ExtremeWireless WiNG

VOIP Recommendations

Published: December 2018

Extreme Networks, Inc.
Phone / +1 408.579.2800
Toll-free / +1 888.257.3000

www.extremenetworks.com

P/N XXXXX-XX

Table of Contents

Overview

Voice over Wireless LAN (VoWLAN) delivers the functionality of an enterprise telephone system in a wireless handset. The handset is a wireless client device, and it shares the wireless network with laptops and other hand-held devices. For enterprise use, the handset is functionally equivalent to a wired desk phone, giving end-users all the features they are used to in a wired office telephone. The benefits of VoWLAN can result in substantial cost savings, leveraging Wi-Fi infrastructure and eliminating recurring charges associated with the use of cell phones, while significantly improving employee mobility.

There are two types of mobility, being mobile and 100%-connected mobility. To help explain this, think of the marketing manager working on a presentation and saving it on a network share. He later wants to give that presentation in the boardroom. If he picks up his laptop, closes the lid, and walks to the boardroom, opens the laptop, connects to the wireless network, and gives his presentation - that is being mobile. His laptop may have disconnected from the wireless network in between his office and the boardroom, but he never noticed. The same manager starting a call on his VoWLAN handset while in his office, remaining on that call as he walked to the elevator, traveled up several floors, and then walked to the boardroom – that is true mobility. If his VoWLAN handset had disconnected during that call, he would have noticed.

True mobility and enterprise-grade VoWLAN requires wireless networks designed to provide the highest audio quality throughout the facility. VoWLAN handsets require continuous, reliable connections as a user moves throughout the coverage area. Voice applications have a low tolerance for network errors and delays, deteriorating with just a few hundred milliseconds of delay or 1% of packet loss.

Coverage

Most data communication protocols provide a mechanism for retransmission of lost or corrupted packets, thus delays caused by retransmissions are not discernable. The real-time nature of a telephone conversation requires that voice packets be received correctly within 100ms of transmission. Lost or corrupted packets are discarded after limited retries. In areas of inadequate wireless coverage, the audio quality of real-time voice will suffer.

Moving handsets make the determination to roam in less than half the overlapping coverage area from a neighboring access point. That Assessment Area must be large enough to allow the handset time to discover, associate with, and connect to the next access point before the signal on the currently connected access point becomes too weak. Understanding what impacts RF coverage, cell size, and overlap is essential to properly design and configure a wireless network for voice usage.

The usable cell size of an access point is dictated by the frequency, signal power level, minimum data rate, number of channels used, and objects that attenuate the signal. A properly designed wireless network positions access points with sufficient overlapping coverage to ensure there are no coverage gaps between them. 20% overlapping coverage between access points will result in seamless hand-offs and excellent voice quality at the average walking speed of 3 mph. If the speed of the moving user is greater (golf cart, fork lift or running/jogging), a larger overlap percentage may be necessary.

Dynamic Channel Assessment (DCA) is generally performed between the transmission of voice and control packets to learn about neighboring access points. It takes approximately 250 ms to process each channel in the channel list. To determine the size of access point Cell Overlap, determine the number of feet covered per second for the average walking speed of 3mph:

- 5,280 feet per mile * 3mph = 15,840 feet per hour
- 15,840 feet per hour / 60 = 264 feet per minute
- 264 feet per minute / 60 = 4.4 feet per second

Then apply that distance to the duration of the DCA Cycle for each band/channel configuration. The Assessment Area is approximately ¾ of the Coverage Overlap Area. Overlap Percentage is based on access points located 60 feet apart.

The following table shows the results of those calculations for various channel configurations:

Band	Number of Channels	Duration (ms)	DCA Cycle (seconds)	Assesment Area	Coverage Overlap	Overlap Percentage
2.4GHz	3	250	0.75	3.30	4.40	7%
5GHz	8	250	2.00	8.80	11.70	20%
5GHz	12	250	3.00	13.20	17.60	29%
5GHz	23	250	5.75	25.30	33.70	56%

Failure to complete the DCA cycle within the assessment area can lead to loss of connectivity, choppy audio, or a dropped call. Give careful consideration to the number of channels deployed in 5 GHz for a VoWLAN environment to avoid this.

There are unique requirements for the various types of WLAN implementations. A data-only implementation does not require significant cell overlap as 802.11 clients typically step down their rate to accommodate the transition to another access point. Typical thresholds for a data-only implementation are a Signal Strength of -82 dBm and a Signal-to-Noise Ratio (SNR) of 10 dB.

The voice-data implementation generally requires a Signal Strength of -65 dBm, a Signal-to-Noise Ratio (SNR) of 25 dB or better, and a Cell Overlap of 20%. The Cell Overlap ensures that a VoWLAN handset can detect and connect to alternative access points before it reaches its current cell boundary. The Signal Strength target of -65 dBm at the cell edge results in more access points running at lower power levels. A same channel separation of 19 dB is necessary to diminish co-channel interference. In a voice-data implementation, a low noise background is as important as high energy density. Transient conditions will make themselves more evident in a voice-data implementation. The actual target minimum Signal Strength depends on the 802.11 frequency band it is operating in, modulation used, data rates enabled on the access point, and data rate used by the handset at any particular time.

2.4GHz 802.11b (CCK)				
Rate (Mbps)	1	2	5.5	11
Minimum RSSI (dBm)	-75	-70	-68	-65

2.4GHz 802.11g (OFDM)								
Rate (Mbps)	6	9	12	18	24	36	48	54
Minimum RSSI (dBm)	-67	-66	-64	-62	-60	-56	-52	-47

5GHz 802.11a (OFDM)								
Rate (Mbps)	6	9	12	18	24	36	48	54
Minimum RSSI (dBm)	-67	-65	-63	-61	-58	-54	-52	-50

Dynamic Channel Assignment and Intelligent Transmit Power Control should be used in all VoWLAN deployments. Transmit Power Minimum and Maximum levels should be established based on the maximum transmit power of the client used. In the case of multiple clients, minimum and maximum levels should be set to accommodate the client with the weakest transmit power. It is essential to prevent the access point from transmitting at a higher power than the client.

QoS

WMM is based on IEEE 802.11e Enhanced Distributed Coordination Access (EDCA). The first component of WMM are the four Access Categories (derived from 802.1d).

WMM Access Category	Priority Level	802.1d Tags	Client wait time + random backoff window (slots)	SIP Traffic Type
Voice (AC_VO)	highest	7,6	2 + 0 to 3	Voice
Video (AC_VI)		5,4	2 + 0 to 7	Call Control
Best Effort		0,3	3 + 0 to 15	Other (PTT, OAI, RTLS)
Background (AC_BK)	lowest	2,1	7 + 0 to 15	Not used

WMM relies on the application to assign the appropriate access category for the traffic it generates. Once the application assigns each packet to an access category, packets are then added to one of four independent transmit queues in the access point and client. Once transmitted onto the wireless network applications compete for available bandwidth, resulting in packet collisions. When this happens the access category used will determine the retransmission timing. The higher the priority level, the lower the required wait time and random "back-off" window.

WMM Power Save is the second component of WMM. Based on the IEEE 802.11e Unscheduled Automatic Power Save Delivery (U-APSD) mechanism, it is an enhancement of the legacy 802.11 power save mechanism. The application-based approach used in WMM Power Save enables individual applications to decide how often the client needs to communicate with the access point and how long it can remain in a "restful" state. In addition, WMM Power Save increases transmission efficiency by transmitting the same amount of data in a shorter time using fewer frames. Power save behavior is negotiated during the association of a handset with an access point.

The third component of WMM, **WMM Admission Control**, allows the access point to manage its available "air time" based on traffic requirements submitted by associated clients. Requests are rejected if insufficient resources are available. Use of WMM Admission Control avoids over-subscribing the access point, preserving and protecting QoS for all associated devices.

Security

Authentication is the process that occurs after WLAN association, where the handset and authentication server verify each other's credentials then allow the handset access to the network. WPA2 has two different authentication modes, Personal and Enterprise. Personal mode uses a password-based authentication method called Pre-Shared Key (PSK). Personal mode is good for time-sensitive applications such as voice, because the key exchange sequence is limited and does not adversely affect roaming between access points. The PSK can be entered in hexadecimal or as an ASCII passphrase from the handset's administration menu or through configuration files.

WPA2 Enterprise security mode requires a WLAN device to mutually validate credentials through 802.1X with a RADIUS server on the network every time the device roams to a new access point. Authentication delays during roaming may cause dropped packets and result in longer delays and audio artifacts. The size of the credentials used and the location of the RADIUS authentication server can significantly affect the duration of that delay. Larger credentials are more secure, but they take more time to process.

Fast access point hand-off techniques allow for the part of the key derived from the authentication server to be cached in the wireless network, thereby shortening the time to renegotiate a secure hand-off. Client handsets generally offer two 802.1X authentication types (PEAPv0 with MSCHAPv2 or EAP-TLS), and two or three fast access point hand-off mechanisms (OKC & PMK Caching or 802.11r on newer handsets). The combination of the selected 802.1X authentication type and fast access point hand-off mechanisms results in faster roaming and fewer audio artifacts. Use of the fast access point hand-off methods does not eliminate situations where full 802.1X key exchanges must re-occur.

PEAP (Protected Extensible Authentication Protocol) was developed by Microsoft, Cisco and RSA Security for 802.1X authentication on WLANs. PEAPv0 with MSCHAPv2 is one of the most-commonly used PEAP

subtypes. PEAP makes use of a server-side public key certificate to authenticate the server and creates an encrypted tunnel to exchange information between the server and the client. Larger certificate key sizes provide stronger encryption, but are more computationally intensive and therefore take more time to process. The longer processing time can result in audio artifacts.

General Wireless Network Best Practices

In order for voice to operate efficiently in a wireless network, it is critical that it be separated from the data traffic by using 802.1q VLANs.

Most access points can be configured to allow or deny association of wireless clients based on their unique MAC address and is sometimes used as a method of securing the WLAN. This process is not recommended for a VoWLAN environment. MAC filtering is ineffective as a security method.

The traffic filtering capabilities of firewalls, Ethernet switches, and wireless controllers can also be used as an additional security layer when configured to allow only certain types of traffic to pass onto specific areas of the LAN. To properly provide access control, it is necessary to understand the type of IP traffic used. Following is a table of common port numbers:

Protocol	Type	Port
FTP	TCP	21
SSH	TCP	22
Telnet	TCP	23
DNS	UDP	53
DHCP	UDP	67
DHCP	UDP	68
TFTP	UDP	69
HTTP	TCP	80
NTP	UDP	123
LDAP	Both	389
HTTPS	TCP	443
Syslog	UDP	514
LDAP over TLS	Both	636
SIP	Both	5060
SIP over TLS	TCP	5061
RTP	UDP	16384-32767

While wireless handsets will generally work through a Firewall (if the appropriate ports are allowed) it is not recommended. Firewalls create jitter which can severely limit the successful and on-time delivery of audio packets.

General Recommendations for VOIP

Setting	Value	Notes
Latency	<100ms	end-to-end
Jitter	<30ms	
Packet Loss	<1%	
Cell Overlap	20%	30% in critical environments
Band	5GHz	2.4GHz will almost never be “clean” enough for stable VOIP
Channel Width	20MHz	
SSIDs per Access Point	<6	

Quality of Service

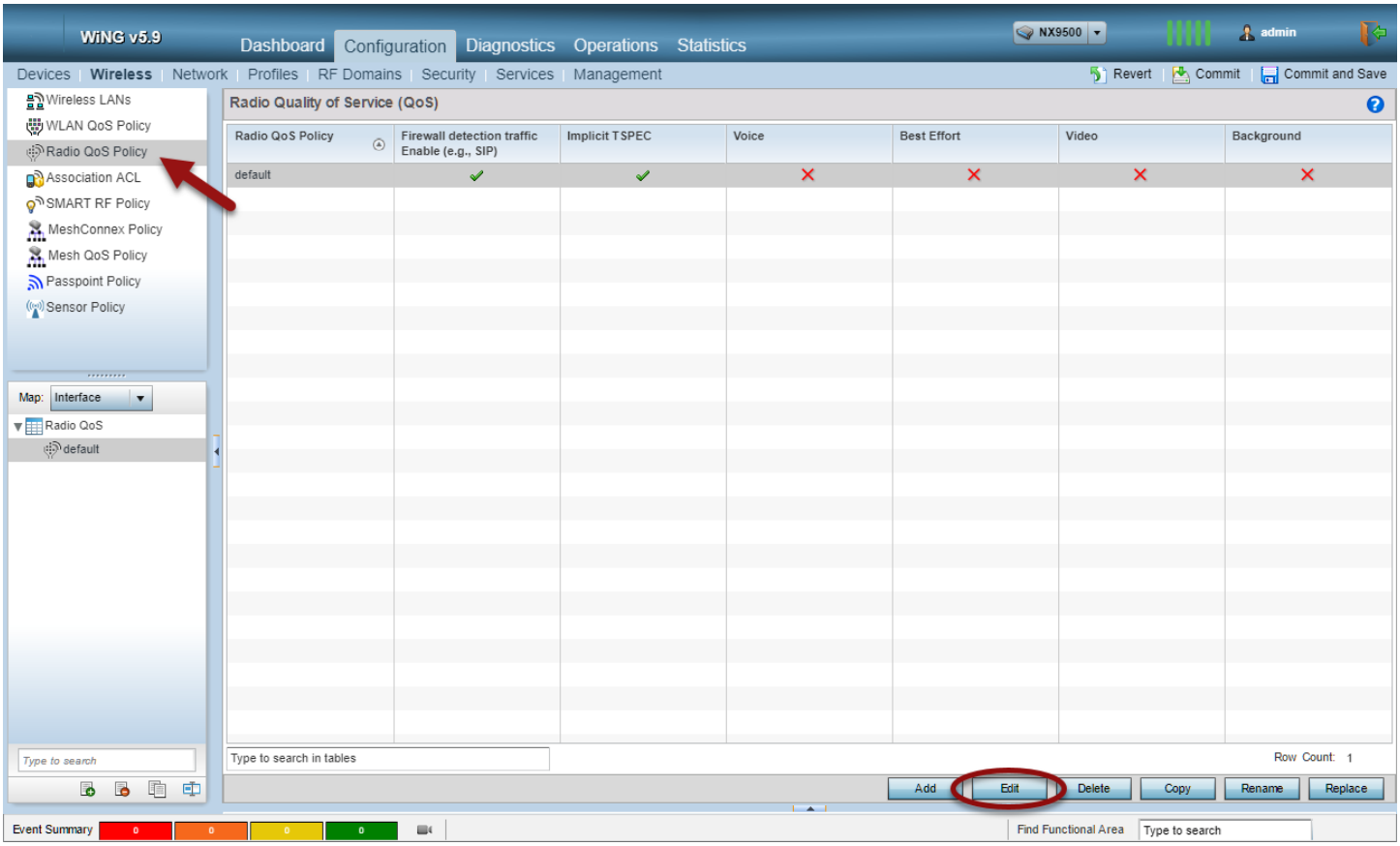
Wireless networks transport a multitude of applications and data, including delay-sensitive data such as real-time voice. Bandwidth-intensive applications stretch network capabilities and resources, but also add value, and enhance business processes. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required Quality of Service (QoS) by managing the delay, delay variation (jitter), bandwidth, and packet loss parameters on a network becomes the secret to a successful end-to-end business solution. Thus, QoS is the set of techniques to manage network resources. Verify or apply the following settings if the intent is to deliver VoIP over this wireless network.

Radio QoS Policy

Radio QoS Policies are applied to individual radios within an Access Point. They are applied through Group Device Profiles.

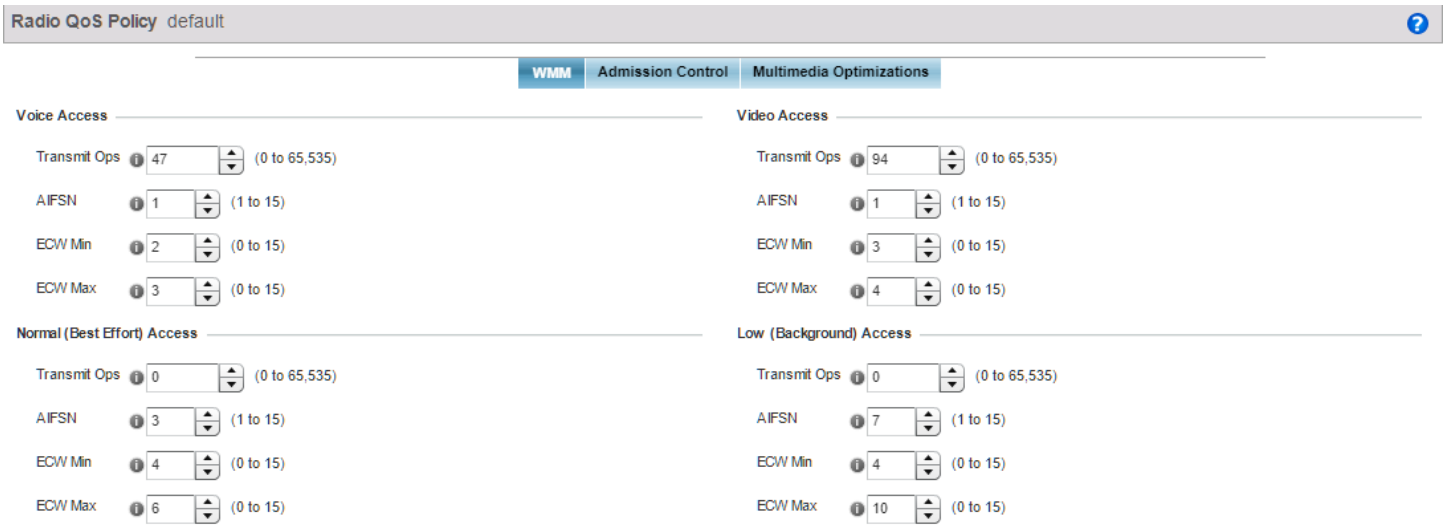
Radio QoS parameters enforce WMM and police the different traffic types at the radio level. The most important of these is Admission Control.

From the GUI, select **Configuration** > **Wireless** > **Radio QoS Policy** > **Edit "default"**.



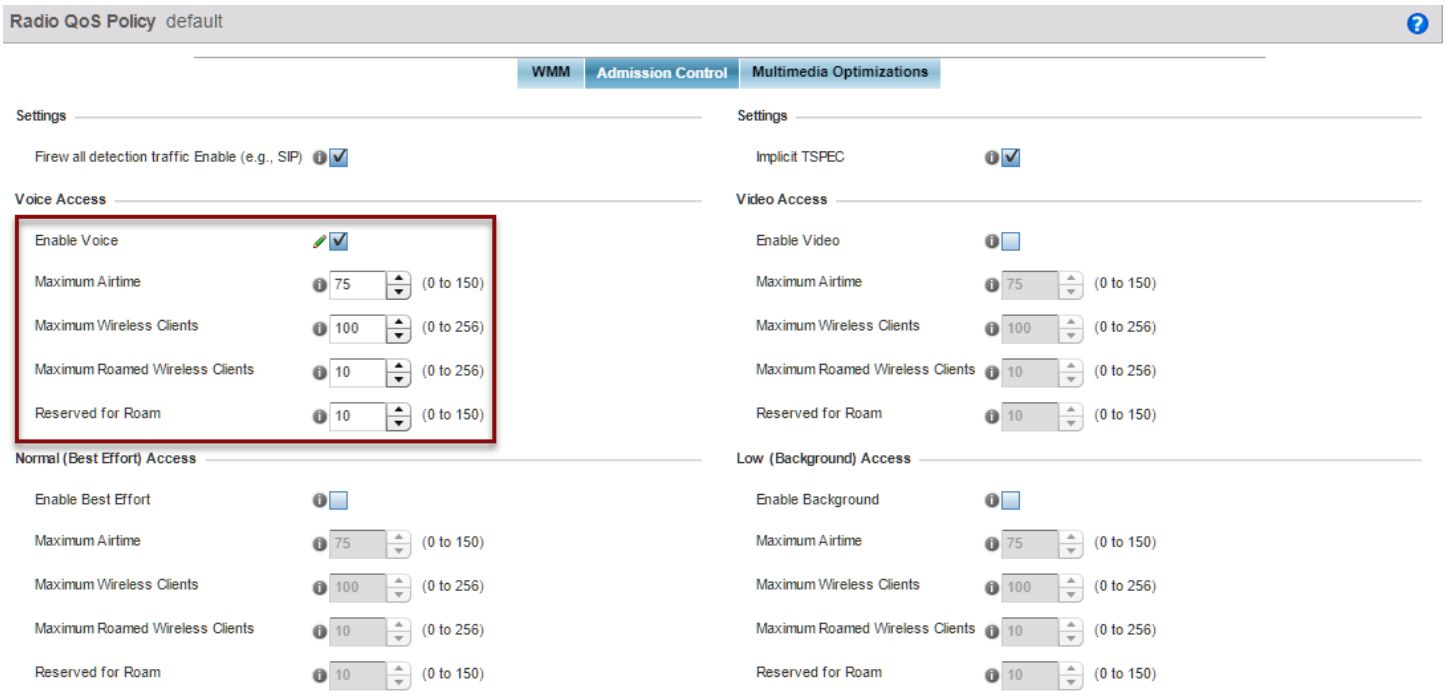
WMM Tab – Voice Access

Currently set to defaults, which should work well with typical Voice handsets and are the same as settings Wi-Fi Alliance tests against for WiFi Enterprise-Voice certification. Adjust as necessary.



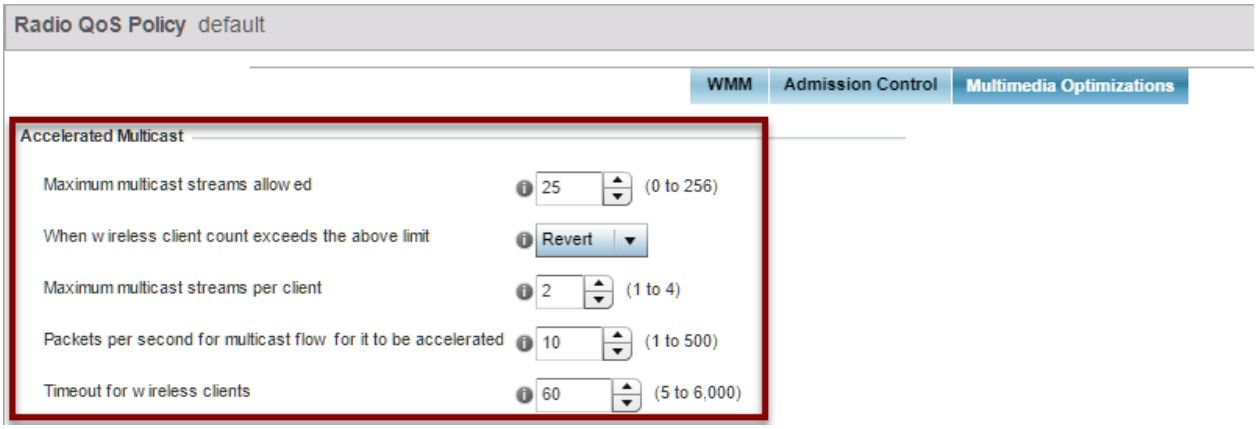
Admission Control Tab – Voice Access

Currently set to defaults, however for VOIP deployment, Admission Control for Voice traffic should be enabled leaving rest of the values as default.



Multimedia Optimizations Tab – Accelerated Multicast

Currently set to defaults, which should work well with majority of modern push-to-talk clients. Adjust as necessary.

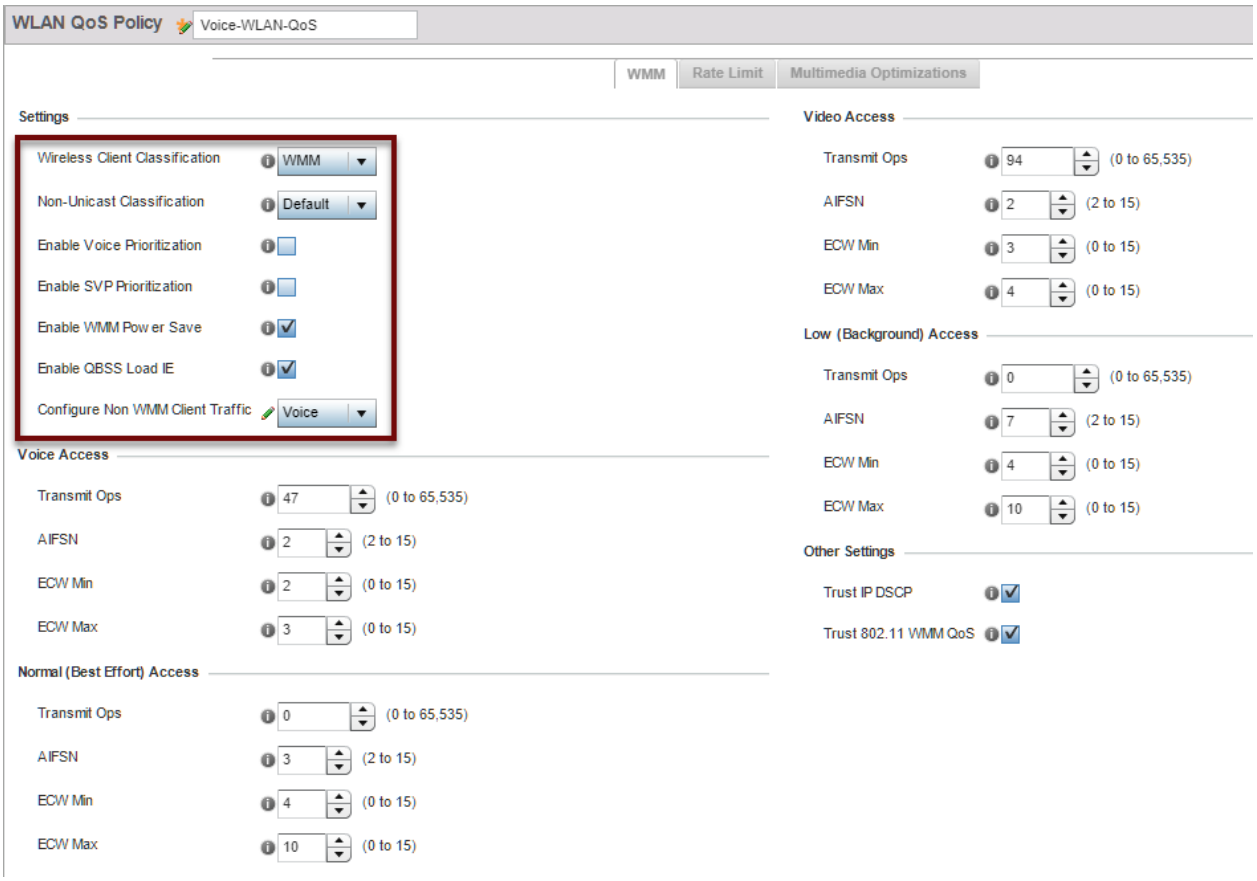


WLAN QoS Policy

WLAN QoS policy unlike the Radio QoS policy applies to a specific SSID that allows more granular control over WMM and legacy non-WMM QoS settings. By defining Guest, Normal and Voice policies and using them appropriately, Voice traffic can be prioritized.

An example of WLAN QoS policy for Voice is shown below. The default settings are optimal for majority of modern VOIP clients. As for the legacy non-WMM capable clients, the following parameters may be optionally enabled to support them (do NOT enable them unless there are clients that need them):

1) Non-WMM Client Traffic Classification – in case there are non-WMM VOIP handsets, you can optionally mark all traffic from non-WMM device into a specific category, such as Voice.
2) Voice-Prioritization – enables support for legacy Symbol VOIP phones (prioritizes traffic from these non-WMM handsets over other non-WMM clients).
3) SVP Prioritization – enables support for legacy SpectraLink and Polycom phones. Do not enable for other voice clients.



Smart RF

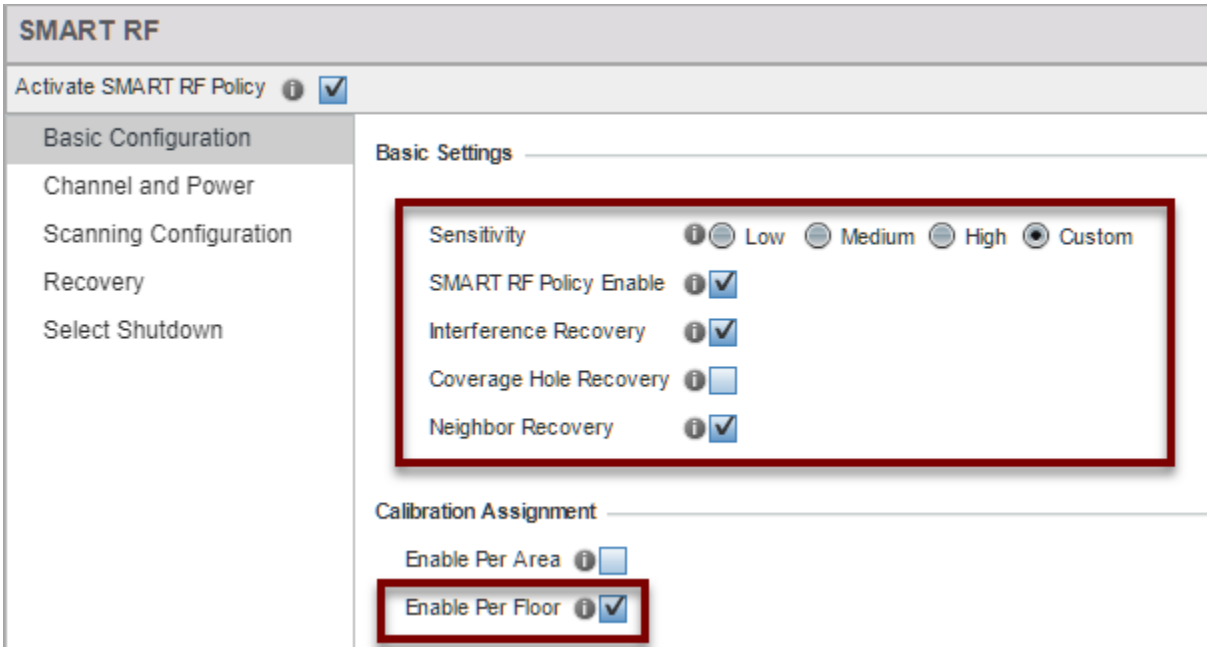
Self-Monitoring At Run Time RF Management is designed to simplify RF configuration and optimize radio performance in dynamic ever-changing environments.

Smart-RF:

- Centralizes the decision process and makes intelligent RF configuration decisions using data obtained from the RF environment.
- Intelligently applies various algorithms to arrive at the optimal channel and power selection for all access points in the network.
- Monitors the network for external WiFi interference, neighbor WiFi interference and non-WiFi interference and client connectivity SNR.
- Provides automatic mitigation from problematic events such as interference, noise, coverage holes and radio failures.
- Reacts to changes in the RF environment, self-healing if necessary.

Recommendations for Voice Deployment

Under basic settings of the SmartRF policy enable Neighbor Recovery (provides automatic cell size change by monitoring neighboring radios and provides self-healing mechanisms in case of radio failure) and Interference Recovery (provides dynamic channel changes in case of WiFi or nonWiFi interference events). Typically, in VOIP deployment it is not required to enable Coverage Hole Detection, as VOIP designs are usually done with higher AP density in mind. In multi-floor building it is important to enable SmartRF grouping by Floor, so it will make decisions based on the floor where AP is located (APs are assigned to floors using profiles or by simple drag&drop in the UI).

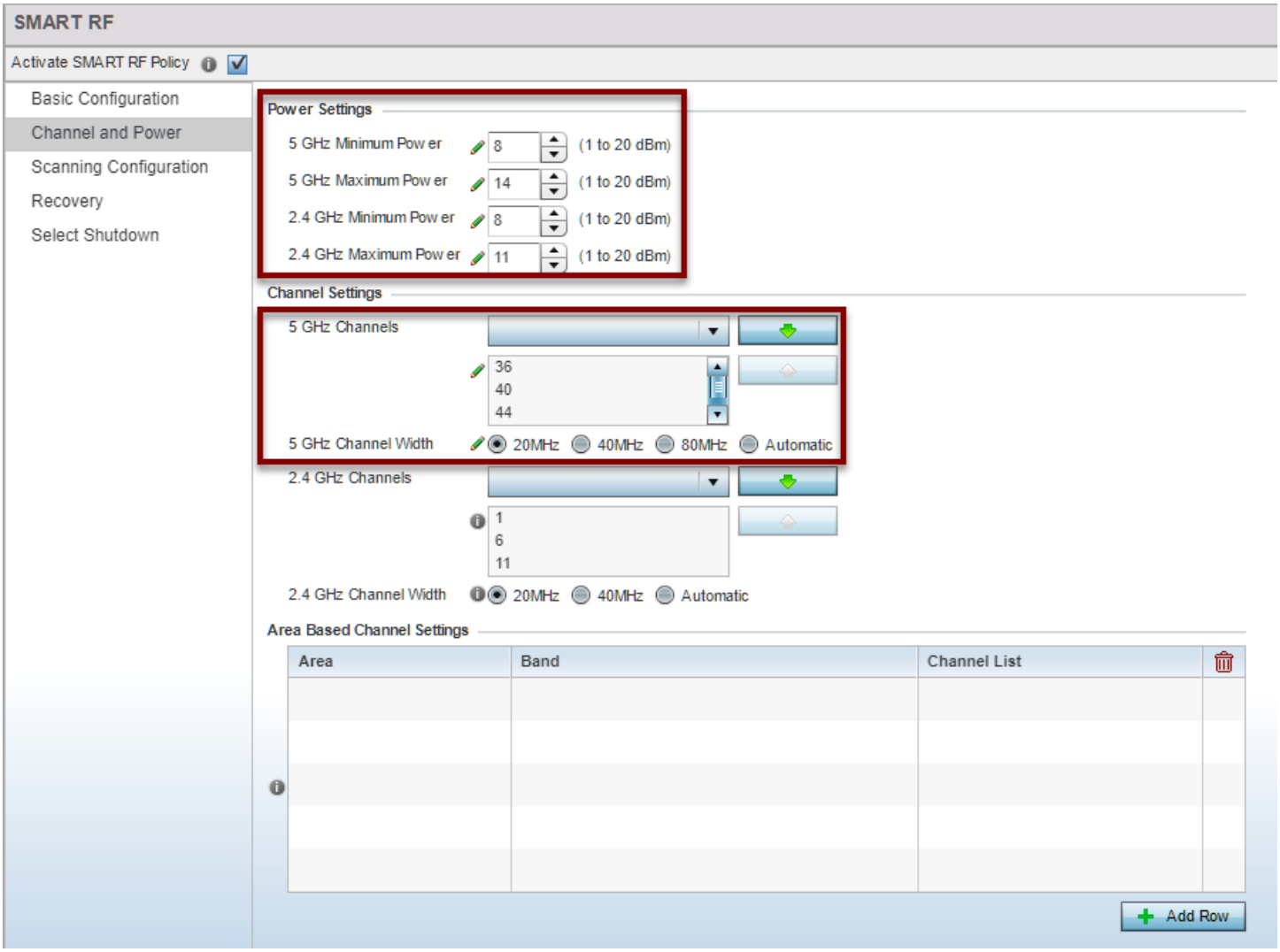


Under channel and power tab, the following recommendations apply for VOIP deployments:

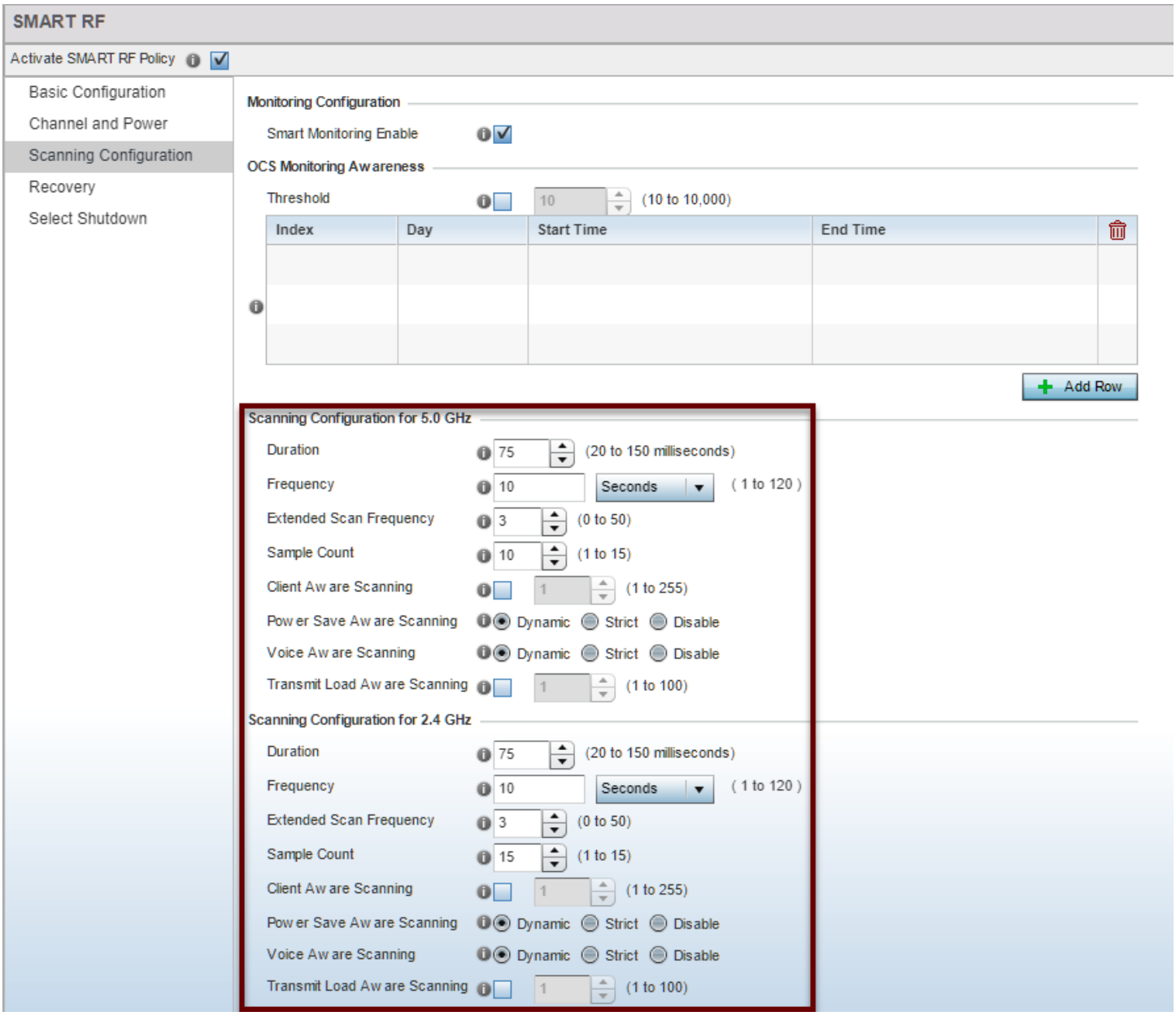
1. Do not exceed max power of 15dBm. Majority of VOIP clients are low-powered devices, hence to maintain symmetrical power between AP and the client, it is recommended not to transmit at very high power.
2. For dual-band deployments, set 5GHz max power about 3dB higher than 2.4GHz max power to naturally let the clients prefer cleaner 5GHz spectrum.
3. 5GHz channel list should include only non-DFS channels. In EU/ETSI regulatory domain those are UNII1 channels 36,40,44,48. In FCC regulatory domains they are 36,40,44,48,149,153,157,161. The reason behind this logic is simple – AP discovery on non-DFS channels for a client is much faster, as client is allowed to send probe requests, rely on 802.11k or listen for a beacon. On

DFS channels, clients are not allowed to transmit probe requests until they can hear a beacon. This may dramatically increase new AP discovery time and result in poor roaming performance.

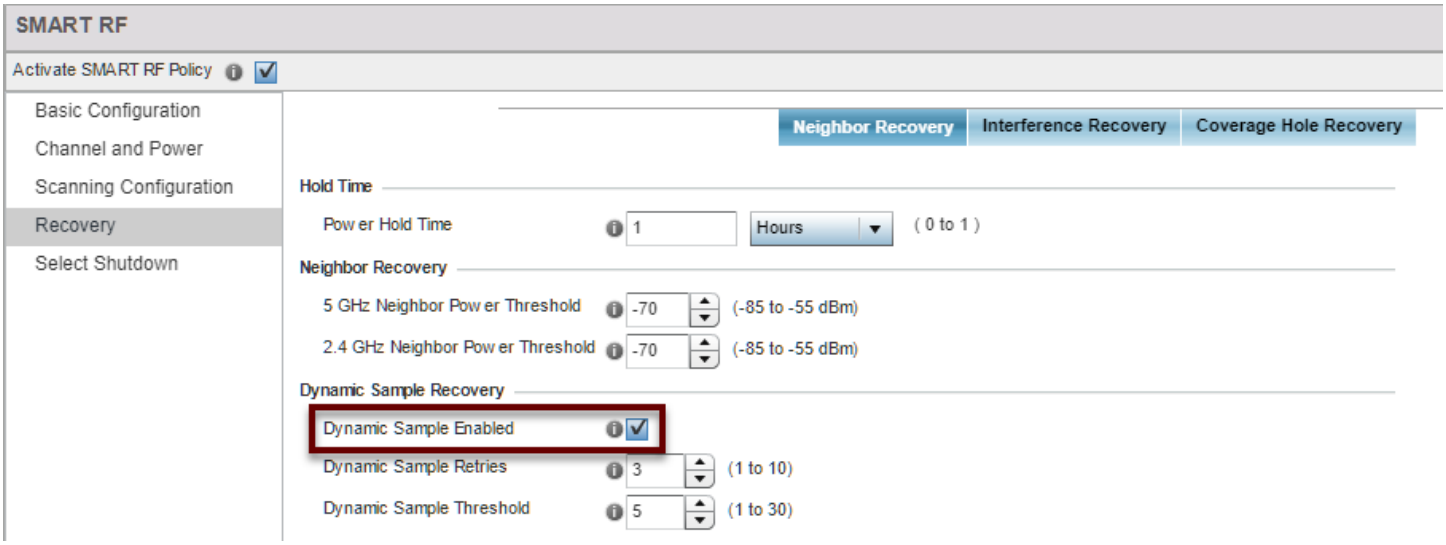
4. Use 20MHz wide channels in 5GHz, to allow for a better channel re-use.



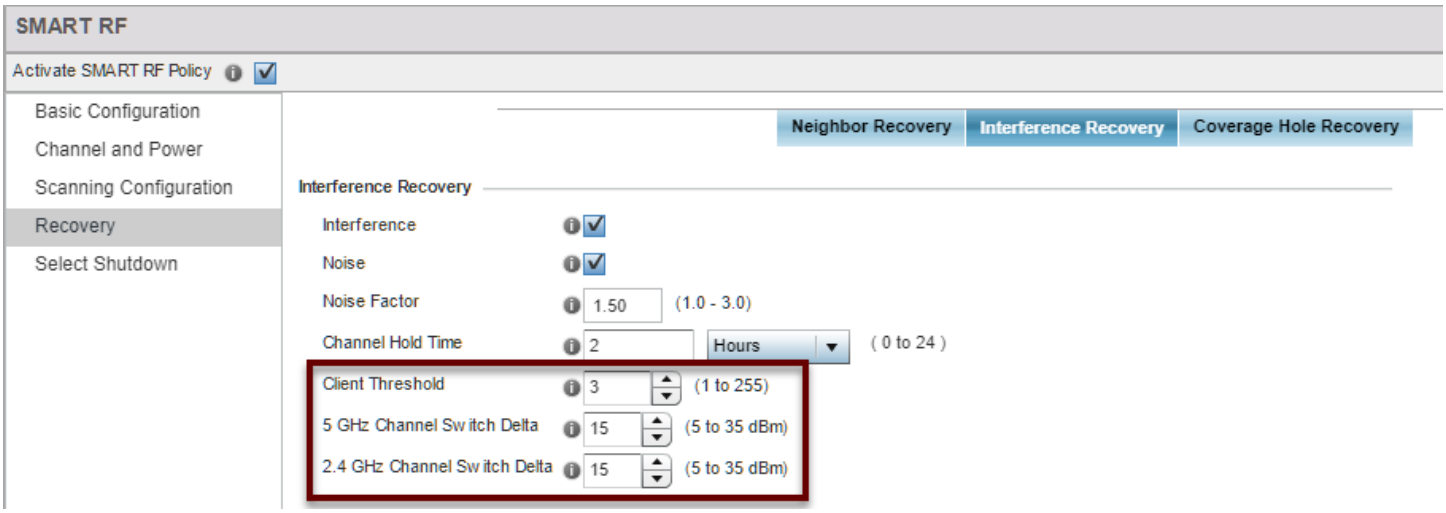
Set the following settings for the Off Channel Scanning mechanism used by SmartRF to monitor the environment:



Under ***Recovery → Neighbor Recovery*** enable *Dynamic Sampling*:



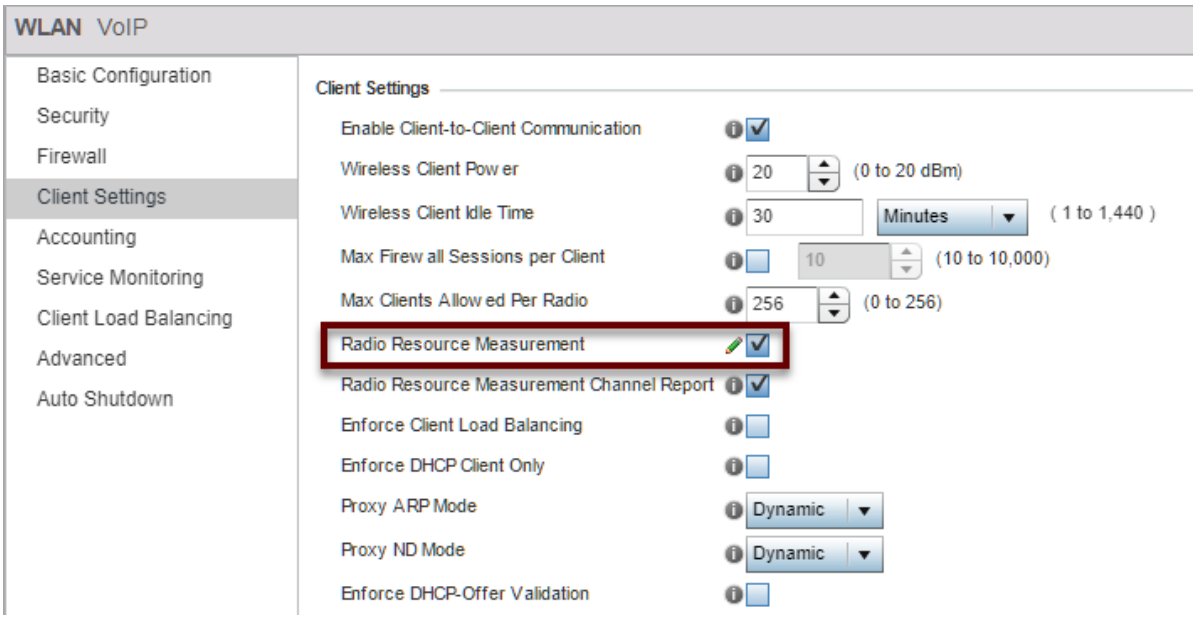
Move to ***Recovery → Interference Recovery*** and change the *client threshold* from default 50 down to 3 and *channel switch delta* to 15 for both 5GHz and 2.4GHz. Lowering down the client threshold prevents SmartRF radio from making a channel change (thus disrupting current clients) unless the radio has 3 or less clients connected. It is all about the balance between "should I switch to a better channel, because current channel is busy" or "should I keep everyone connected, no matter how bad/good their current experience is". Channel switch delta determines the SNR difference between current and potential new channel, i.e. if the new channel is by 15dB cleaner, then the radio will switch the channel.



WLAN Settings

Voice-enabled WLAN needs to have the following settings implemented as best practices:

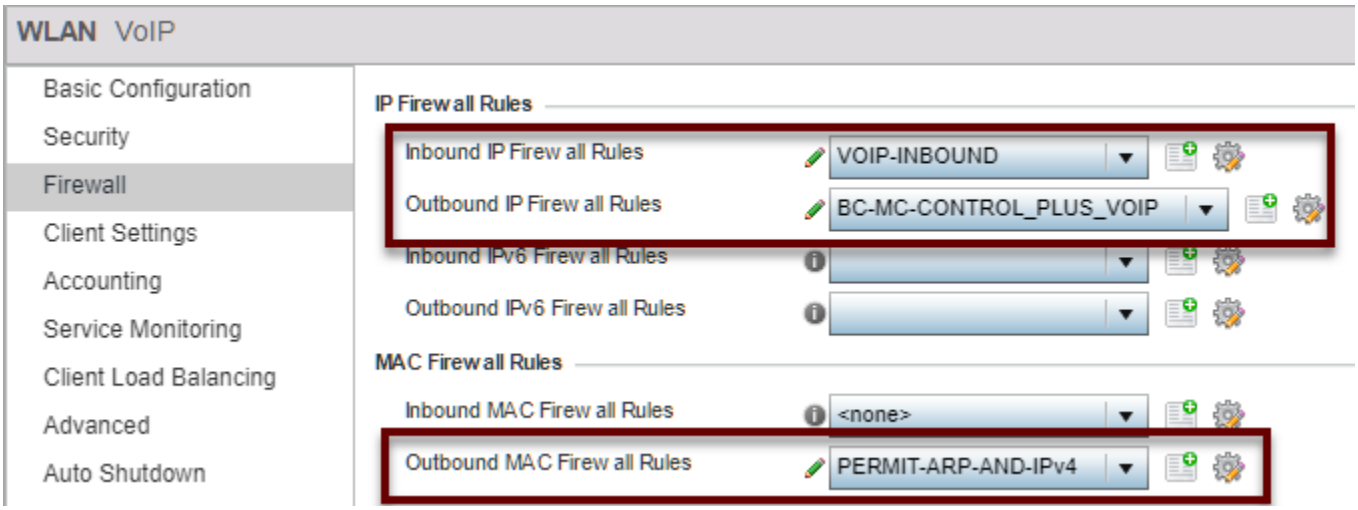
1. Assign Voice WLAN QoS policy created in the previous step
2. Enable Radio Resource Management (802.11k) for modern clients based on Android or iOS:

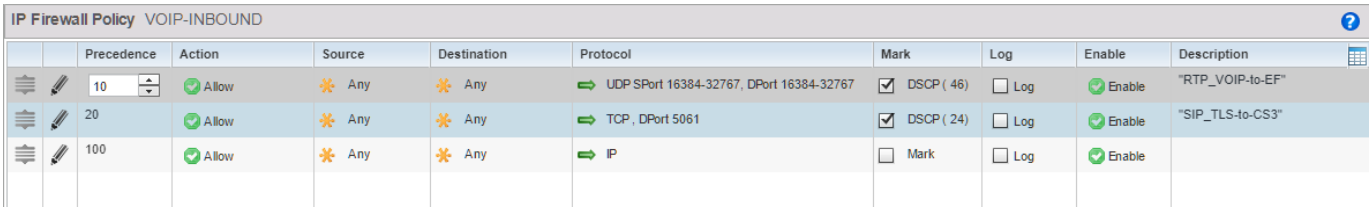


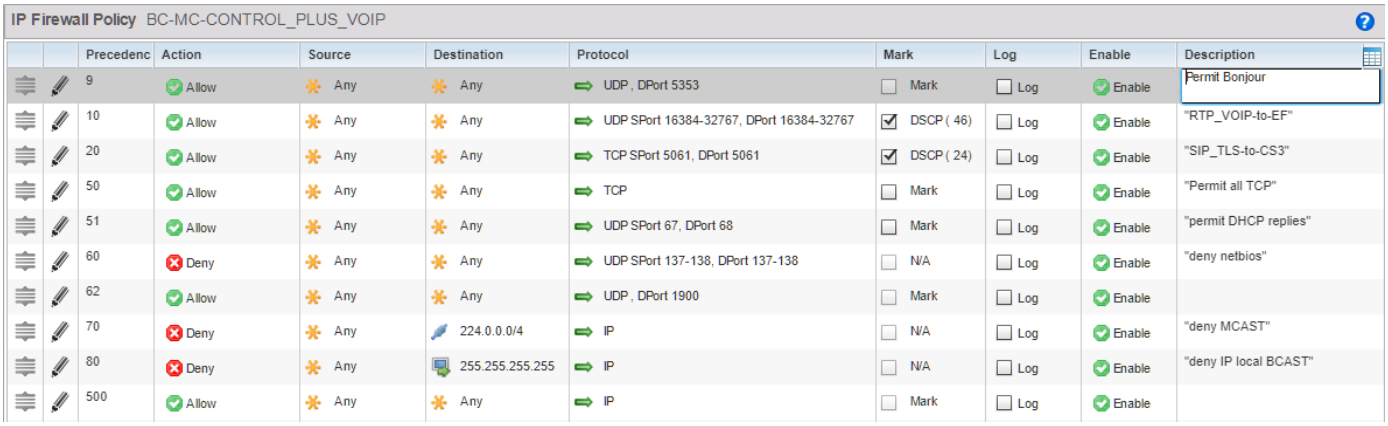
3. IP and MAC Access Lists

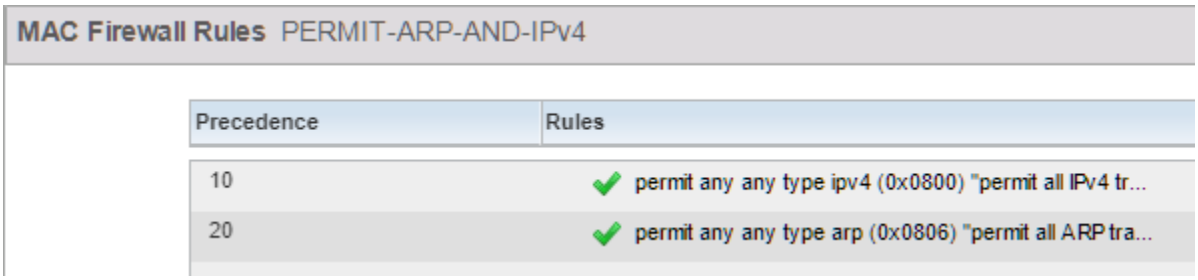
   It is always recommended to limit amount of Broadcast / Multicast traffic in the air. For this purpose, default Access Lists can be utilized for each WLAN outbound direction. These ACLs will limit amount of unneeded broadcast/multicast traffic hitting the air. In case some multicast addresses must be allowed in the air (e.g. Video streaming or PTT), these ACLs may be adjusted according to the particular use-case:

   Recommended WLAN ACL assignments:

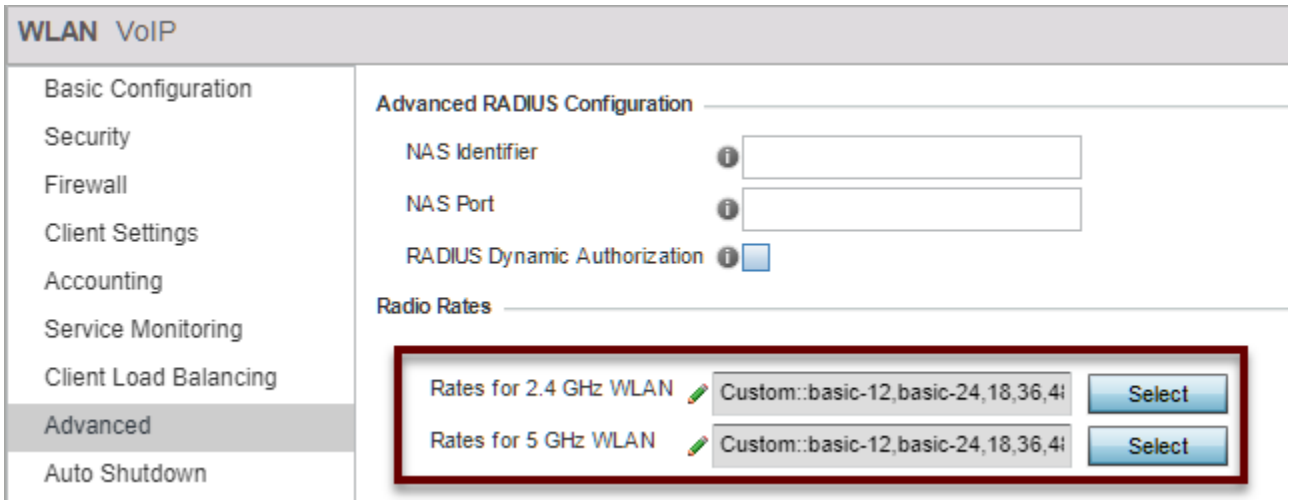


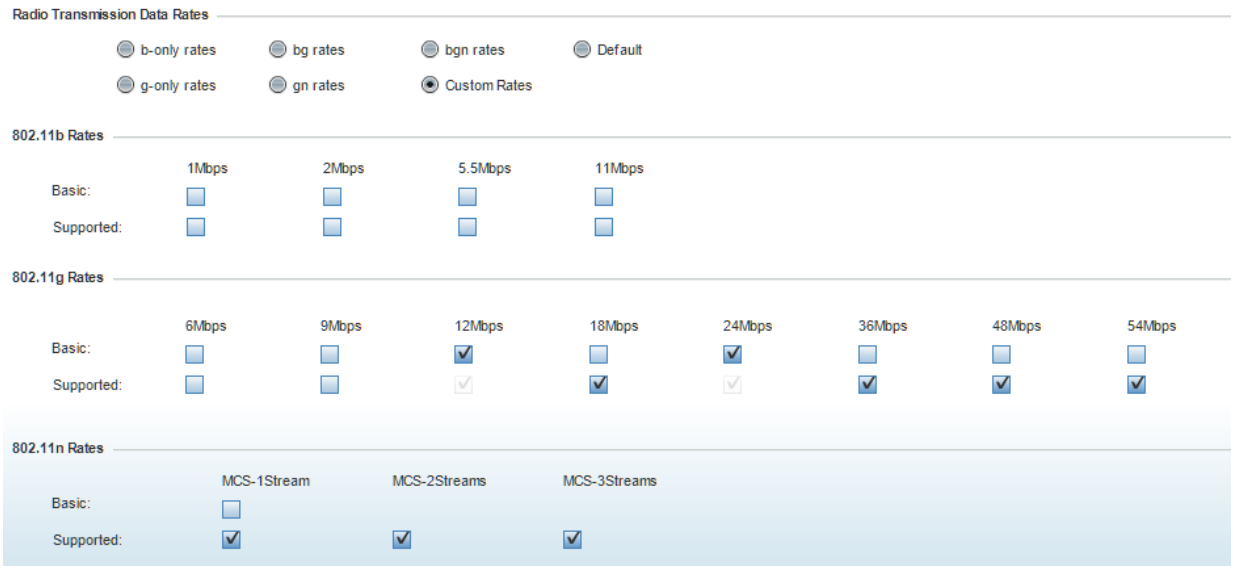






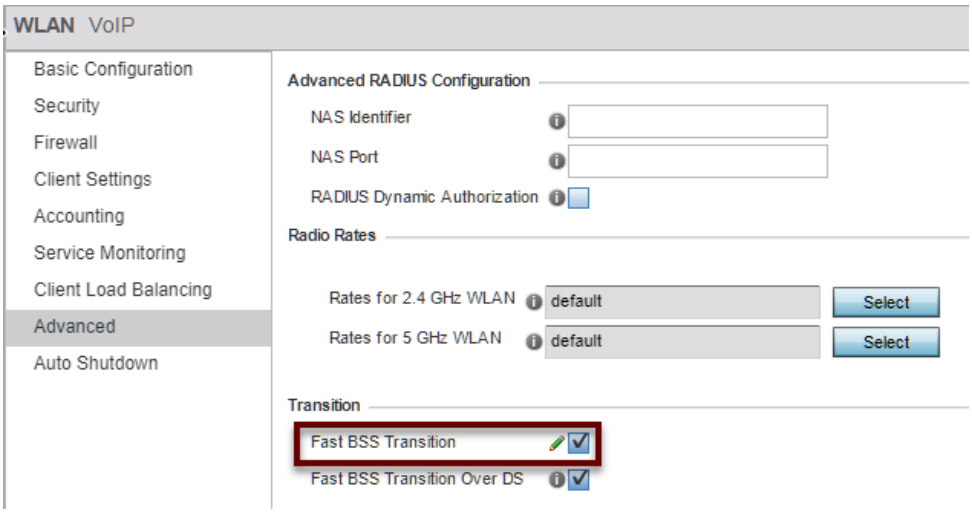
4. Set data-rates according to the AP density and use the following as guidelines:
   - For 2.4GHz disable 802.11b at the very minimum (you should not have any 802.11b-only voice phones hopefully). If AP density permits, disable 6 and 9 Mbps and leave 12Mbps as minimum basic rate.
   - For 5GHz with higher AP density start with 12Mbps as a minimum basic. Do not trip the minimum basic rate more than 24Mbps, as this might negatively affect clients.
   - For any Push-to-Talk services using multicast, carefully select highest basic rate, as this rate is going to be used to deliver multicast traffic. Leaving it at 24Mbps usually works very well.
   - Do not set all rates as basic.





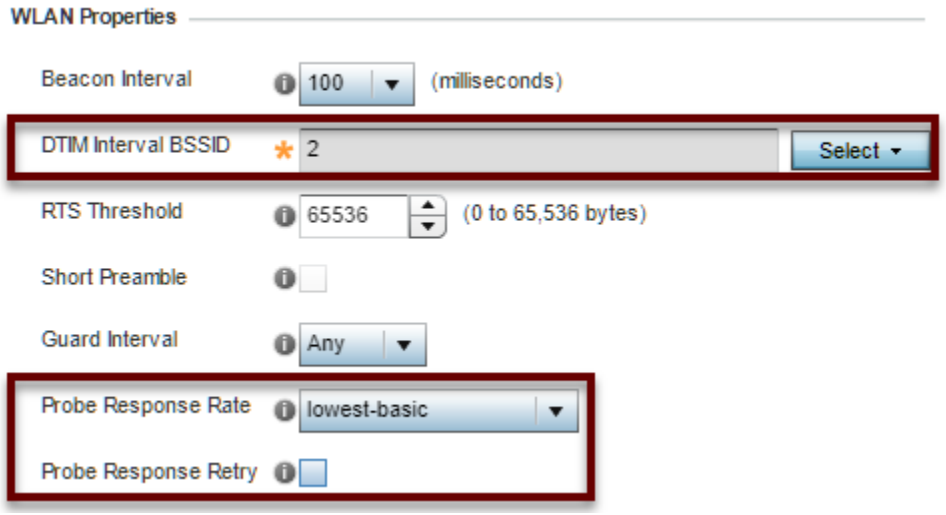
5. Chose authentication / encryption methods wisely. It is not only important to find out which authentication and encryption methods are supported by the VOIP client (WPA2-Enterprise with EAP authentication or WPA2-Personal with PSK), but also what type of fast roaming methods are supported by the client. It is crucial to make the roam time lower than 150ms to keep the voice call from dropping and keep acceptable voice quality.

   - Many legacy phones do not support any fast roaming methods, therefore implementing WPA2-Enterprise on a VOIP SSID is not recommended, as roaming times will be about 1 second, which will always result in dropped calls. In these cases, PSK authentication with CCMP encryption is the best way forward.
   - Most modern devices will support non-standardized fast roaming mechanisms, such as ***PMK*** caching and/or ***Opportunistic Key Caching (OKC)***. These fast roaming methods allow to completely skip EAP exchange during roam, and only perform 4way handshake for dynamic key generation. This makes roaming as fast, as with PSK network (about 50ms on average). The difference between PMK and OKC caching is that PMK caching only provides fast-roam "back to the old AP", while it does full EAP exchange and 4way handshake when client roams to a new AP. With OKC caching, fast roam is happening regardless if the AP is new, or the old "known" one. Both methods are enabled by default on WLAN settings.
   - The newest VOIP clients will support ***802.11r*** standard that provides extremely fast roaming times (about 5ms on average) for both WPA2-Enterprise or WPA2-Personal, as it allows to not only skip the EAP exchange, but also the 4way handshake. If your VOIP client supports 802.11r, it is recommended to enable in on WLAN settings:



Radio Settings

When trimming data-rates it is important to make sure that AP will respond to the client using a minimum basic rate configured, as opposed to the data rate at which client was probing. In addition, it is recommended to disable retrying of probe responses on the AP. DTIM settings should be configured based on the VOIP phone manufacturer recommendation, however the default setting of 2 will work well in most cases:



Mobility

Seamless Roaming Checklist

For seamless wireless client roaming and handoff following items must be ensured:

- Sufficient coverage cell overlap, i.e. the worst client should hear an AP at least at -67dBm.
- Key Caching must be enabled on the WLAN for secure fast roaming. OKC and PMK caching is enabled by default. It is recommended to enable 802.11r (fast-bss-transition) when clients support it.
- WNMP roaming notifications are responsible for updating wired infrastructure MAC address tables, as well as key cache exchange between the Access Points. It is important to ensure that:

For locally bridged WLANs:

- DST MAC `01:A0:F8:F0:F0:04` (WNMP roam notification) is allowed on the wired switches for all user VLANs, at least on the switchports going out to the APs.

For tunneled VLANs:

- DST MAC `01:A0:F8:F0:F0:04` (WNMP roam notification) is allowed on the wired switches for all user VLANs, on the switchports going out to the controllers.
- In case with MiNT level 2 tunneling and controller-managed RF Domains in a campus deployment “mint inter-tunnel-bridging” should be enabled only on the controller side to allow passing WNMP roam notifications between multiple MiNT tunnels. It must not be enabled in NOC deployments.
- In case with L2TPv3 tunnels from every AP back to the controllers, “`l2tpv3 inter-tunnel-bridging`” must be enabled on the controller side to allow passing of WNMP messages. It is not required when each remote site is tunneling via an RF Domain Manager.
- Wireless Firewall is enabled for client session migration to work. Additionally, for this feature to work Access Points must be able to discover each other over MiNT either at level 1 or level 2.

Stateful Firewall

For a highly mobile environment with a lot of handheld devices and roaming, for application and voice performance we would recommend disabling the layer 2 stateful packet inspection firewall:

For Voice there are multiple Application Layer Gateways (ALGs) available for various voice protocols and applications. They take care you automatically prioritizing voice traffic flow after a call session has been established and migrate session information upon client roam.

SIP ALG – Any typical SIP/RTP implementation will be supported by this ALG.

SCCP ALG – Skinny Call Control Protocol (Cisco).

FaceTime ALG – Apple's facetime audio/video protocol.

Configuration → Security → Wireless Firewall: