Reliable Skype for Business Voice with Dell Networking Switches and Wireless

Dell Network Solutions Engineering
February 2016

A Dell EMC Deployment and Configuration Guide

Revisions

Date	Description	Authors
February 2016	Initial release	DNSE: CK

Table of contents

1 Introduction

The numbers are staggering: According to Business Insider, over 100 million people use Microsoft Lync (now Skype for Business) to communicate and collaborate at work. The same article indicates that enterprises either already use Lync for voice calls or are planning on adding that feature soon.

The verdict is in. Organizations have acknowledged that in order to stay competitive they must use Skype for Business or similar platforms. A Dell-sponsored study in 2014 of 200 Lync users indicated that the top two reasons organizations deployed Lync were improvement of internal communication/collaboration and reduction of costs. Businesses have also leveraged Skype to stay in touch with customers and improve customer support.

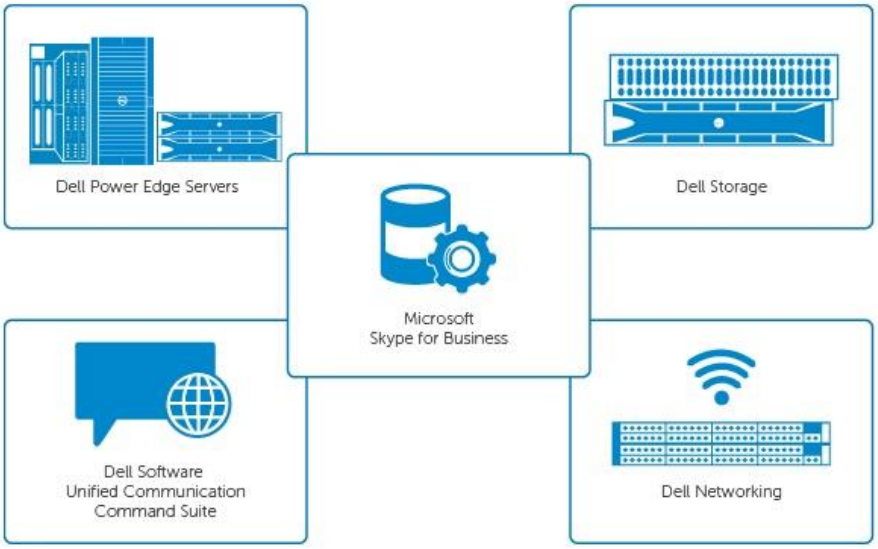

Figure 1 Dell EMC solutions to enhance Microsoft Skype for Business

Dell EMC is a leading Microsoft partner across the globe and provides many products and services that enhance the value of Skype for Business. Our cost-effective solutions address both business and technology needs, enabling organizations to upgrade or replace their current voice and/or video platforms. Our solutions work with Skype for Business to combine email, voicemail, telephony, audio conferencing and video conferencing over an IP network. This makes all five tools accessible over a single unified interface and can result in a dramatic boost to workforce efficiency. At the same time, IT professionals must keep in mind that moving to Skype for Business can be complex and require a well thought-out and balanced approach.

This deployment guide provides a broad example and serves as a high-level guide for customers deploying the voice component of Skype for Business. Since quality of service (QoS) is a key requirement of any voice deployment, this deployment guide provides specific examples of QoS configurations.

To enable reliable enterprise voice traffic delivery for the vast majority of deployments, having a well-planned strategy and configuring your network with robust QoS is crucial. This document applies to any Skype for Business deployment regardless of network topology or client. The examples and information on QoS provide a foundation to enable any administrator to deploy high-quality voice networks.

2 QoS in deployments of Skype for Business

QoS protocols provide reliable voice calls in the presence of data traffic on a network. Dell Networking switches and wireless 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.

Networked devices use QoS to influence traffic delivery. QoS can reduce latency and/or ensure the allocation of sufficient bandwidth for a particular traffic type. Reduced latency and jitter is critical in delay-sensitive applications such as Skype for Business. Several QoS mechanisms, including classification, marking, policing, shaping, mapping and queuing accomplish these results.

2.1 Campus switches

Classification identifies the type of traffic passing through an interface. Access Control Lists (ACLs) can perform classification enabling network routers to mark the traffic, which allows network devices farther upstream to perform QoS actions on the traffic without reclassification. Policing and shaping mechanisms control the bandwidth used for a particular traffic type. Each interface includes a transmit buffer divided into several queues configured with scheduling policies that determine the order of frame transmission onto the network.

2.1.1 Differentiated Services Code Point (DSCP)

DSCP (also known as DiffServ) is an OSI reference model layer 3—the network layer—marking mechanism that uses a 6-bit value found in the IP header. Administrators can configure Dell Networking N-Series switches to trust the DSCP marking of incoming packets and apply a scheduling policy for this traffic.

2.1.2 Queue scheduler types

Dell Networking N-Series switches support two queue scheduler types:

- Strict priority schedulers
- Weighted schedulers

Strict priority scheduler

This queue scheduler type services these queues before weighted queues. It sends data from the highest numbered strict queue, then the next highest strict queue, and so on, until it services all strict queues. A queue with strict priority can starve other queues in the same port-pipe.

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 help determine the total number of bytes, not packets, transmitted. These queues comprise the transmit buffers of each interface.

Table 1 shows an example of the following calculations:

1. Add 1 to each Queue ID value to find the weights of the queues.
2. Add together the weight values of the queues.
3. Divide the weight of each queue by the total weight to find the bandwidth percentage for that queue.

Table 1 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.

2.2 Data center switches

Data center switches also use classification to identify the type of traffic passing through an interface. Access Control Lists (ACLs) perform classification by enabling network routers to mark the traffic. This allows network devices farther upstream to perform QoS actions on the traffic without re-classification. Policing and shaping mechanisms control the bandwidth used for a particular traffic type. Each interface includes a transmit buffer divided into several queues configured with scheduling policies that determine the order of frame transmission onto the network.

2.2.1 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 S-Series switches can be configured to trust the DSCP marking of incoming packets and apply a scheduling policy for this traffic.

2.2.2 Queue scheduler types

The Dell Networking S-Series switches support two queue scheduler types:

- Strict priority scheduler
- Weighted scheduler

Strict Priority Scheduler

This queue scheduler type services these queues before weighted queues. It sends data from the highest numbered strict queue, then the next highest strict queue, and so on, until it services all strict queues. A queue with strict priority can starve other queues in the same port-pipe.

Weighted scheduler

This queue scheduler type selects packets for transmission based on weights assigned to each queue. Table 2 shows the default weight for each queue. The table shows the equivalent percentage. Calculate the percentage by dividing the weight by the sum of all queue weights. Weights calculated in this way show the total number of bytes, not packets, transmitted. These queues comprise the transmit buffers of each interface.

Note: In Dell Networking OS, we support eight data queues in S4048, S6000, Z9500; and four data queues in S3048, S4810, S4820T, and S5000.

Table 2 Default bandwidth weights

S4048, S6000 and Z9500 switches			S3048, S4820T and S5000 switches		
Queue	Weight	Bandwidth	Queue	Weight	Bandwidth
0	1	6.67% (1/15)	0	1	1% (1/100)
1	2	13.33% (2/15)	1	2	2% (2/100)
2	4	26.67% (4/15)	2	3	3% (3/100)
3	8	53.33% (8/15)	3	4	4% (4/100)
			4	5	5% (5/100)
			5	10	10% (10/100)
			6	25	25% (25/100)
			7	50	50% (50/100)

2.3 WLAN 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, the Access Point (AP) coordinates and controls transmissions. WMM shortens the time between packet transmissions for traffic marked with a higher priority. While QoS on a wired medium focuses on bandwidth and the amount of traffic in queues, WMM mainly focuses on access to the wireless medium.

Priority and DSCP values map directly to WMM classifications. Wireless LAN controllers have a default DSCP mapping scheme used to mark traffic for routing out to the greater wired infrastructure. Table 3 shows the default DSCP to WMM mapping for Dell Networking W-series WLAN controllers.

Table 3 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 wireless LAN controllers provide a configuration option to use custom mappings to change the default behavior, which is detailed in Section 3.3. If using DSCP values and mapping them to traffic queues on the wired network, use the same DSCP values in both wireless and wired networks for convenience. This document uses the DSCP value of 46 for voice on the wired network. Therefore, wireless requires a custom mapping.

3 Skype for Business Voice - wired and wireless example

3.1 Network topology

Figure 2 shows the network topology used during the validation of the configurations.

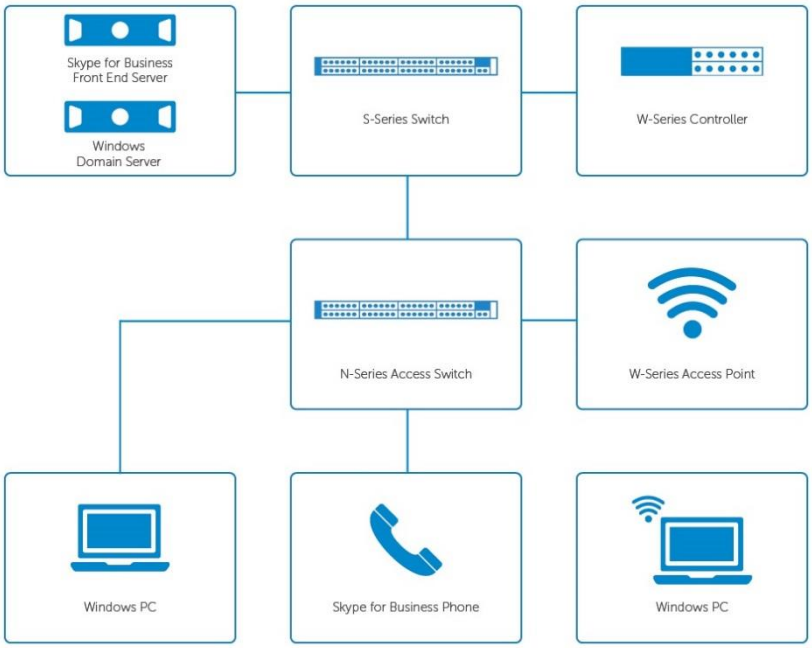

Figure 2 Wired and Wireless VoIP example topology

The topology above shows a campus network with a distribution switch, access switch and WLAN controller. A single S-series switch comprises the distribution layer in this example. The N-Series access switch and wireless LAN controllers connect to the distribution layer, while the APs, wired clients and wired phones connect to the access switch.

The Skype for Business deployment used in this example is an on-premise, Standard Edition, single front-end server installation. This deployment guide focuses on the QoS configuration of the networking components specifically for the voice component of Skype for Business.

3.2 Wired voice configuration

3.2.1 Dell Networking N-series campus switch configuration

The default setting of N-Series switches is to trust the dot1p markings of incoming traffic. Therefore, the first step in configuring N-Series switches in DSCP deployments is to configure the switch to trust the DSCP markings of your endpoints. The global command **`classofservice trust ip-dscp`** accomplishes this.

Note: Administrators can only configure interfaces to trust one marking type (DSCP or dot1p) at a time.

Note: This example assumes all clients are trusted, and DSCP markings are being applied using Group Policy. See section 3.4.2 for more information on setting up clients.

The **`show classofservice ip-dscp-mapping`** command shows the currently configured DSCP-to-Traffic Class (queue) mappings. A DSCP marking of 46 maps into queue 2 by default. This example uses queue 5, so the administrator needs to change the default behavior to map the DSCP value to queue 5. The command **`classofservice ip-dscp-mapping 46 5`** accomplishes this.

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

Note: The configuration commands used in this section can be entered in global or interface configuration mode. These examples configure the commands in global configuration mode so that they are effective for all interfaces on the switch.

Enter the commands shown in Table 4 on all of the N-Series switches.

Table 4 N-series switch commands

N-Series Switches	Description of commands

`configure`
 	
`classofservice trust ip-dscp`
 	
`classofservice ip-dscp-mapping 46 5`
 	
`cos-queue strict 5`
 	
`exit`
	
	← Trust incoming DSCP markings
	← Map DSCP marking 46 to queue 5
	← Set queue 5 to strict priority scheduling

The DSCP voice value commonly defaults to 46 for most VoIP systems. This example uses 46 as the Skype for Business voice value, but administrators can use a value that satisfies their own network policy. The

mapping of DSCP 46 to cos-queue 5 is also flexible. Dell N-Series switches have a total of 7 queues numbered 0 thru 6. Network control traffic commonly receives the highest queue, therefore the first available queue for voice traffic is usually queue 5. Network administrators should evaluate all traffic on their networks and assign the appropriate DSCP and queue priority to each traffic type. This example places Skype for Business voice as the highest priority for user traffic.

3.2.2 Dell Networking data center switch configuration

The QoS features and settings for Dell Networking data center switches use a policy-based methodology for configuration. This methodology defines policies then applies them to the desired interface.

The **`show qos policy-map detail [interface]`** command shows the currently configured policy mappings on the identified interface number. The detail also lists whether the interface trusts previously configured DSCP markings.

The methodology for identifying voice traffic marked as DSCP 46 and applying it to a specific queue is as follows:

1. Create a class-map to match traffic containing a value of DSCP 46.
2. Create a policy-map to assign the above class to queue 2.
   Set the policy to trust all DSCP markings.
3. Set a strict priority to queue 2
4. Apply the policy to the desired interface

By setting queue 2 to strict, this egress queue transmits its traffic before processing any packets in the weighted queues. Configurations including multiple strict queues send traffic in the highest numbered strict queue first, then the next highest numbered queue, and so on. The default scheduler type for all queues is weighted.

Note: This example assumes all clients are trusted and applies DSCP markings using Group Policy. Further, the example expects all traffic with DSCP value of 46 to be voice on the network. See section 3.4.2 for more information on setting up clients.

Table 5 Data center switch commands

Data Center Switches	Description of commands
configure class-map match-any voice match ip dscp 46 policy-map-input skype_voice trust diffserv service-queue 2 class-map voice strict-priority unicast 2 interface TenGigabitEthernet 0/13 portmode hybrid switchport service-policy input skype_voice no shutdown exit	 *← Matches all traffic with DSCP value of 46 to a class map* *← Trust incoming DSCP markings. Assigns all traffic in class "voice" to queue 2* *← Set queue 2 to strict priority scheduling* *← Example of an interface configuration. The policy "skype_voice" is applied to the interface ingress.*

Note: The interface configuration example above shows the application of a service policy to the input (ingress) of the interface. The output (egress) of any interface can also use the "policy map output" configuration.

3.3 Wireless voice configuration

3.3.1 Dell Networking W-series WLAN controller configuration

While Skype for Business is capable of voice, IM, file transfer, and video, the WLAN example in this document focuses on the voice component.

Note: Configuration of the basic WLAN network is out of scope for this document, which only describes the applicable QoS and key settings related to the example. For assistance on configuring a W-Series controller, see the User Guide located at http://dell.com/support.

This example begins with a fully functioning WLAN network. An administrator can add the features described below to any WLAN network, AP group, or Virtual AP profile.

Dell Networking W-Series has several features to assist in marking Skype for Business voice traffic. This document focuses on the heuristic-based Skype for Business traffic classification. This method allows for the classification of voice traffic at the controller if it has not been tagged by the client.

The following key features and settings must use heuristics-based classification and effectively enable QoS on the WLAN:

Enable WMM

To enable WMM, navigate to the desired SSID profile and click the advanced tab. Figure 3 and Figure 4 show a split view of the SSID profile and Advanced tab area where the WMM setting is located. Click the checkbox to enable WMM.

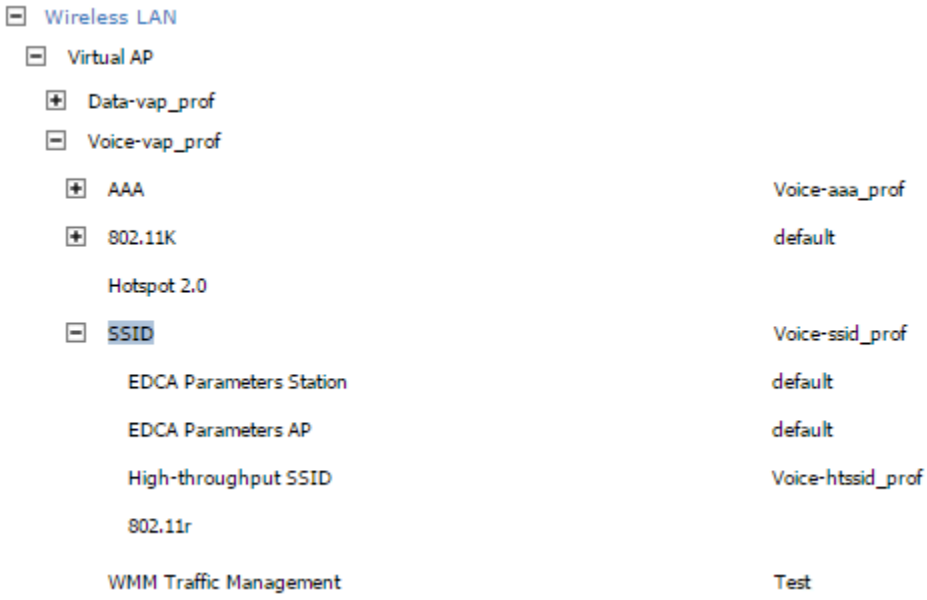

Figure 3 W-Series SSID profile, click **SSID**

Note: In this example the virtual AP profile is named "**voice-vap_prof**". This profile is for carrying both data and voice.

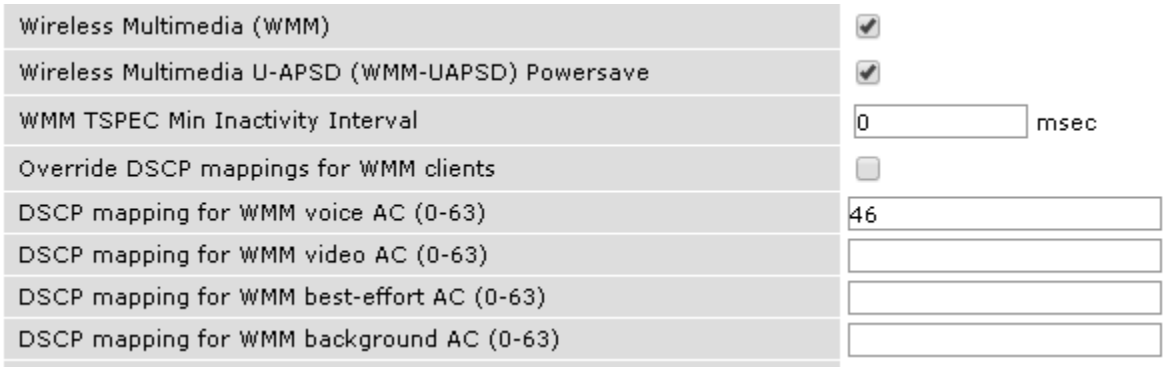

Figure 4 W-Series Advanced Tab, WMM settings

The custom mapping for DSCP values to WMM can bet set within the same location. In this example, the wired network and wired phones use DSCP of 46 for voice traffic. All traffic with a WMM value of 6 translates to a DSCP value of 46.

The WMM checkbox is the only setting that is required for enabling wireless QoS functionality. Any client associated with an SSID that has WMM enabled and can support WMM itself can have its traffic prioritized according to the four WMM classifications.

Fair access station shaping policy in the traffic management profile

Expand the QoS profile within the AP Group settings. Create a new 802.11a Traffic Management profile and change the Station Shaping Policy to **fair-access,** as shown in Figure 5. Create this profile for both bands if needed.

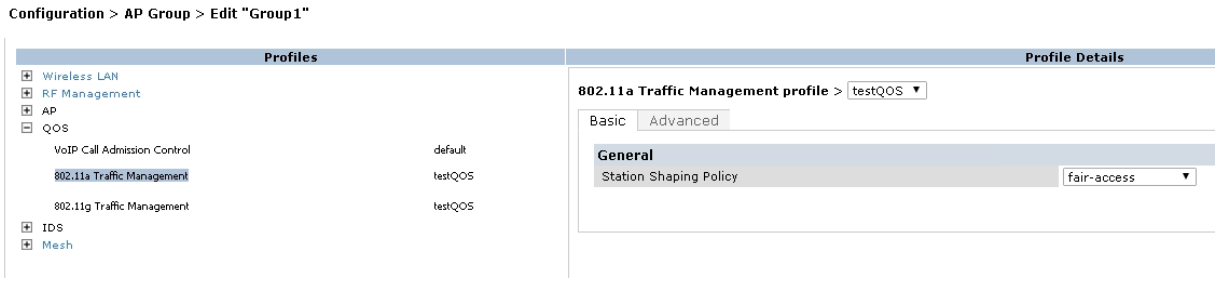

Figure 5 802.11a Traffic Management profile

Adaptive Radio Management Profile (ARM)

Expand the RF Management profile within the AP Group, as shown in Figure 6.

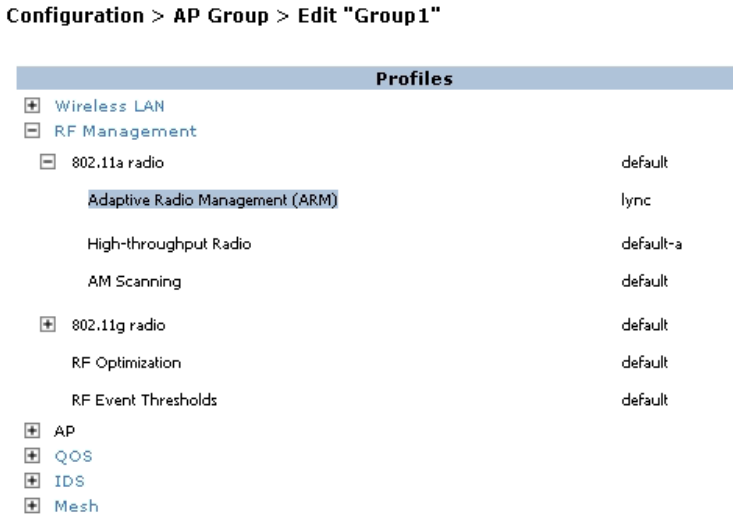

Figure 6 ARM profile

On the Basic tab, enable the VoIP Aware Scan, as shown in Figure 7.

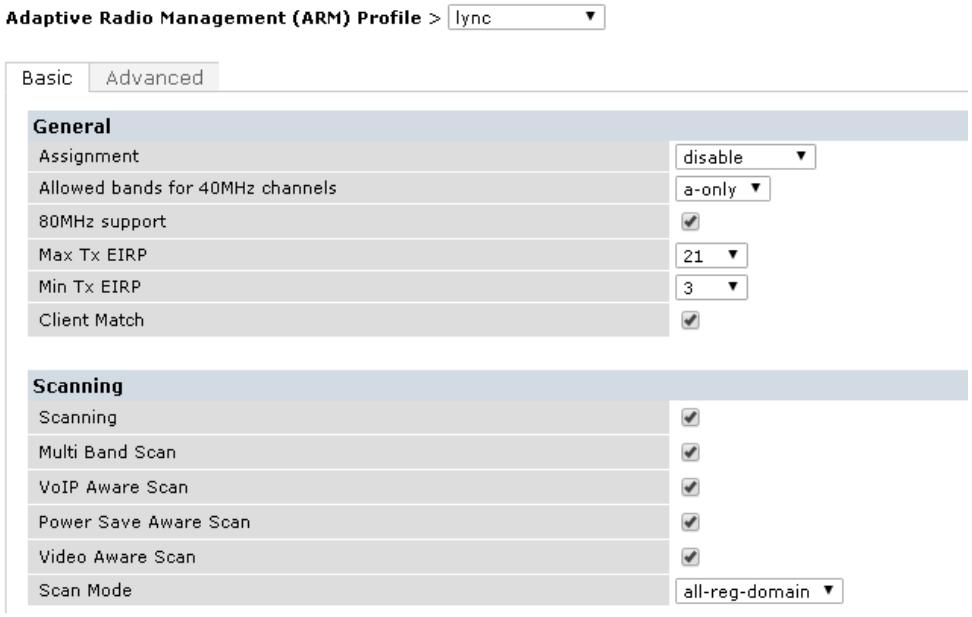

Figure 7 VoIP aware scan enabled

On the Advanced tab ensure Client Match is enabled, as shown in Figure 8.

Figure 8 Client Match enabled

Netdestination alias

Setup an alias for the Skype for Business Server to use in subsequent access lists. Navigate to the Stateful Firewall settings within Advanced Services. On the Destination tab, create an entry for all Skype for Business servers, as shown in Figure 9.

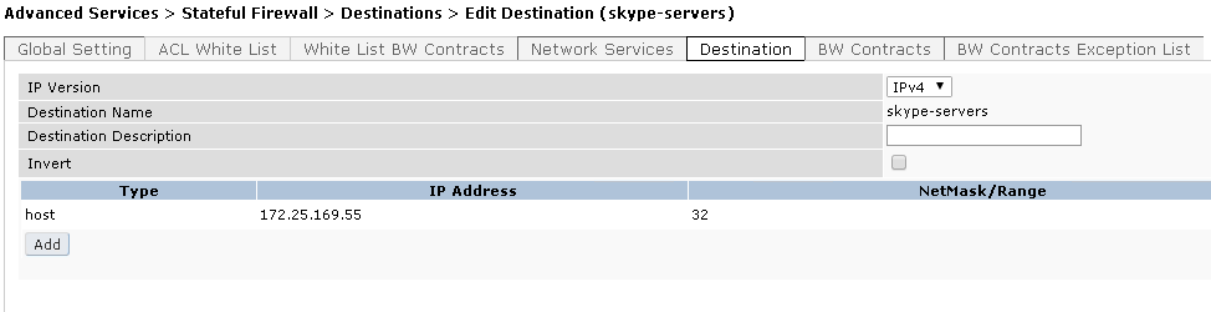

Figure 9 Netdestination alias

Stateful SIPS processing

Navigate to the Global Setting tab within the Stateful Firewall settings. Ensure that the Stateful SIPS Processing setting is enabled, as shown in Figure 10.

Figure 10 Stateful SIPS Processing

Access Lists to enable classification
To accomplish voice classification, identify the Skype for Business control traffic used to setup the calls. Skype for Business uses SIPS on port 5061 and HTTPS on port 443.

Navigate to the Access Control, and click the Policies tab. Click **Add** to create a new policy.

Enter an appropriate policy name, and add the following two rules to the policy, as shown in Figure 11:

Source: any
Destination: alias > skype-servers (from netdestination settings)
Service: SIPS
Action: permit
Queue: high
Classification: checked

Source: any
Destination: alias > skype-servers (from netdestination settings)
Service: https
Action: permit
Queue: high
Classification: checked

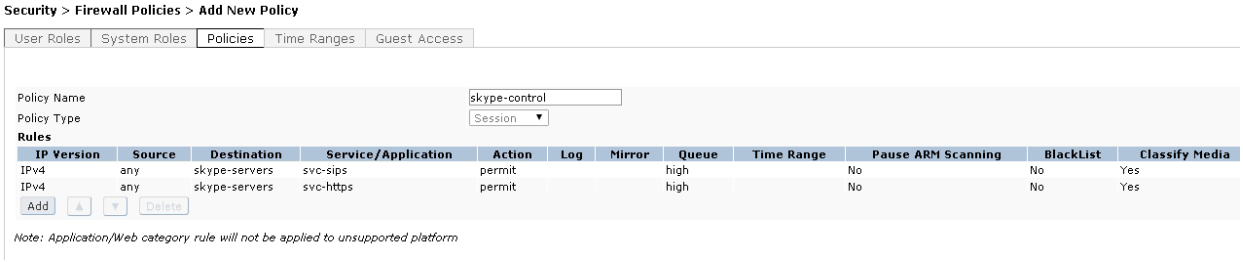

Figure 11 Skype control traffic policy with classification

To allow voice traffic, administrators must configure another access list. The Skype client application can use any port between 1024 and 65535. It may be beneficial to explicitly define the port ranges for voice, video and other Skype for Business features. Define these ranges within each of the Skype for Business front end servers. For more information on setting ranges see section 3.4.1. This example uses the full range.

STUN message requires an additional udp port 3478.

Navigate to the Access Control, and click the Policies tab. Click **Add** to create a new policy.

Enter an appropriate policy name, and add the following two rules to the policy:

Source: any
Destination: any
Service: udp, min port 1024, max port 65535
Action: permit
Queue: low
Classification: not checked

Source: any
Destination: any
Service: udp, min port 3478, max port 3478
Action: permit
Queue: low
Classification: not checked

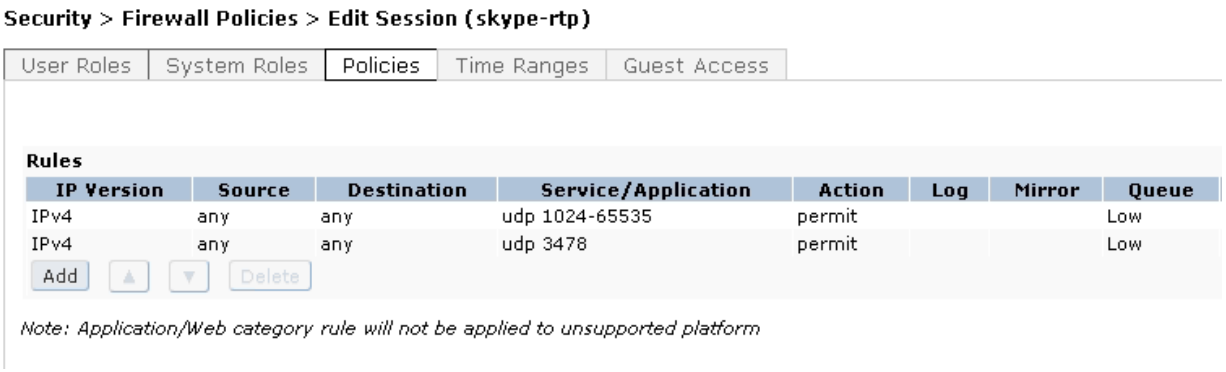

Figure 12 Skype for Business udp policy

Traffic Control Prioritization

Navigate to All Profiles within the Advanced Services section. Click **Traffic Control Prioritization** under the Other Profiles list. Add a new profile by entering an appropriate name into the field next to the Add button and click **Add**. Click on the name of the profile just created. Click the **Prioritize voice** check box, as shown in Figure 13. The next step uses this profile within the User Role.

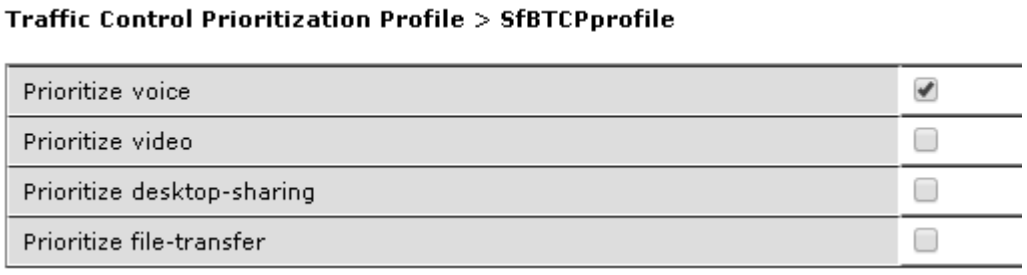

Figure 13 Traffic Control Prioritization profile

User Role for Skype for Business user

The preceding access lists must be applied to the User Role of anyone using Skype for Business. In this example, the User Role shown is simplistic, only incorporating rules associated with this document.

Navigate to the User Role tab within the Security > Access Control section. Edit an existing User Role or add a new one. Add the two policies created for skype control and udp traffic in the preceding steps, as shown in Figure 14:

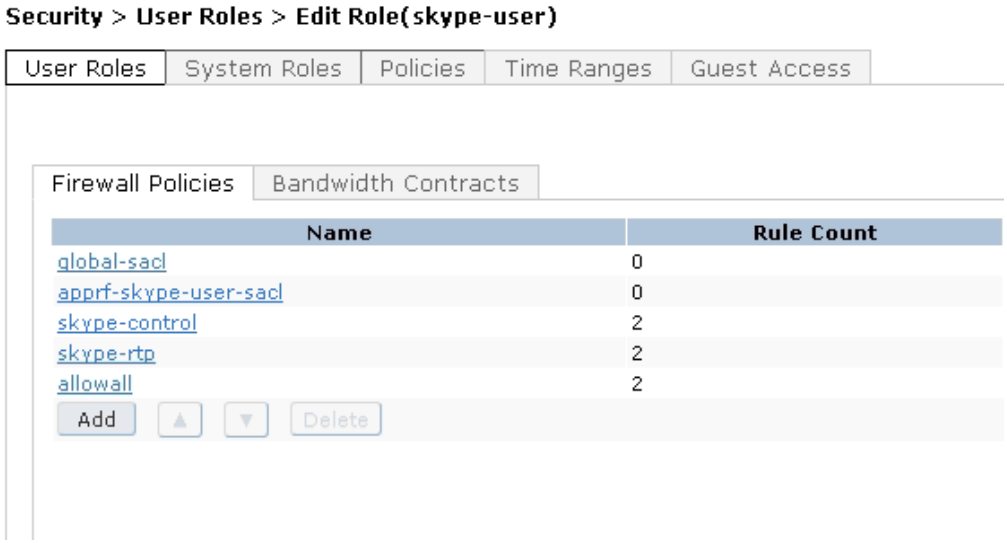

Figure 14 User Role – access lists

On the right-hand side of the User Role configuration find the Traffic Control Profile and select the profile created in the preceding step from the drop-down menu, as shown in Figure 15:

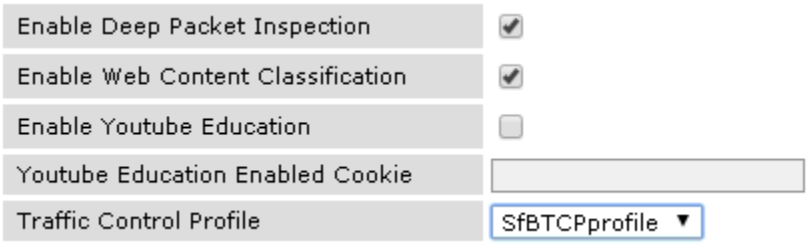

Figure 15 User Role – traffic control profile

This completes the minimum configuration steps to enable WMM and heuristic classification on the W-Series controllers.

3.4 Configuring Skype for Business front end server and Windows clients

3.4.1 Skype for Business front end server

The front end server controls the ports used by the clients during call setup. It also separates voice, video, file transfer, and application-sharing traffic into port ranges for classification. A network administrator can take these concepts and build QoS policies for video, file transfer, and application sharing.

To learn more about setting port ranges and QoS on the Skype for Business Server side, please go to the following online resource: https://technet.microsoft.com/en-us/library/jj204760(v=ocs.15).aspx

3.4.2 Windows clients

To take advantage of WMM capabilities from the client to the AP, Skype for Business traffic must be marked with the appropriate DCSP values at the client. Without the WMM values, the client does not get priority in the direction of the client to the access point.

Administrators can easily configure clients using a Group Policy Object (GPO) to add a QoS policy. It is out of the scope of this document to show how to deploy a GPO throughout an install-base of clients. Please go to the following online resource to learn how to configure a GPO:

https://technet.microsoft.com/EN-US/library/jj205371(v=ocs.15).aspx

3.5 Other considerations for WLAN to LAN

WLAN to LAN conversions are difficult to manage. As shown in Table 6, DSCP values translate to WMM values that may not line up with traditional LAN use cases. Default DSCP values for many VoIP systems are set at 46 (Hex value 46). However, a DSCP value of 46 translates to a WMM category of video.

Table 6 WMM to DSCP mapping

DSCP value	WMM Classification
0	Background
21	
22	Best Effort
31	
32	Video
47	
48	Voice
63	

This behavior causes issues if Group Policy marks the Skype for Business traffic at the client. The WLAN module translates the DSCP value of 46, set by Group Policy, to a WMM value of Video. To work around this, set the GPO to a value between 48 and 63, for example 56. However, if the user also connects via a wired LAN, then the higher DSCP 56 marking must be addressed on the wired network. One option is to add another class-map to match DSCP 56. Within the same policy-map, a second service queue could be used map to the new class-map. Strict-priority can still be used for each queue, assuming sufficiently balanced WLAN and LAN voice such that neither queue would starve the other.

Figure 16 and Figure 17 illustrate the behavior described above and its solution:

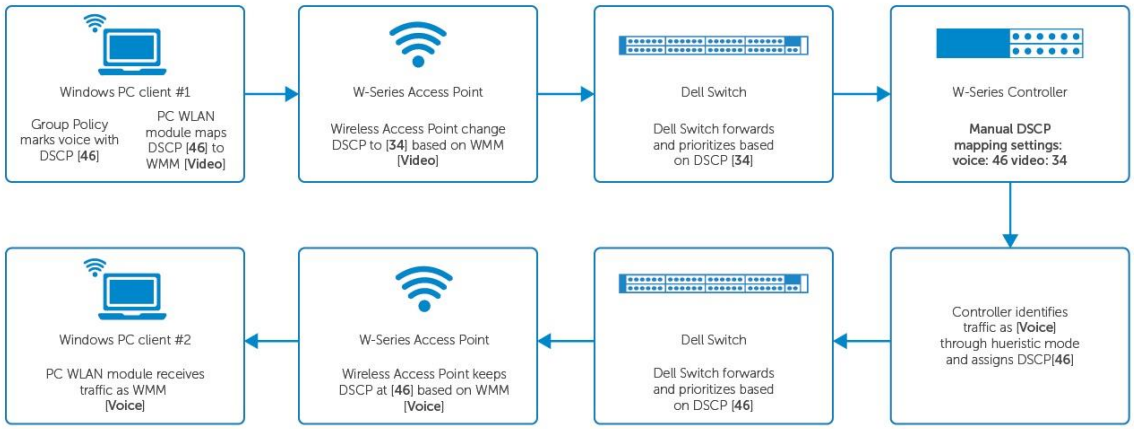

Figure 16 DSCP to WWM default mapping to video at client WLAN module

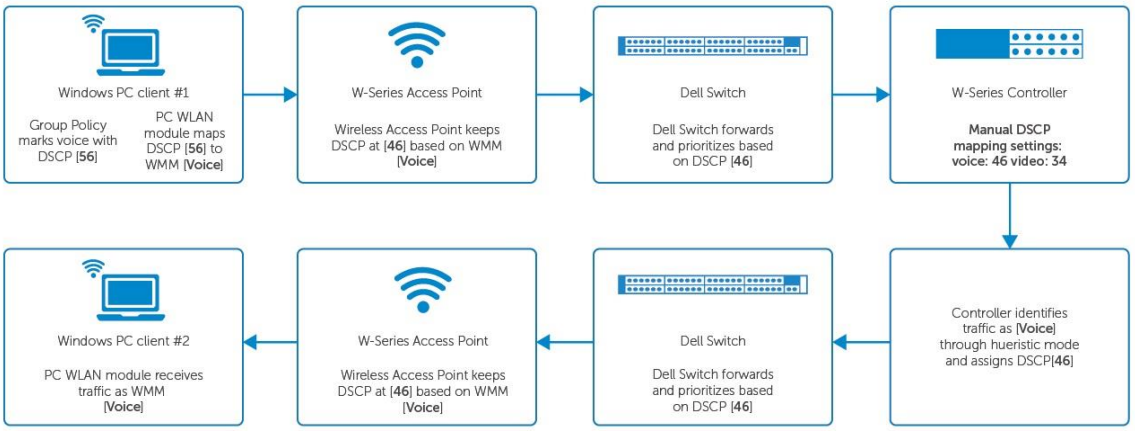

Figure 17 Increasing DSCP value at client to force desired DSCP to WMM mapping

If the traffic on your network is sufficiently complex and needs a wide variety of classifications and queues, the next step would be to plan out color marking and use Weighted Early Random Detect (WRED) and/or Explicit Congestion Notification (ECN). Administrators can investigate these options in the user guides for each switch model at http://dell.com/support.

A Additional resources

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

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

Referenced or recommended Dell EMC 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 and Firmware Downloads

http://www.dell.com/wireless

B Configuration details

This paper was compiled using the components and versions shown in Table 7.

Table 7 Components and versions

Component	Version
Dell Networking N3000	6.2.6.6 firmware
Dell Networking S4810	9.9(P1) firmware
Dell Networking W-Series	6.4.3.5 firmware
Skype for Business	Standard Edition 2015
Server Operating System	Microsoft Windows Server 2012 R2 Standard

C Supported models

The following Dell Networking switch models support the configuration examples included in this document:

Dell Networking campus switches

- N1524 / N1524P
- N1548 / N1548P
- N2024 / N2024P
- N3024 / N3024P / N3024F
- N3048 / N3048P
- N4032 / N4032F
- N4064 / N4064F

Dell Networking data center switches

- M I/O Aggregator
- MXL 10/40 GbE
- S4810
- S4810T
- S4820T
- S5000
- S6000
- Z9500
- Z9000
- S4048
- S3048
- C9010 & C1048P
- Z9100
- FN410S
- FN410T
- FN2210S

Dell Networking W-series WLAN controllers

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

D Support and feedback

Contacting technical support

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

Feedback for this document

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

About Dell EMC

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