



Wireless Network Infrastructure

The Wireless IP Telephony network, just like a wired IP Telephony network, requires careful planning for VLAN configuration, network sizing, multicast transport, and equipment choices. For both wired and wireless IP Telephony networks, you should configure separate voice and data VLANs, provision sufficient network bandwidth, select the appropriate protocols and transport mechanisms, properly plan and configure connectivity to other networks, and select servers and switches for the network based on expected loads, numbers of users, and required features.

The following sections discuss various components and configurations that you should consider when designing a Wireless IP Telephony network:

- [VLANs, page 4-1](#)
- [Network Sizing, page 4-2](#)
- [Multicast and Wireless Voice, page 4-3](#)
- [Server and Switch Recommendations, page 4-4](#)
- [Interconnecting WLANs to the Cisco Campus Infrastructure, page 4-6](#)

VLANs

Virtual LANs (VLANs) provide a mechanism for segmenting networks into one or more broadcast domains. VLANs are especially important for IP Telephony networks, where the typical recommendation is to separate voice and data traffic into different Layer-2 domains.

Purpose of VLANs

Wireless LANs (WLANs) use VLANs to provide the following functions:

- Segment traffic into distinct broadcast domains or IP subnets
- Create separate security domains for various security models (Open, WEP, LEAP, PEAP, and EAP-TLS).

Voice and Data VLANs

Cisco recommends that you configure separate VLANs for voice and data traffic: a native VLAN for data traffic and a voice or auxiliary VLAN for voice traffic. A separate voice VLAN enables the network to take advantage of Layer-2 marking and provides priority queuing at the Layer-2 access switch port, thus ensuring that appropriate QoS is provided for various classes of traffic and helping to resolve addressing issues such as IP addressing, security, and network dimensioning.

Number of VLANs and SSIDs

Cisco Aironet 350, 1100, and 1200 Series Access Points support up to 16 VLANs. Cisco APs can be connected to Cisco Catalyst Switches via 802.1Q trunks. (In hybrid mode, the native VLAN's Port VLAN ID (PVID) is not tagged.) Each VLAN is then mapped to a unique Service Set Identifier (SSID) on the AP. Users (or IP Phones) can then be assigned to VLANs either statically based on SSID or dynamically through use of RADIUS authentication. Each VLAN can use a different security mechanism, although only one can be unencrypted (open).

For more details on deploying VLANs in wireless networks, refer to the Cisco Aironet 350, 1100, or 1200 Series *Wireless Virtual LAN Deployment Guide*, available at

<http://www.cisco.com>

Network Sizing

IP Telephony network sizing is essential to ensure that adequate bandwidth and resources are available to carry mission-critical voice traffic. In addition to the usual IP Telephony design guidelines for sizing components such as PSTN gateway ports, transcoders, WAN bandwidth, and so forth, also consider the following 802.11b issues when sizing your Wireless IP Telephony network:

Number of 802.11b Devices per AP

Cisco recommends that you have no more than 15 to 25 802.11b devices per AP.

Number of 802.11b Phones per AP

Before any discussion about network planning can take place, it helps to understand the basics of the overall network capacity.

The following network capacity guidelines apply to sizing the Wireless IP Telephony network:

- No more than 7 concurrent G.711 calls per AP.
- No more than 8 concurrent G.729 calls per AP.



Note

These design recommendations assume that Voice Activity Detection (VAD) has been disabled on the Cisco 7920 Wireless IP Phones. Use of VAD on the Cisco 7920 phones can conserve bandwidth, but Cisco recommends that you disable VAD on all Cisco CallManager servers to provide better overall voice quality.

In addition to determining how much bandwidth is needed for an 802.11b VoIP call, you must also consider overall radio contention for a particular RF channel. The general rule is that you should not deploy any more than 20 to 25 802.11b endpoints per AP. The more endpoints you add to an AP, the more you reduce the amount of overall bandwidth and potentially increase transmission delays.

The maximum number of phones per AP depends on the calling patterns of individual users (based on Erlang ratios). Cisco recommends no more than 7 concurrent calls using G.711 or 8 concurrent calls using G.729. Beyond that number of calls, when excessive background data is present, the voice quality of all calls becomes unacceptable.

Packetization rates for these recommendations are based on 20-ms sample rates with VAD disabled. This rate generates 50 packets per second (pps) in each direction. Using a larger sample size (such as 40 ms) could result in a larger number of simultaneous calls, but it will also increase the end-to-end delay of the VoIP calls.

Number of 802.11b Phones per Layer-2 Subnet or VLAN

The number of 802.11b phones you can deploy per Layer-2 subnet or VLAN depends on the following factors.

- No more than seven G.711 or eight G.729 active calls per AP
- The calling ratio used to determine the number of active and non-active calls. This ratio is often determined using Erlang calculators.

Based on these factors and normal business-class Erlang ratios (between 3:1 and 5:1), Cisco recommends that you deploy no more than 450 to 600 Cisco 7920 phones per Layer-2 subnet or VLAN.

Multicast and Wireless Voice

Multicast network traffic can be problematic on a wireless network, especially for wireless voice networks. Although 802.11b WLANs are capable of sending multicast IP packets, there are technical limitations that make multicast unsuitable for voice networks and real-time applications such as multicast music on hold (MoH).

Multicast network traffic can be an issue on wireless networks due to the following factors:

- Multicast transport on the WLAN is unacknowledged. While this factor might seem irrelevant for UDP packets such as voice traffic, the difference is that an Ethernet connection has a bit-error rate (BER) of about 10^{10} while a WLAN has a BER of about 10^5 . WLANs resolve this issue by using acknowledgements on the link layer to ensure reliable delivery. This reliable delivery does not occur for multicast traffic.
- Multicast packets are transmitted at the lowest rate of any device associated with the AP, whether that client wants the multicast packets or not. Thus, an AP supporting multiple bit rates will send multicast traffic at the lowest bit rate. This behavior degrades the overall performance of the WLAN.
- When devices operate in power-save mode (such as when a Cisco 7920 phone enters power-save mode to extend its battery life), the AP buffers the multicast packets and does not send them until the devices are no longer in power-save mode. This practice ensures that all clients receive the multicast traffic.

For these reasons, the Cisco 7920 Wireless IP Phone does not support multicast traffic, and Cisco recommends unicast-only traffic in wireless telephony environments. Although it is usually desirable to send traffic such as music-on-hold to phones via multicast for all voice endpoint devices, multicast is not possible for the Cisco 7920 phone because only unicast MoH is supported. Currently Cisco CallManager software has no ability to differentiate automatically between those endpoint devices that are enabled for multicast and endpoint devices that are capable of unicast only. Thus, even if a Cisco CallManager is configured with both multicast and unicast MoH resources, it has no way to determine dynamically which devices are capable of receiving multicast streams. To handle a mixture of multicast and non-multicast endpoint devices, Cisco CallManager must be told which devices can receive multicast

MoH streams and which devices can receive only unicast MoH streams. You can provide Cisco CallManager with this information by configuring separate media resource groups (MRG) and media resource group lists (MRGL) for multicast and unicast resources.

Server and Switch Recommendations

The following sections recommend server and switch types to use in building the wireless network infrastructure for the Cisco 7920 Wireless IP Phones.

Server Recommendations

A voice network requires at least one Cisco CallManager server. This server can be located either on-site or remotely over a WAN link; however, servers located over a WAN link can cause delays in phone registration, roaming, and call set-up. If problems arise, test the scenario with wired phones going to the same Cisco CallManager to test the WAN speeds. The wired phone must be on the same VLAN and switch port as the AP in order to check the entire path of the packet, just as if it came from the AP to the Cisco CallManager server. It might become necessary to either decrease the delay times on the WAN link or move the Cisco CallManager server on-site.

**Note**

Cisco recommends that you use Cisco CallManager Release 3.3 (3) SR1 or later for wireless voice deployments.

A central authentication, authorization, and accounting (AAA) server can be used to perform LEAP and/or MAC authentication. This server can also be placed on-site or over a WAN link. A WAN link can add considerable delays in authentication, so Cisco generally recommends that you deploy a local AAA server to expedite the authentication process. AAA functions can also be performed by a dedicated Cisco IOS AP that is running local authentication. However, this AP can only support 50 users and should be considered only in small offices or specialty locations (for example, retail stores).

**Note**

Cisco recommends that you use Cisco Authentication and Control Server (ACS) version 3.1 or later for wireless voice deployments.

If two APs terminate on the same network appliance, Cisco highly recommend that you do *not* use a hub because the hub will add delays on the Ethernet interface as well as on the RF interface. Rather, use a switch, which has multiple collision domains. In addition, Cisco recommends that you do not use hubs anywhere that devices connect to an AP because the hub will send unnecessary data to the AP.

Switch Recommendations

**Note**

If you are using a Cisco Catalyst 4000 Series Switch as the main router in the network, ensure that it contains, at a minimum, either a Supervisor Engine 2+ (SUP2+) or Supervisor Engine 3 (SUP3) module. The SUP1 or SUP2 module can cause roaming delays, as can the Cisco Catalyst 2948G, 2980G, 2980G-A, 4912, and 2948G-GE-TX switches.

You can create a switch port template for use when configuring any switch port for connection to an AP. This template should add all the baseline security and resiliency features of the Standard Desktop template. In addition, when attaching the AP to a Cisco Catalyst 3550 switch, you can optimize the performance of the AP by using Multilayer Switching (MLS) QoS commands to limit the port rate and to map Class of Service (CoS) to Differentiated Services Code Point (DSCP) settings. For an example of an AP switch port template for the Catalyst 3550 switch, see [Interconnecting WLANs to the Cisco Campus Infrastructure, page 4-6](#).

While Ethernet switch ports can typically transmit and receive at 100 Mbps, APs (depending on the type of radio) have a lower throughput rate because individual 802.11 standards allow for a maximum data rate of 54 Mbps. Furthermore, wireless LANs are a shared medium and, due to contention for this medium, the actual throughput is substantially lower. This throughput mismatch means that, with a burst of traffic, the AP will drop packets, thus adding excessive processor burden to the unit and affecting performance.

By taking advantage of the Catalyst 3550 policing and rate limiting capabilities, you can eliminate the need for the AP to drop excessive packets. The proposed AP switch port template will rate-limit the port to the practical throughput of 7 Mbps for 802.11b and guarantee 1 Mbps for high-priority voice and control traffic. With this prioritization, the template can be used with the Cisco 7920 Wireless IP Phones. [Table 4-1](#) shows the allowed throughput for various types of AP radios.

Table 4-1 Switch Port Throughput for Various Radio Types

Type of Radio	Throughput Allowed by Switch Port
802.11a	42 Mbps
802.11b	7 Mbps
802.11g	36 Mbps
802.11a + 802.11b	49 Mbps
802.11a + 802.11g	78 Mbps

This template helps create a secure and resilient network connection with the following features:

- Return Port Configurations to "default" — Prevents configuration conflicts by clearing any pre-existing port configurations.
- Disable Dynamic Trunking Protocol (DTP) — Disables dynamic trunking, which is not needed for connection to an AP.
- Disable Port Aggregation Protocol (PagP) — PagP is enabled by default but is not needed for user-facing ports.
- Enable Port Fast — Allows a switch to quickly resume forwarding traffic if a Spanning Tree link goes down.
- Configure Wireless VLAN — Creates a unique wireless VLAN that isolates wireless traffic from other data, voice, and management VLANs, thereby isolating traffic and ensuring greater control of traffic.
- Enable Quality of Service (QoS); Don't trust port (mark down to 0) — Ensures appropriate treatment of high-priority traffic, including softphones, and prevents users from consuming excessive bandwidth by reconfiguring their PCs.

Cisco 3550-24-PWR Inline Power Switches can be used to provide power to APs that are capable of receiving inline power.

Interconnecting WLANs to the Cisco Campus Infrastructure

The following switch configuration shows an example of a switch port template for connecting APs to the Cisco Catalyst 3550 switch.

Example 4-1 Connecting APs to Catalyst 3550 SMI/EMI

```

default interface <xx/yy>
spanning-tree bpduguard enable
spanning-tree bpdufilter enable
no channel-protocol pagp
spanning-tree portfast
!
mls qos
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos map policed-dscp 24 26 46 to 8
mls qos aggregate-policer AGG-POL-1M-VOICE-OUT 1000000 8000 exceed-action
policed-dscp-transmit
mls qos aggregate-policer AGG-POL-6M-DEFAULT-OUT 6000000 8000 exceed-action drop
!
class-map match-all EGRESS-DSCP-0
  match ip dscp 0
class-map match-all EGRESS-DSCP-8
  match ip dscp 8
class-map match-all EGRESS-DSCP-16
  match ip dscp 16
class-map match-all EGRESS-DSCP-32
  match ip dscp 32
class-map match-all EGRESS-DSCP-48
  match ip dscp 48
class-map match-all EGRESS-DSCP-56
  match ip dscp 56
class-map match-any VOICE-SIGNALING
  match ip dscp 24
  match ip dscp 26
class-map match-all VOICE
  match ip dscp 46
class-map match-all INGRESS-DATA
  match any
class-map match-all INGRESS-VVLAN-VOICE
  match vlan 3
  match class-map VOICE
class-map match-all INGRESS-VVLAN-VOICE-SIGNALING
  match vlan 3
  match class-map VOICE-SIGNALING
class-map match-all INGRESS-DVLAN
  match vlan 2
  match class-map INGRESS-DATA
!
policy-map EGRESS-RATE-LIMITER
class EGRESS-DSCP-0
  police aggregate AGG-POL-6M-DEFAULT-OUT
class EGRESS-DSCP-8
  police aggregate AGG-POL-6M-DEFAULT-OUT
class EGRESS-DSCP-16
  police aggregate AGG-POL-6M-DEFAULT-OUT
class EGRESS-DSCP-32
  police aggregate AGG-POL-6M-DEFAULT-OUT
class EGRESS-DSCP-48
  police aggregate AGG-POL-6M-DEFAULT-OUT
class EGRESS-DSCP-56
  police aggregate AGG-POL-6M-DEFAULT-OUT

```

```
class VOICE
  police aggregate AGG-POL-1M-VOICE-OUT
class VOICE-SIGNALING
  police aggregate AGG-POL-1M-VOICE-OUT
!
policy-map INGRESS-QOS
class INGRESS-VVLAN-VOICE
  set ip dscp 46
class INGRESS-VVLAN-VOICE-SIGNALING
  set ip dscp 24
class INGRESS-DVLAN
  set ip dscp 0
!
!
interface [interface id]
description 11Mb towards Wireless Access Point
switchport access vlan 2
switchport voice vlan 3
no ip address
mls qos monitor dscp 0 10 18 24 26 34 46 48
mls qos monitor dscp 56
service-policy output EGRESS-RATE-LIMITER
service-policy input INGRESS-QOS
wrr-queue bandwidth 5 25 70 1
wrr-queue cos-map 1 1
wrr-queue cos-map 2 0
wrr-queue cos-map 3 2 3 4 6 7
wrr-queue cos-map 4 5
priority-queue out
```

