS for N-Series Switches

Classification is used to identify the type of traffic entering an interface. Access Control Lists (ACLs) can be used to perform classification. Once the traffic has been classified, it is often marked. Marking traffic allows upstream network devices to perform QoS actions on the traffic without needing to perform classification all over again. Policing and shaping are mechanisms that control the bandwidth used for a particular traffic type. Each interface has a transmit buffer that is divided into several queues. Each queue is configured with a scheduling policy to determine the order in which frames are transmitted onto the network.

2.1.1 Differentiated Services Code Point (DSCP)

DSCP (also known as DiffServ) is a layer 3 marking mechanism that uses a 6-bit value found in the IP header. Dell Networking N-Series switches can be configured to trust the DSCP marking of incoming packets. A scheduling policy can then be applied for this traffic.

2.1.2 Queue Scheduler Types

The Dell Networking N-Series switches support two queue scheduler types: strict priority scheduler and weighted scheduler.

Strict Priority Scheduler

These queues are serviced first, before any weighted queues, with the highest numbered queue sending data first, advancing to the next highest strict queue until all queues have been serviced.

Weighted Scheduler

This queue scheduler type selects packets for transmission based on weights assigned to each queue. The default weight for each queue is equal to the Queue ID + 1. These weights are used to calculate the total number of bytes, not packets that are transmitted. The transmit buffers of each interface are comprised of these queues.

An example of these calculations is shown below.

1. Add 1 to each Queue ID value to find the weights of the queues (Table 5).
   For example, Queue ID 6 has a weight of 7.
2. Add together the weight values of the queues.
   In this case, the total weight of the queues is 22.
3. Divide the weight of each queue by the total weight to find the bandwidth percentage for that queue (Table 5).

Table 5 Calculating the Weight and Bandwidth of a queue

Queue ID	+ 1	= Weight	Bandwidth
0	+ 1	1	4% (1/22)
1	+ 1	2	9% (2/22)
2	+ 1	3	14% (3/22)
3	+ 1	4	18% (4/22)
4	+ 1	5	23% (5/22)
6	+ 1	7	32% (7/22)
Total Bandwidth:			**100% (22/22)**

Note: Queues in strict mode (Queue ID 5 in this example) are not included in the calculation.

A graphical representation of the calculated bandwidth for weighted queues (Table 5) is shown in Figure 2.

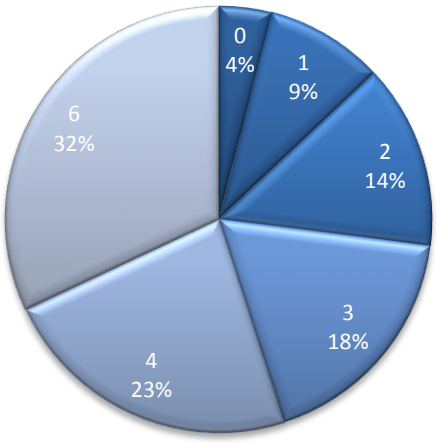

Figure 2 Calculated Bandwidth for Weighted Queues

2.2 QoS for W-Series Controllers

QoS features used to classify traffic for 802.11 are commonly called Wi-Fi Multi Media (WMM). WMM is a Wi-Fi Alliance certification based on the IEEE 802.11e standard for WLANs.

WMM is the QoS feature used for the RF medium and can be considered as over the air. Since wireless is a shared medium, transmissions are coordinated and controlled by the Access Point (AP). WMM shortens the time between packet transmission for traffic that is marked with a higher priority. While QoS on a wired medium is focused on bandwidth and the amount of traffic in queues, WMM is mainly focused on access to the wireless medium.

Priority and DSCP values are directly mapped to WMM classifications. W-Series has a default DSCP mapping scheme used to mark traffic for routing out to the greater wired infrastructure. Table 6 shows the default DSCP to WMM mapping.

Table 6 Priority and DCSP value to WMM classification mapping

Traffic Type	Priority	DSCP value	WMM Classification
Background	1	8	Background
Spare	2	16	
Best Effort	0	0	Best Effort
Excellent Effort	3	24	
Controlled Load	4	32	Video
Video	5	40	
Voice	6	48	Voice
Network Control	7	56	

Note: This mapping is calculated based on the hexadecimal to binary conversion of the DSCP value. The first three bits from the six-bit binary value are used to map back into a priority value, which corresponds to a WMM classification.

The default mappings shown above do not always correspond with an administrator's overall QoS scheme for wired and wireless integration. The W-Series provide a configuration option to use custom mappings to change the default behavior, which is detailed in Section 3.3. If DSCP values are being used and mapped to traffic queues on the wired network, it is convenient to use the same DSCP values in wireless as used on the wired network. For this document, the DSCP value of 46 is used for voice on the wired network, therefore a custom mapping is required for wireless.

3 VoIP-Wired and Wireless Deployment Example

3.1 Network Topology

The network topology used during the validation of the configurations is shown in Figure 3.

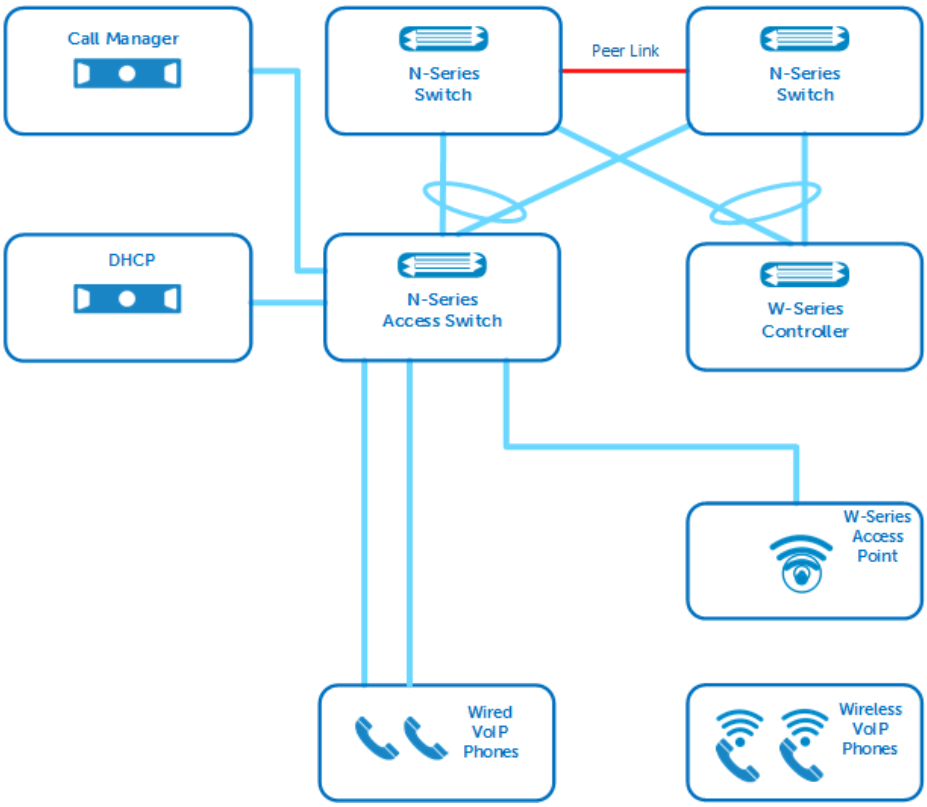

Figure 3 Wired and Wireless VoIP example topology

The topology above shows a campus network with a distribution layer, access layer and WLAN controller. The distribution layer in this example is comprised of two N-Series switches deployed in a MLAG configuration. The N-Series access switch and W-Series controller are connected to the distribution layer, while the APs and wired phones are connected to the access switch. The example configurations in the following paragraphs reference a single generic access switch. However, this topology is scalable to allow for many access switches, whether they are located in wiring closets or in the main data center.

3.2 Wired VoIP Configuration

3.2.1 Cisco Unified Communications Manager (CM) 10.5

The feature set of the Dell Networking N-Series switches enable seamless integration with Cisco's VoIP products. The example in this section, configures QoS on Dell Networking N-Series switches to use the DSCP values provided by the Cisco Unified CM environment.

Cisco recommends marking traffic to be handled by QoS as close to the edge as possible. Cisco IP phones accomplish this by downloading configuration files from the Cisco Unified CM when they boot up. Default DSCP values of 24 and 46 are used in this configuration for call control and voice streams, respectively. The Cisco phones mark their own traffic. As the example shows, only minimal configuration of the Dell Networking N-Series is needed to perform QoS and optimize VoIP traffic on the network.

3.2.2 Configuring the Cisco Unified CM

The default installation of Cisco Unified CM matches the DSCP values used in this example. The configuration value for Call Control is named "DSCP for Cisco CallManager to Device Interface" and found in Enterprise Parameters. The configuration value for streaming voice traffic is named "DSCP for Audio Calls" and found in the Service Parameter Configuration.

To verify these settings, follow the steps below.

1. Log into the Cisco Unified CM Administration Web UI.
2. Click on the **System** tab and then select **Enterprise Parameters**.
3. In the first section labeled **Enterprise Parameters Configuration**, observe the value for DSCP for Cisco CallManager to Device Interface – The default value is CS3, or 24 in decimal.
4. Click on the **System** tab and then select **Service Parameters**.
5. Select the Cisco Unified CM Server from the **Server** drop-down box.
6. Select **Cisco CallManager (Active)** from the **Service** drop-down box.
7. Scroll down the web page to the section labelled **Clusterwide Parameters (System – QOS)**. Observe the value for the setting **DSCP for Audio Calls** – The default value is 46.

Note: In this example, only a single Cisco Unified CM instance was installed. The CallManager service was not activated by default after installation.

Follow the steps below to confirm the service is activated and started.

1. Log into the Cisco Unified CM Administration Web UI.
2. From the drop down box in the upper right part of the screen, select **Cisco Unified Serviceability** and click **Go**.
3. Click the **Tools** tab and then click on **Service Activation**.
4. Select your Cisco Unified CM server from the drop down box and click **Go**.
5. If not checked, check the checkbox next to **Cisco CallManager** and click **Save**.
6. Click the **Tools** tab then **Control Center – Feature Services**.

7. Check the status of the **Cisco CallManager** service. If the service is not started, select the radio button next to the service name and click the **Start** button.

3.2.3 Dell Networking N-Series Configuration

The default setting of N-Series switches is to trust the dot1p markings of incoming traffic. Therefore, the first step in configuring the N-Series switch in a DSCP deployment is to configure the switch to trust the DSCP markings of your endpoints. This can be done with the global command **`classofservice trust ip-dscp`**.

Note: Interfaces can only be configured to trust one marking type (DSCP or dot1p) at a time.

The **`show classofservice ip-dscp-mapping`** command can be used to see the currently configured DSCP to Traffic Class (queue) mappings. The default DSCP markings for Cisco VoIP traffic are 24 (CS3) and 46 (EF). The default DSCP to queue mappings will place this traffic in queues 1 and 2, respectively. This example uses queue 5, so the default behavior needs to be changed so the DSCP values are mapped to queue 5. The commands **`classofservice ip-dscp-mapping 24 5`** and **`classofservice ip-dscp-mapping 46 5`** are used to do this.

The scheduling mode for queue 5 is set to strict priority with the command **`cos-queue strict 5`**. By setting queue 5 to strict, traffic in this egress queue will be transmitted before any packets in the weighted queues are processed. If multiple queues are set to strict, traffic in the highest numbered strict queue is sent first, then the next highest numbered queue, and so on. The default scheduler type for all queues is weighted.

The configuration commands used in this section can be entered in global or interface configuration mode. In these examples, the commands are configured in global configuration mode so that they are effective for all interfaces on the switch.

Enter the following commands on all of the N-Series switches.

All N-Series Switches	Description of commands
`configure`	
`voice vlan`	← *Globally enable Voice VLAN.*
`classofservice trust ip-dscp`	← *Trust incoming DSCP markings*
`classofservice ip-dscp-mapping 24 5` `classofservice ip-dscp-mapping 46 5`	← *Map DSCP markings 24 and 46 to queue 5*
`cos-queue strict 5`	← *Set queue 5 to strict priority scheduling*
`exit`	

Enter the following commands on the access switch. Note the first interface listed below is for the interface connected to a server containing the DHCP server and Cisco Unified CM.

Access Switch N3024P	Description of commands
configure interface gigabit 1/0/1 switchport access vlan 100 voice vlan 100 voice vlan auth disable interface range gigabit 1/0/2-24 switchport mode general switchport general allow vlan add 100 tagged switchport general allow vlan add 200 voice vlan 100 voice vlan auth disable exit	← *Assign access port for the Cisco Unified CM server, making sure it is in the Voice VLAN.* ← *Configure switch ports used by wired phones and PCs. Specify the voice vlan, and disable authentication.*

3.2.4 Configuring VoIP phones for Cisco Unified CM

Four Cisco phones are used in this example. Two 9971 Cisco phones are connected to the access switch. The remaining two phones are Cisco 7926G wireless handsets. Most wired Cisco phones, including those used in this example, have CDP and LLDP enabled by default. These are used to configure voice VLAN and PoE parameters. When using Cisco phones with Cisco Unified CM, the phones will download a configuration file automatically during boot-up in a process called auto-provisioning. For this to work, the phone needs to be configured with a TFTP server address and several steps need to be performed in the Cisco Unified CM Administration Web UI so that the phone can download a configuration file.

To configure a Windows Server 2012 DHCP server to assign the phones a TFTP server address, perform the following steps.

1. Open the DHCP Manager.
2. Expand the Scope being used for your VoIP phones.
3. Right-click on **Scope Options**, then click on **Configure Options...**.
4. Scroll down to, and check the **150 TFTP Servers** checkbox.
5. Enter the IP address of your Cisco Unified CM server and then click **Add**.

The following steps will configure the Cisco 9971 or 7926G IP phones used with the minimum configuration required to make and receive calls. Most production Cisco Unified CM environments will involve additional steps that are not covered in this guide. Before starting, you will need the MAC address of the phones you will be configuring.

1. Log into the Cisco Unified CM Administration Web UI.
2. Click on the **User Management** tab and then click on **End User**.
3. Click Add **New**.
4. Complete the following fields
   a. User ID.

b. Password.
c. Confirm Password.
d. Last Name.

5. Click **Save**.
6. Click the **Device** tab then **Phone**.
7. Click Add **New**.
8. Select the phone model in the dropdown box.
9. Click **Next**.
10. On the next page, complete the following fields.
11. In the **Device Information** section,
    a. Enter the phone's MAC address.
    b. Select **Default** from the **Device Pool** dropdown box.
    c. Select a Phone Button Template (e.g. "Standard 9971 SIP").
    d. Select a user in the **Owner User ID** dropdown box (select the user configured in step 4).
12. In the **Protocol Specific Information** section,
    a. Select a Device Security Profile for your phone model.
    b. Select **Standard SIP Profile** from the SIP Profile dropdown box. (N/A for Cisco 7926G)
13. Click **Save**, then click **OK** to acknowledge the message from the webpage.
14. Click on **Line [1] – Add a new DN** to assign a phone number to this phone.
15. Configure the **Directory Number** field (e.g. 3006).
16. Click **Save**.
17. Scroll to the end of the page and click **Associate End Users** button.
18. In the next Pop-Up window, click the **Find** button to list all Users on the system.
19. Click the checkbox next to the User ID that you want to associate with this phone and then click **Add Selected**.
20. Click **Save**.
21. Click on the **User Management** tab and then **End User**.
22. Click the **Find** button to list all the users on the system.
23. Click on the User ID of the user configured in step 4.
24. Click on the **Device Association** button, located about half way down the page.
25. Click the **Find** button to list all User Device Associations.
26. Click the checkbox next to the **Device Name** just added. The device name will be **SEP** followed by the MAC address entered in step 11a.
27. Click **Save Selected/Changes**.

Repeat the steps above for each phone to be configured.

Plug the phones into the N3000 Series switch. If the phones are already plugged in, power cycle them by disconnecting them from the switch or disabling the interface they are plugged into, and then enabling the interface using the **`shutdown`** and **`no shutdown`** commands for the interfaces from the appropriate switch CLI.

3.2.5 Connecting PCs to Phones

Most IP phones today incorporate a multi-port switch. This allows for a single cable connection from the switch to the user location for both the IP phone and a PC. To allow PC traffic to transmit without hindering the voice traffic, the PC and IP phone are placed into separate VLANs. Figure 4 shows how different device types are associated with each of the two VLANs.

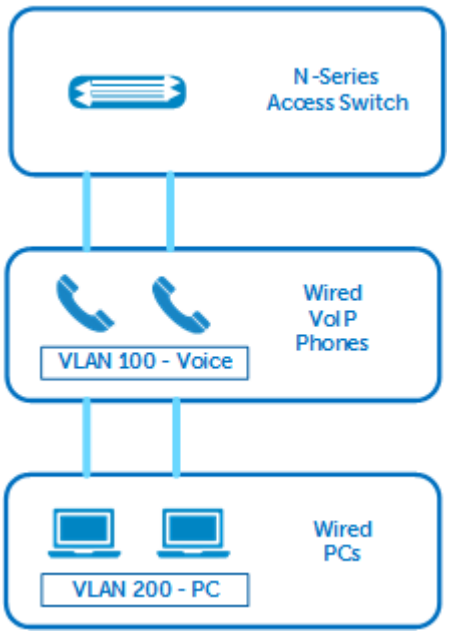

Figure 4 Connecting PCs to IP Phones

The configurations in this document already separate voice and data traffic. The Port VLAN ID (PVID) is the only remaining setting that needs to be configured to allow the phones to see and then pass non-voice traffic. The PVID will take all incoming untagged frames, like those coming from a PC connected to the phone, and tag each one as a VLAN 200 frame.

Setting the PVID on a switch port with both a phone and PC connected will allow proper operation of both voice on the phone and data on the PC. For port security in production environments, consider using 802.1x to provide authenticated, unauthenticated and guest VLANs on your network. More details on configuring 802.1x authentication can be found in the Dell Networking N-Series User Guide.

The following table includes the entire set of commands to configure an interface with a PVID. For this example, the phone plugged into port Gi1/0/14 has a PC connected that needs access to data VLAN 200.

Commands	Description of commands

`configure`
 	
`interface Gi1/0/14`
`switchport mode general`
`switchport general pvid 200`
`switchport general allowed vlan add 200`
`switchport general allowed vlan add 100 tagged`
`voice vlan 100`
`voice vlan auth disable`
	
	← set the PVID for untagged (non-voice VLAN 200) frames
	← these commands are required on the port to separate voice and data traffic

3.3 Wireless VoIP Configuration

3.3.1 Cisco Unified Communications Manager (CM) 10.5

The call manager for the WLAN VoIP phones is the same installation as described in Section 3.2.2. With the exception of the individual phone settings, no additional configuration is necessary.

3.3.2 Configuring VoIP phones for Cisco Unified CM

Configuring VLAN VoIP phones is included in the procedure described in Section 3.2.4. Ensure the correct phone model number is selected. The WLAN phones used in this example are Cisco Skinny Client Control Protocol (SCCP) based, while the wired phones use Session Initiation Protocol (SIP).

3.3.3 Dell Networking W-Series Configuration

While many phones are capable of data and voice, including soft phones (PC based), the WLAN VoIP phones used in this example are assumed to deliver mainly voice traffic.

Dell Networking W-Series Controllers and Access Points are capable of supporting many virtual access points. Each virtual access point is its own WLAN, operating with its own SSID. For this example, the WLAN network will be split into two virtual access points, one for voice and one for data. The WLAN VoIP phones will associate to a SSID named "Voice". All other devices using data are associating to a SSID named "Data". Figure 5 shows the AP Group settings with the two virtual access point profiles.

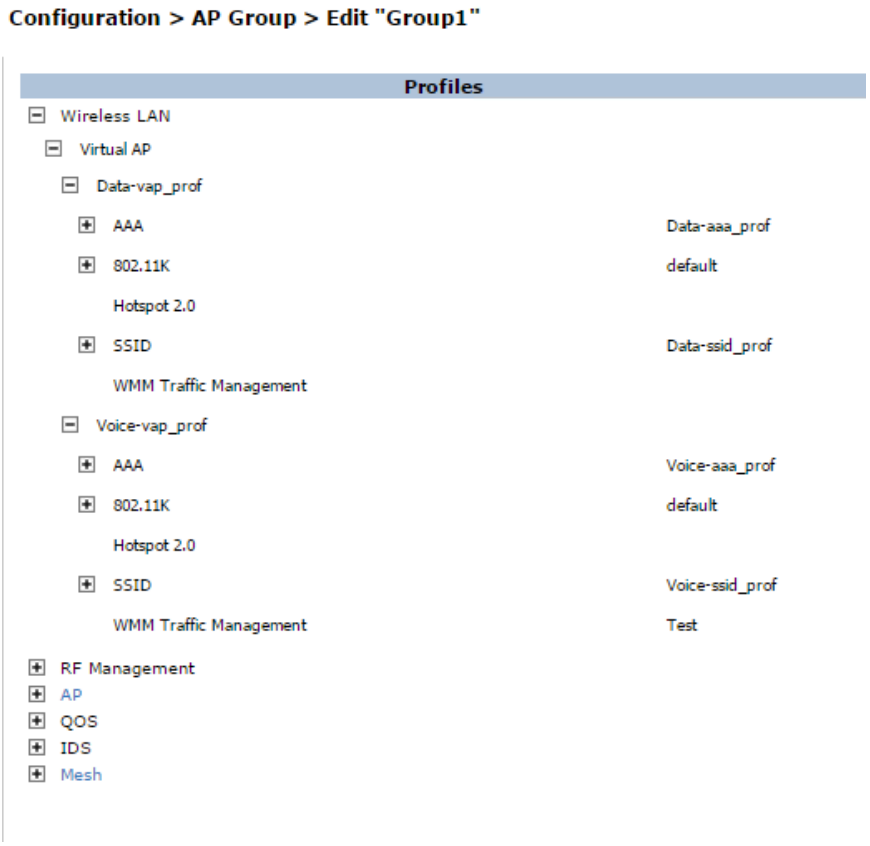

Figure 5 W-Series AP Group with virtual access point configuration

Note: The configuration of the basic WLAN network is not shown in this document. Only the applicable QoS and key settings related to the example are described. For assistance on configuring a W-Series controller, see the User Guide located at http://dell.com/support.

To enable Wireless Multimedia (WMM), navigate to the "Voice" SSID profile and click on the advanced tab. Figure 6 and Figure 7 show a split view of the SSID profile and Advanced tab area where the WMM setting is located. Click on the checkbox to enable WMM.

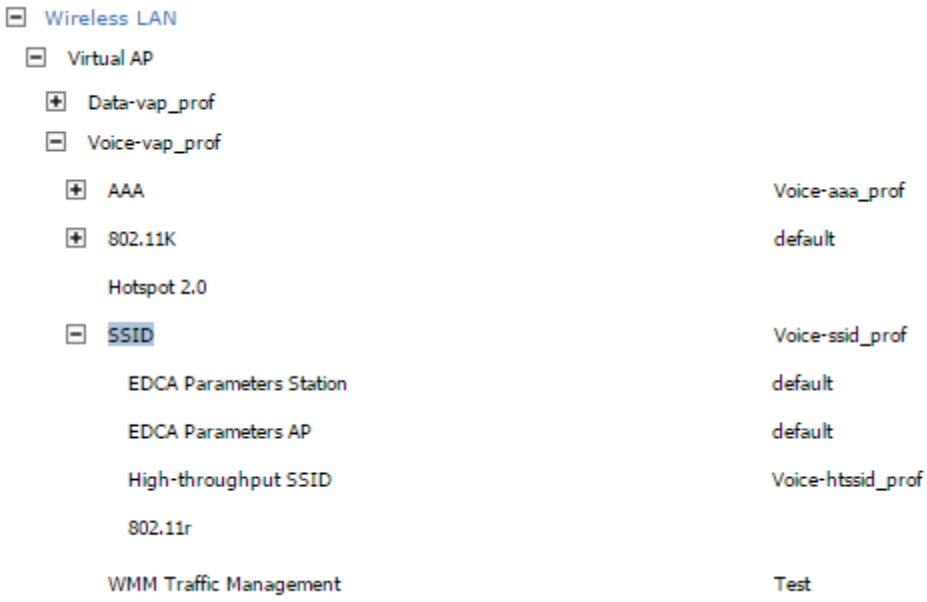

Figure 6 W-Series SSID profile, "Voice" SSID selected

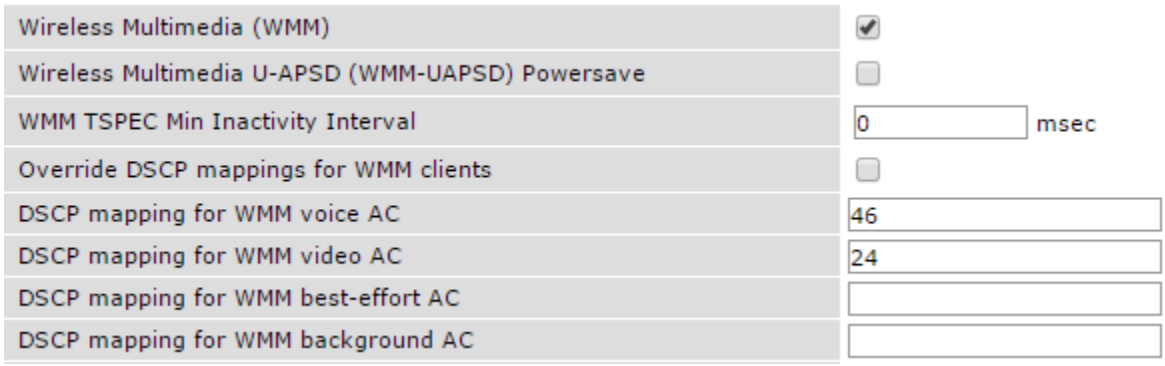

Figure 7 W-Series Advanced Tab, WMM settings

Within the same location, the custom mapping for DSCP values to WMM can bet set. In this example, the wired network and wired phones are using DSCP of 46 for voice traffic and 24 for call control traffic. For continuity between wired and wireless, a custom mapping is being used to force all voice traffic to be translated to a DSCP value of 46. Without this custom mapping, voice traffic marked with a priority of 6 would be mapped to a DSCP value of 48, as shown in Table 6.

All traffic originating from the WLAN VoIP phones used in this example are marked with a priority value of 6. Other WLAN VoIP phones models may have different default settings or options. See the appropriate user guide of the WLAN VoIP phones for your deployment.

The WMM checkbox is the only setting that is required for wireless QoS to be enabled and function. Any client associating to a SSID that has WMM enabled and can support WMM itself, can have its traffic

prioritized according to the four WMM classifications. The next section describes some additional features on W-Series that have an effect on voice quality and traffic priority.

3.3.4 W-Series Policing Policies and Miscellaneous Features

Wireless Multimedia (WMM) is the main mechanism for enabling prioritization of voice traffic. However, there are several other considerations in the features and behavior of wireless clients that can greatly affect voice quality. The following items are presented as configurable options to consider in any wireless network. How much of an effect changes in these options have on voice quality will depend on many factors including other traffic types, wireless interference, client behavior, etc. It is recommended that the use of any of these features be evaluated based on the unique environment and traffic requirements of each wireless network.

WMM Traffic Management Profile

When the wireless medium is congested, a traffic management profile can be used to further specify sharing priority of the wireless spectrum. This profile is configured on a per SSID basis, and is located within the virtual AP profile. Figure 8 shows the profile with some arbitrary values set.

Figure 8 W-Series WMM Traffic Management

Traffic Management – Virtual AP

Traffic management can also be applied on a per band basis, setting access percentages for each virtual AP. This method is especially useful if voice traffic is highly concentrated to a particular virtual AP or SSID, as done in this document's example. This profile is located within the AP Group settings under QOS. Figure 9 shows the profile for the 802.11a band with some arbitrary vales set.

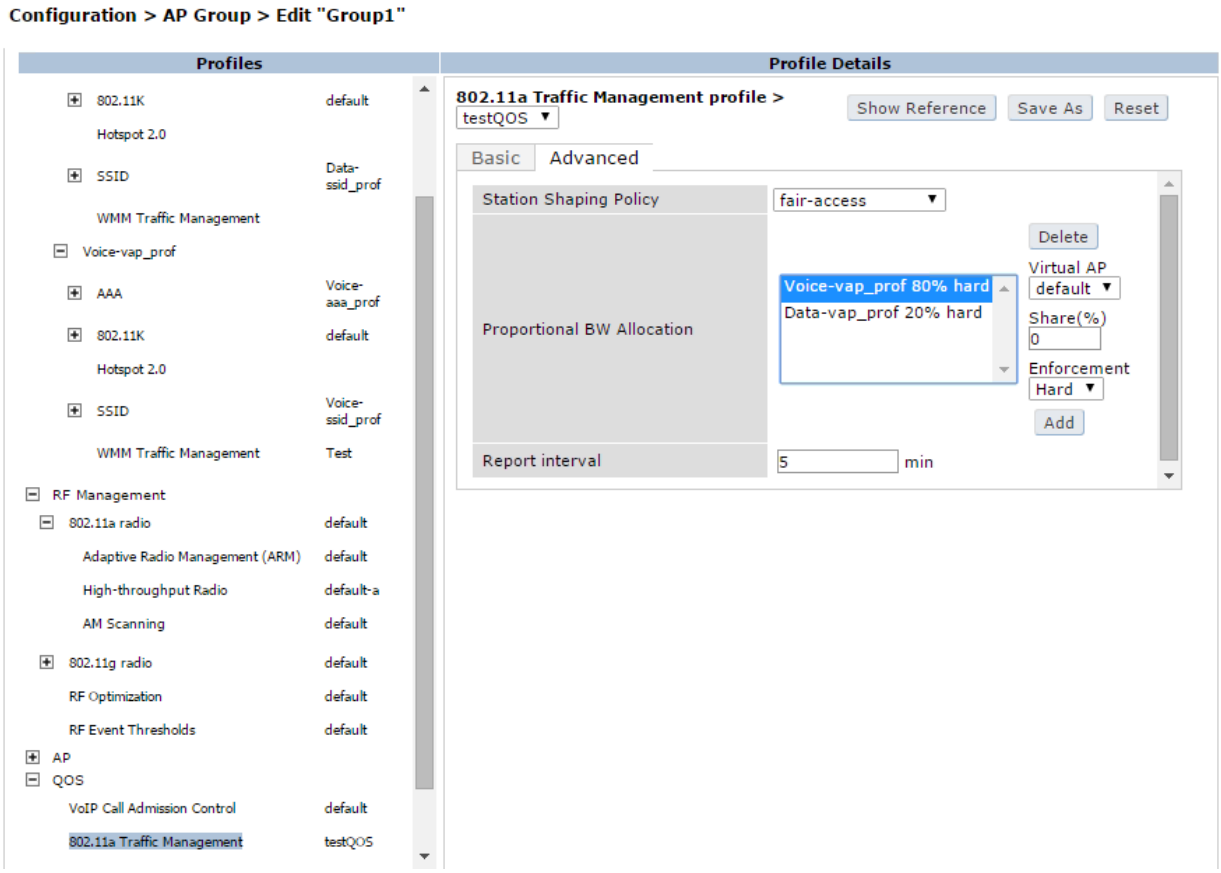

Figure 9 W-Series QOS Traffic Management

Adaptive Radio Management Features

W-Series controllers automatically manage the RF spectrum. Adaptive Radio Management (ARM) adjusts the RF properties of access points to ensure optimal performance. There are settings within the ARM feature that can further aid in voice quality. The following can be enabled to increase voice quality:

- VoIP Aware Scan – prevents scanning during active calls.
- Band Steering – encourages client devices to use 5GHz, which is commonly less congested.
- Spectrum Load Balancing – balances the number of clients associated per AP within a given area.

The following figures show these ARM settings:

For VoIP aware scan (Figure 10), navigate to the RF Management profile within the AP Group. ARM settings are configured per band.

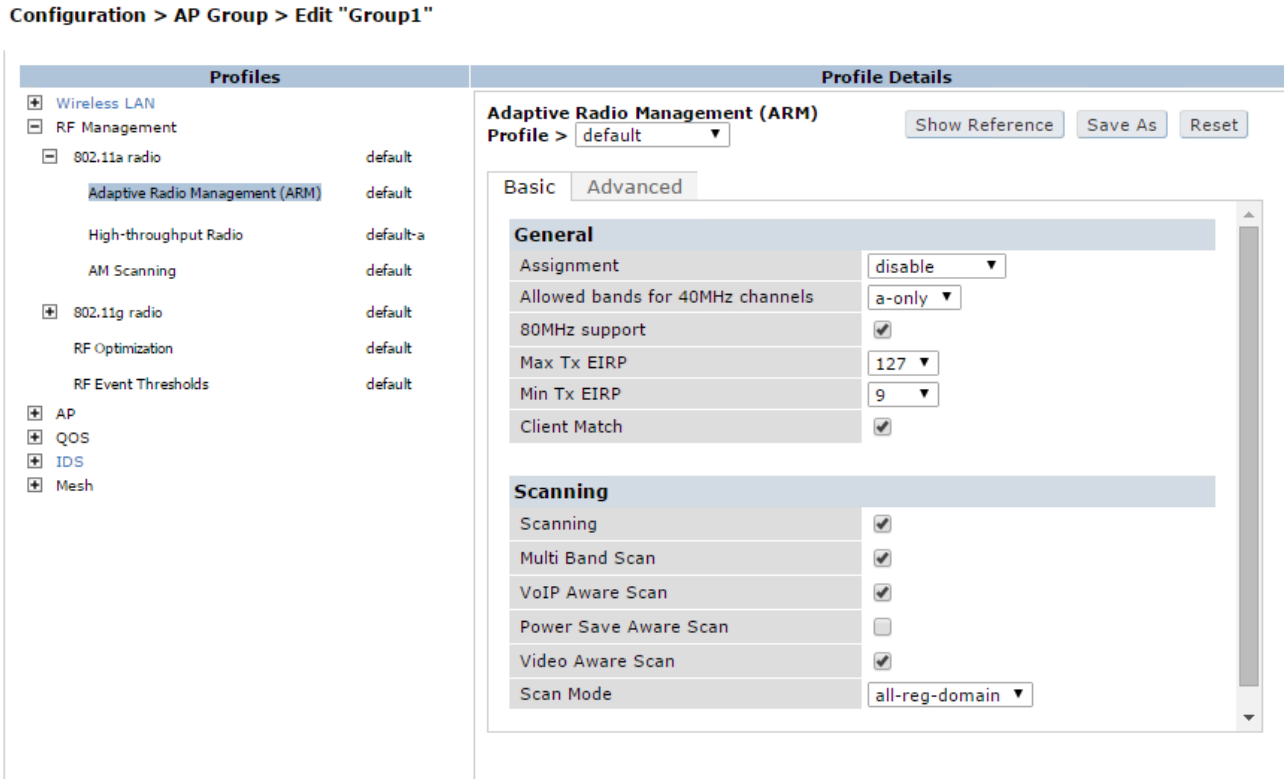

Figure 10 W-Series ARM VoIP Aware Scan

For Band Steering (Figure 11), navigate to the Basic tab of the appropriate virtual AP profile.

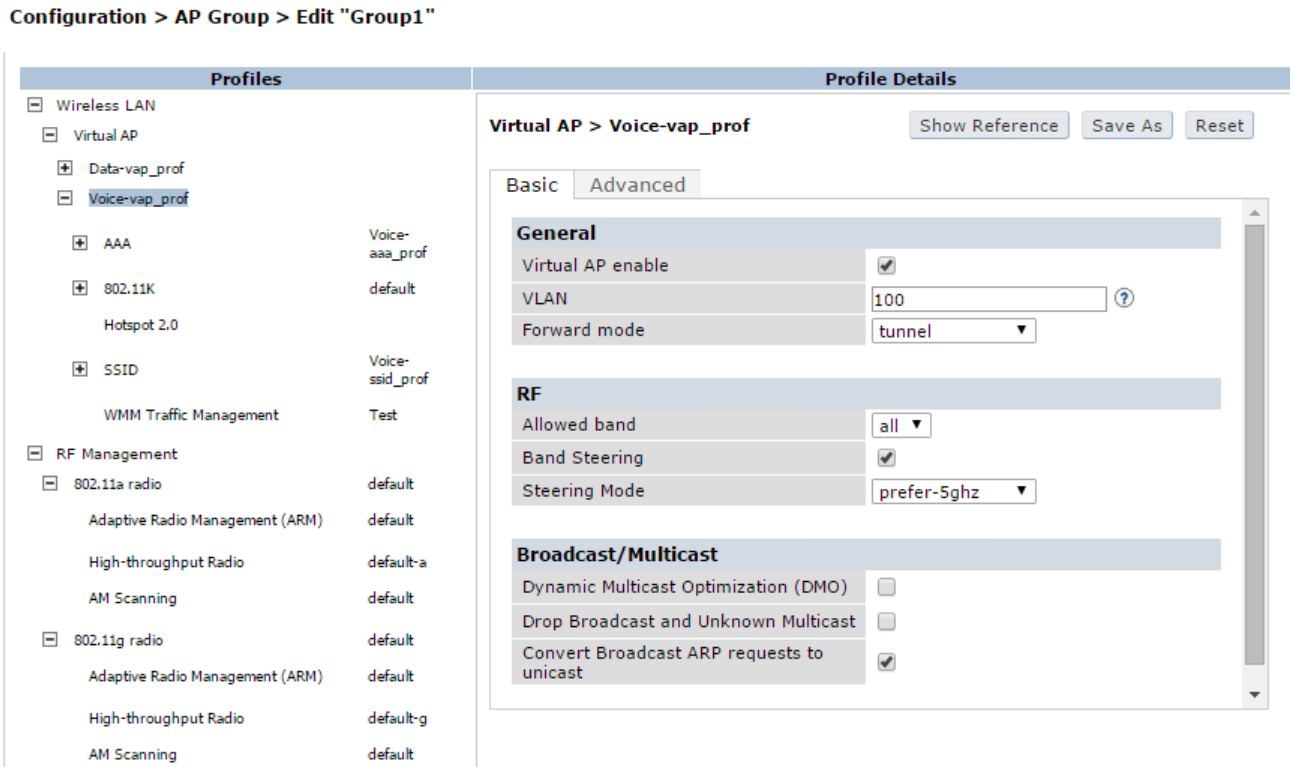

Figure 11 W-Series ARM Band Steering

For Spectrum Load Balancing (Figure 12), navigate to the RF Management profile within the AP Group. ARM setting are configured per band, and Spectrum Load Balancing is in the Advanced tab.

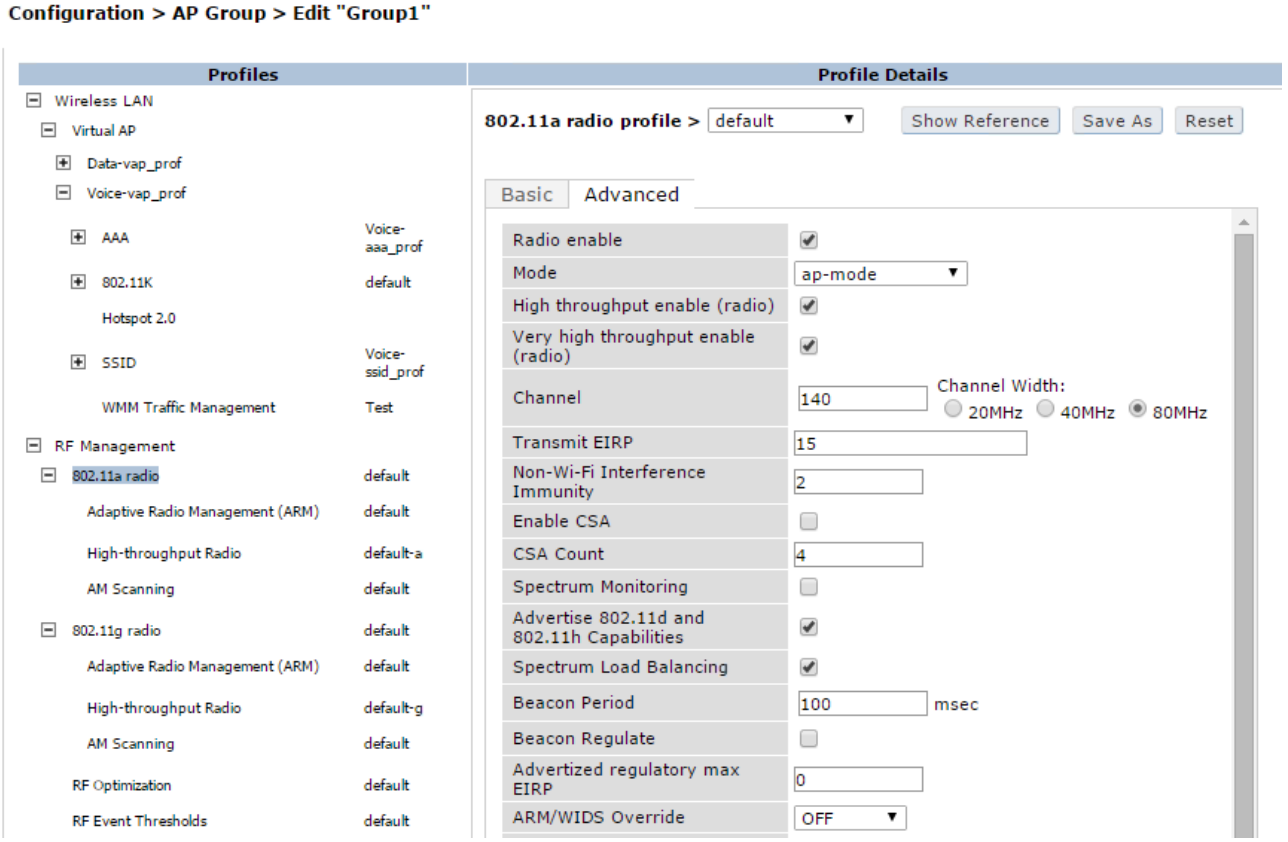

Figure 12 W-Series ARM Spectrum Load Balancing

Maximum Transmit Attempts and Maximum Transmit Failures

Setting the maximum transmit attempts and failures can help a client in a situation of poor signal strength or possibly interference. Fewer attempts and failures can promote a client to associate to a better access point. When configuring these settings, there is no absolute recommendation for every environment. Certain WLAN phones have preferred or best practice settings. The values in the screenshots below (Figure 13 and Figure 14) are arbitrary, and may not be best for your deployment.

Navigate to the appropriate AP Group, virtual AP, SSID profile. These settings are located in the Advanced tab of the SSID profile.

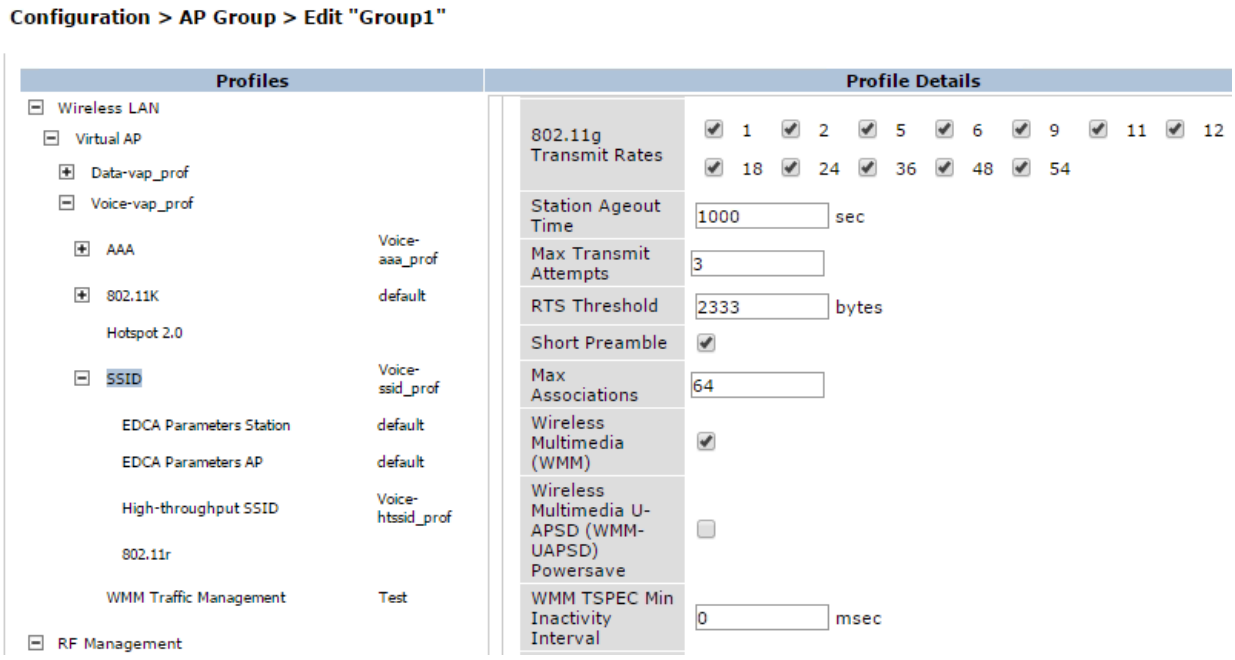

Figure 13 W-Series Max Transmit Attempts

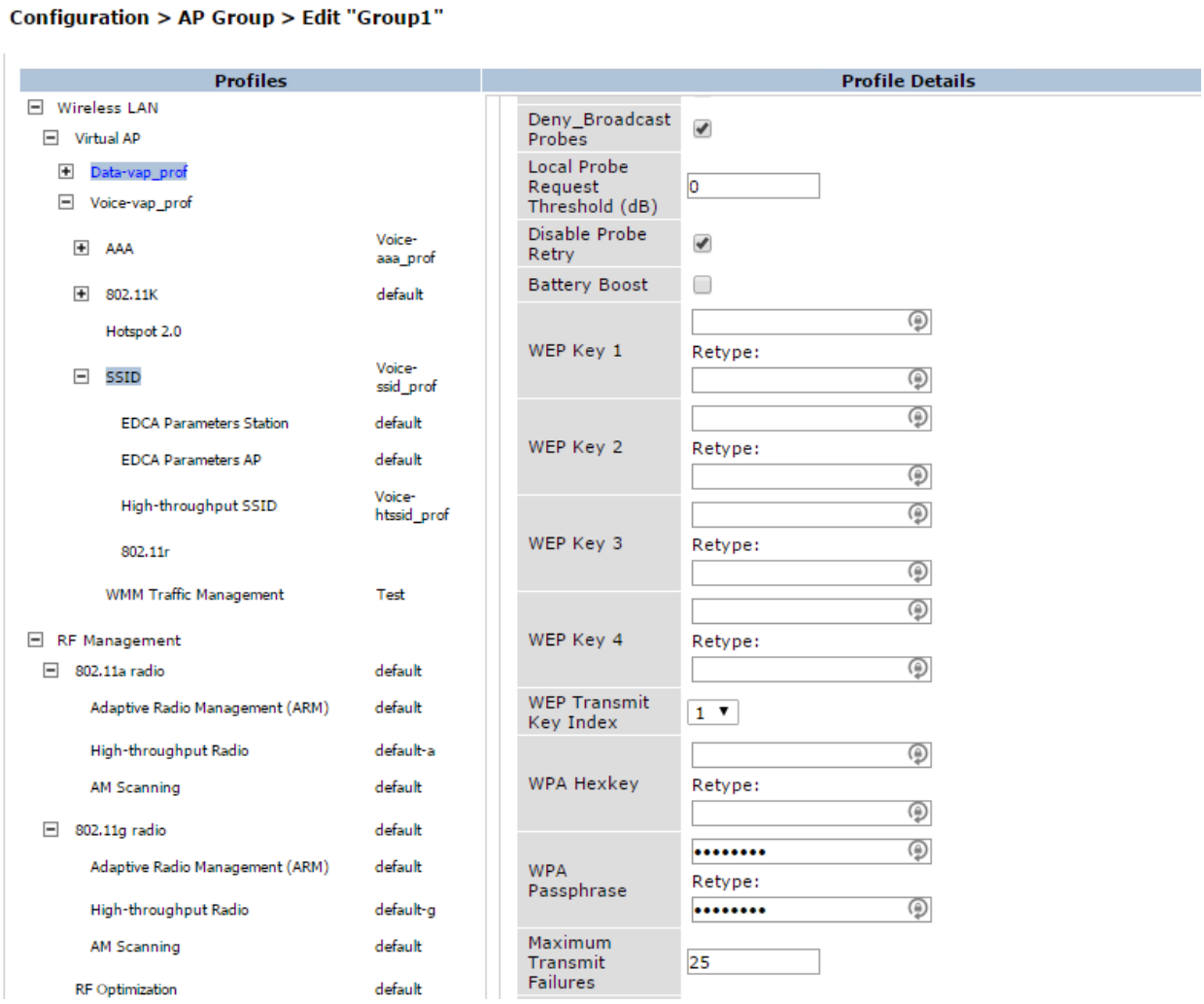

Figure 14 W-Series Maximum Transmit Failures

4 Conclusion

Dell Networking provides customers with a wide variety of solutions for their networking requirements. VoIP is a progressively critical service on modern networks, and administrators need the right features to optimize these networks. This document details two features, DSCP and WMM, which enable the reader to improve voice quality on wired and wireless networks.

A Additional Resources

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

DellTechCenter.com is an IT Community where you can connect with Dell Customers and Dell employees to share knowledge, best practices and information about Dell products and installations.

Referenced or recommended Dell publications:

- Dell Networking Whitepapers
  http://en.community.dell.com/techcenter/networking/p/guides
- Dell Networking N-Series User Guides
  http://en.community.dell.com/techcenter/networking/p/guides#N-series
- Dell Networking N-Series Firmware Downloads
  http://www.dell.com/support/home/us/en/04/Products/ser_stor_net/networking/net_fxd_prt_swtchs
- Dell Networking W-Series User Guides
  http://www.dell.com/wireless
- Dell Networking W-Series Firmware Downloads
  http://www.dell.com/wireless

B Configuration details

This paper was compiled using the following components and versions (Table 7).

Table 7 Components and Versions

Component	Version
Dell Networking N2000, N3000, N4000 series	6.2.0.5 firmware
Dell Networking N1500 series	6.2.5.0 firmware
Dell Networking W-Series	6.4.2.8 firmware
Dell Server	PowerEdge R620
Server Operating System	Microsoft Windows Server 2012 R2 Standard
Cisco UCS C-Series Server	C220
Cisco Unified CM	10.5
Cisco VoIP Phones	Models 9971 and CP-7926G

C Design Validation

During the validation of the configurations in this paper, high volume Ixia VoIPSIP validation tests were performed on the overall topology. A score of **A** was awarded for the number of calls that were successfully executed, as well a score of **A** for the Voice Quality. During the two-hour test, over 1.6 million calls were attempted and 1.6 million calls were completed with zero failures. Zero calls were dropped, and zero packets were lost. The setup involved using 30,000 virtual phones connected to 20 ports, with half of the phones calling the other half and "talking" for an average of 33 seconds. Audio statistics showed nearly one trillion bytes sent and one trillion bytes received.

A second validation test was performed to test the strict scheduling for queue 5. This test involved oversubscribing the switches to produce congestion and a traffic mix of voice and non-voice traffic to utilize multiple queues. During this two-hour test, normal layer 2 packets were dropped in other queues but no calls were dropped in the strict queue, which contained the highest priority of all traffic, voice traffic.

Validation of wireless network included air packet captures to verify WMM tagging.

Wireless performance related configurations were verified using IXIA IxVeriWave simulations.

D Status and Diagnostic Tools

The following section provides commands and tools useful during troubleshooting and configuring the network.

D.1 N-Series Switch Show Commands

The following show commands can be used to troubleshoot the concepts in this document.

The **show lldp remote-device all** command displays LLDP supported phones that have been discovered by the switch.

```
show lldp remote-device all

 LLDP Remote Device Summary

 Local
 Interface  RemID  Chassis ID         Port ID            System Name
 ---------  -----  ------------       ---------------    ---------------
 Gi1/0/10   6      192.168.1.201      000413485F67:P1    snom821
 Gi1/0/23   2      D0:67:E5:95:0B:83  Te1/1/2
 Gi1/0/24   1      D0:67:E5:95:0B:57  Te1/1/2
```

The **show lldp remote-device detail gigabitethernet 1/0/10** command can be run on the port that the LLDP phone resides to gather more information.

```
show lldp remote-device detail gigabitethernet 1/0/10

 LLDP Remote Device Detail

 Local Interface: Gi1/0/10

 Remote Identifier: 6
 Chassis ID Subtype: Network Address
 Chassis ID: 192.168.1.201
 Port ID Subtype: Local
 Port ID: 000413485F67:P1
 System Name: snom821
 System Description: snom;snom821-SIP 8.7.3.25;lid:8.7.3.25
 Port Description: NET PORT
 System Capabilities Supported: bridge, telephone
 System Capabilities Enabled: bridge, telephone
 Time to Live: 145 seconds
```

The **show isdp neighbors** command displays ISDP supported phones that have been discovered by the switch.

```
show isdp neighbors
 Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge,
            S - Switch, H - Host, I - IGMP, r - Repeater
 Device ID        Intf     Holdtime Capability Platform           Port ID
 ---------------  -------  -------- ---------- --------------    -------
 SEP0004f24cfd5d  Gi1/0/8   124      H          Polycom SoundPoi  Port 1
 N4000-38         Gi1/0/23  165      R          N4064F            Te1/1/1
 N4000-37         Gi1/0/24  158      R          N4064F            Te1/1/1
```

The **show isdp neighbors gigabitethernet 1/0/8 detail** command can be run on the port the ISDP phone resides to gather more information.

```
show isdp neighbors gigabitethernet 1/0/8 detail

 Device ID                SEP0004f24cfd5d
 Address(es):
   IP Address:            192.168.1.200
 Capability               Host
 Platform                 Polycom SoundPoint IP 335
 Interface                Gi1/0/8
 Port ID                  Port 1
 Holdtime                 142
 Advertisement Version    2
 Time when last changed   7 days 23:51:08
 Version:
 BootROM: 4.3.1, App: 3.3.3
```

The **show voice vlan** command can be used to verify the voice vlan is enabled globally.

```
show voice vlan

 Administrative Mode.............. Enable
```

The **show voice vlan interface gigabitethernet 1/0/8** command displays voice VLAN details for the port specified.

```
show voice vlan interface gigabitethernet 1/0/8

 Interface..................................... Gi1/0/8
 Voice VLAN Interface Mode..... Enabled
 Voice VLAN ID..... 100
 Voice VLAN COS Override..... False
 Voice VLAN DSCP Value..... 46
 Voice VLAN Port Status..... Enabled
 Voice VLAN Authentication..... Disabled
 Voice Device MAC Address
 ------------------------------
 0004.F24C.FD5D
```

The **show interface cos-queue** command displays priority modes for all queues. Strict queues are processed before Weighted queues.

```
show interface cos-queue

 Global Configuration
 Interface Shaping Rate..................... 0 kbps
 WRED Decay Exponent........................ 9

 Queue Id    Min. Bandwidth     Scheduler Type    Queue Management Type
 ----------  ---------------    ---------------   --------------------
 0           0                  Weighted          Tail Drop
 1           0                  Weighted          Tail Drop
 2           0                  Weighted          Tail Drop
 3           0                  Weighted          Tail Drop
 4           0                  Weighted          Tail Drop
 5           0                  Strict            Tail Drop
 6           0                  Weighted          Tail Drop
```

The **show classofservice dot1p-mapping** displays the Traffic Class (queue) to which each User Priority (CoS marking) is assigned.

```
 show classofservice dot1p-mapping

 User Priority   Traffic Class
  -------------  -------------
        0            1
        1            0
        2            0
        3            1
        4            2
        5            2
        6            3
        7            3
```

The **`show classofservice ip-dscp-mapping`** displays the Traffic Class (queue) to which each DSCP marking is assigned.

Note: In order to condense this output, several lines have been removed.

```
show classofservice ip-dscp-mapping

    IP DSCP        Traffic Class
-------------     -------------
  0(be/cs0)          1
  1                  1
  2                  1
  3                  1
  4                  1
  5                  1
  6                  1
  7                  1
  8(cs1)             0
  9                  0
  10(af11)           0

   ...               ...

  46(ef)             5
  47                 2
  48(cs6)            3
  49                 3
  50                 3
  5                  3
  52                 3
  53                 3
  54                 3
  55                 3
  56(cs7)            3
  57                 3
  58                 3
  59                 3
  60                 3
  61                 3
  62                 3
  63                 3
```

D.2 W-Series Controller Show Commands

The following show commands are useful in determining how the traffic is being processed within the controller.

The **`show datapath session`** command inspects sessions for high priority classification. There should be a "H" flag present for all voice sessions

```
(W7010_NSE) #show datapath session


Datapath Session Table Entries
------------------------------

Flags: F - fast age, S - src NAT, N - dest NAT
       D - deny, R - redirect, Y - no syn
       H - high prio, P - set prio, T - set ToS
       C - client, M - mirror, V - VOIP
       Q - Real-Time Quality analysis
       I - Deep inspect, U - Locally destined
       E - Media Deep Inspect, G - media signal
       A - Application Firewall Inspect


Source IP       Destination IP  Prot SPort DPort Cntr  Prio ToS Age Destination TAge Packets    Bytes      Flags
--------------- --------------- ---- ----- ----- ----- ---- --- --- ----------- ---- ---------  --------- --------
-------
192.168.1.206   192.168.1.50    6    1024  2000  0/0   6    24  0   tunnel 9    3f   40         3240       CI
74:26:AC:62:F5:07               2000               0/0   0    0   1   tunnel 9    10   0          0          F
74:26:AC:62:D9:71               2000               0/0   0    0   1   tunnel 9    10   0          0          F
192.168.3.52    192.168.3.3     47   0     0       0/0   0    40  0   pc1         e7   2201       535524     FC
192.168.1.206   192.168.1.200   17   22097 28257   0/0   0    46  1   sysmsg 107  35   3          300        FRHV
192.168.3.3     192.168.3.52    47   0     0       0/0   5    4   0   pc1         e7   2203       538720     F
192.168.1.200   192.168.1.206   17   28256 22096   0/0   6    46  0   vlan 54     35   987        197400     FHTCV
192.168.1.50    192.168.1.206   6    2000  1024    0/0   6    24  0   tunnel 9    3f   41         4512       I
192.168.1.200   192.168.1.50    6    1024  2000    0/0   6    24  0   tunnel 9    3f   56         5008       CI
F8:B1:56:29:FC:E8               8809               0/0   0    0   0   pc1         1    0          0          F


192.168.1.50    192.168.1.200   6    2000  1024    0/0   6    24  0   tunnel 9    41   63         6812       I
F8:B1:56:29:FC:E8               4242               0/0   0    0   0   pc1         116  0          0          F
192.168.3.3     192.168.3.52    17   8494  8211    0/0   0    0   0   pc1         2    1          195        FI
192.168.1.206   192.168.1.200   17   22096 28256   0/0   6    46  0   vlan 54     37   1085       217000     FHTV
F8:B1:56:29:FC:C8               8809               0/0   0    0   1   pc1         e    0          0          F
192.168.3.52    192.168.3.3     17   8211  8419    0/0   0    0   0   pc1         2    0          0          FYCI
192.168.1.200   192.168.1.206   17   28257 22097   0/0   0    46  0   sysmsg 107  37   5          500        FRHCV
```

The **`show ap debug client-stats <client-mac> | include WMM`** command verifies traffic is being queued into the correct WMM classification.

```
(W7010_NSE) #show ap debug  client-stats 74:26:ac:62:f5:07 | include WMM
Tx WMM [BE]                      654311424
Tx WMM [VI]                      83886080
Tx WMM [VO]                      589168640
Rx WMM [BE]                      1814233088
```

Note: At the time of publication, a known cosmetic issue with the show command incorrectly shows the classification of all RX traffic as Best Effort [BE]. This issue has been corrected in version 6.4.3.x, an Early Deployment release at the time of publication. Users can verify that the session is being classified as High Priority by using the "show datapath session" command on current GA releases.

E 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

Dell 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 website at http://www.dell.com.