Real-time Traffic over WLAN Overview

This chapter discusses about drivers and benefits of implementing an RToWLAN deployment followed by an illustration that depicts an enterprise solution reference network architecture. This chapter also identifies the high-level touch points of the RToWLAN solution deployment, provides a brief overview of RToWLAN solution architecture, and describes the following three main RToWLAN solution components:

- 802.11 enterprise WLAN solution infrastructure
- Enterprise collaboration solution applications and services
- Real-time Traffic over WLAN endpoints

After the description of the components, the chapter describes common RToWLAN solution design considerations across both single-site and distributed multisite deployments with specific focus on quality of service (QoS), security, high availability, and capacity planning.

RToWLAN solution drivers and benefits

Enterprises today are faster-paced than ever before. To succeed, grow, and stay ahead of the competition, enterprises depend on efficient employees, collaboration, and a timely business process. While maintaining a secure corporate data and communications infrastructure, enterprises are encouraging a mobile work style to get more work done. Additionally, enterprises are not just streamlining processes through technology but

are also looking to increase their revenue and reduce costs with new technology that improves user productivity and accelerates business processes.

Real-time traffic applications and services that are delivered over WLAN networks provide the following benefits:

- **Eliminates the need for mobile cellular devices in the enterprise:** IP voice and video over WLAN calls traverse the enterprise WLAN in whole or in part, providing cost savings over direct cellular network calls. Employees can use their voice or video over WLAN endpoint or client on campus instead of consuming voice minutes over the cellular voice network.
- **Reduces dependency on mobile provider network coverage within the enterprise:** By leveraging 802.11 WLAN network connectivity, enterprises provide adequate network coverage and capacity by deploying sufficient number of access points and at the same time reducing or eliminating dependency on mobile provider network coverage within the enterprise.
- **Enablement of employee-owned personal and guest devices:** With the prevalence of personal mobile devices like smartphones and tablets, there is an increasing inflow of these devices into the enterprise. This type of enterprise is often called *bring your own device* (BYOD). Enabling employee-owned or guest devices with a BYOD solution:
  - increases overall employee satisfaction.
  - improves productivity when enabling device for real-time traffic collaboration applications and services.
- **Maximizes availability and reachability of mobile employees:** By enabling mobile devices for enterprise collaboration, you can reach employees anywhere within the enterprise, and the user experience on the mobile device is equivalent to that of the traditional enterprise endpoint. This flexibility provides a smooth experience to users who transition between many enterprise clients and devices.
- **Ensures high-quality voice and video calls and seamless mobile user experience for fixed mobile substitution (FMS) deployments:** To enable enterprise directory number use on dual-mode mobile smartphones and tablets through enterprise IP telephony systems, you must send IP voice and video calls over the enterprise WLAN network. A RToWLAN network is tuned to provide optimal bandwidth and throughput as well as higher-priority queuing or transmission on the network for real-time traffic. In the case of IP-based voice and video calls, this means minimized packet loss, jitter, and delay translating to high-quality voice and video. Enabling the enterprise directory number usage on mobile endpoints and clients:
  - provides integration to enterprise IP call-control features.
  - provides enterprise dial plan, enabling seamless user experience across enterprise devices.
  - eliminates the need for an enterprise deskphone for mobile employees.

RToWLAN deployments can help enterprises to:

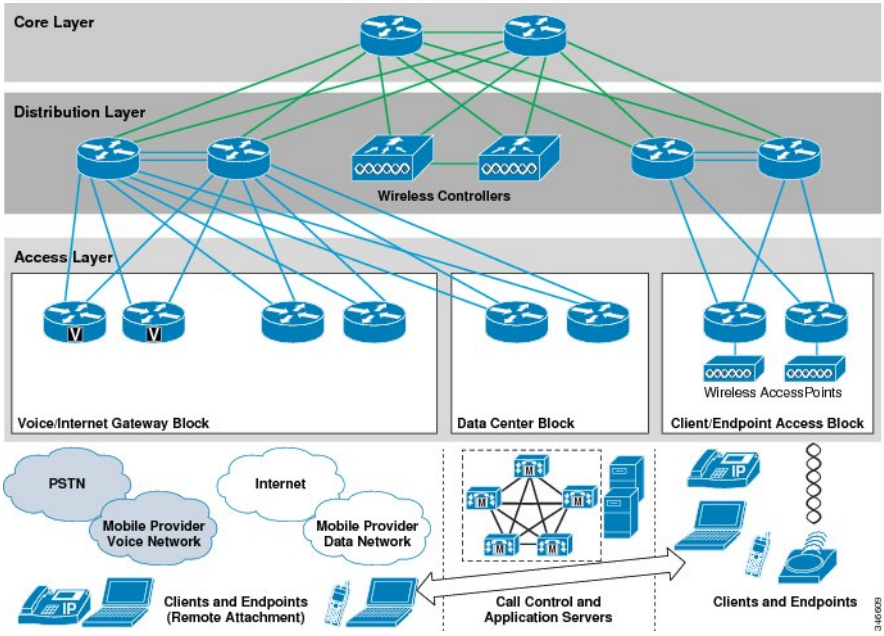
- Reduce expenditures for mobile provider voice and data services.
- Improve employee productivity, reachability, and availability.
- Leverage the increased presence of personal mobile devices within the enterprise for collaboration and communication at less or no cost with BYOD solutions.
- Improve employee satisfaction when they engage with collaboration and other business applications and services by providing flexibility and a seamless user experience.

RToWLAN solution reference network design architecture

This section provides a high-level example network topology (see Figure 1: Real-Time Traffic over WLAN Solution Network Topology Overview, on page 3) for deploying real-time traffic applications and services for wireless endpoints and clients. This RToWLAN solution design example uses a typical hierarchical, access, distribution, and core campus network as a basis. The following additional components are included in this design:

- WLAN Controller (WLC) and Access Points (APs) to provide the wireless network infrastructure for carrying real-time and other IP network traffic.
- Wireless access points added to Client and Endpoint Access Blocks for client and mobile endpoint wireless network attachment.
- Data Center Block including call control and other application servers for enabling real-time traffic.
- Voice and Internet Gateway Block for access to PSTN and to provide access to and from the enterprise.

Figure 1: Real-Time Traffic over WLAN Solution Network Topology Overview



The two key solution component areas of focus for any enterprise RToWLAN deployment are:

- Enterprise 802.11 wireless infrastructure enabled within the Distribution and Client and Endpoint Access blocks as shown in the preceding figure.
- Enterprise collaboration infrastructure enabled within the Data Center and Voice and Internet gateway as shown in the preceding figure.

Enterprise wireless LAN overview

The enterprise 802.11 wireless LAN (WLAN) infrastructure is the underlying foundation for any RToWLAN solution deployment. The enterprise wireless network must be designed to ensure that network connectivity is available for wireless endpoints and that sufficient bandwidth and throughput for real-time traffic is provided. The WLAN must be designed with sufficient capacity for the number of RToWLAN endpoint devices expected to be deployed. The WLAN must also be designed with sufficient redundancy such that hardware or IP connection failures do not completely eliminate WLAN network availability.

The WLAN infrastructure not only provides network connectivity but just as with wired networks, the infrastructure also provides authentication and encryption security services and quality of service for better than best effort treatment for select traffic. To deliver this functionality, the 802.11 WLAN infrastructure consists of a number of components and applications including wireless LAN controllers (WLCs), wireless access points (APs), and wireless LAN management applications.

Enterprise collaboration overview

Collaboration systems enable a large number of features and services. The most common and prevalent feature is voice and video over IP calling. However, these collaboration systems can provide communication features and functions above and beyond traditional IP telephony including conferencing, messaging, presence, information and document sharing, fixed mobile convergence, and directory integration. These features and services are often deployed in tandem, providing a comprehensive collaboration solution for enterprises and their workers. To deliver these features and services, the collaboration system relies on a number of components and applications including voice and video endpoints, gateways and application servers including voicemail and presence.

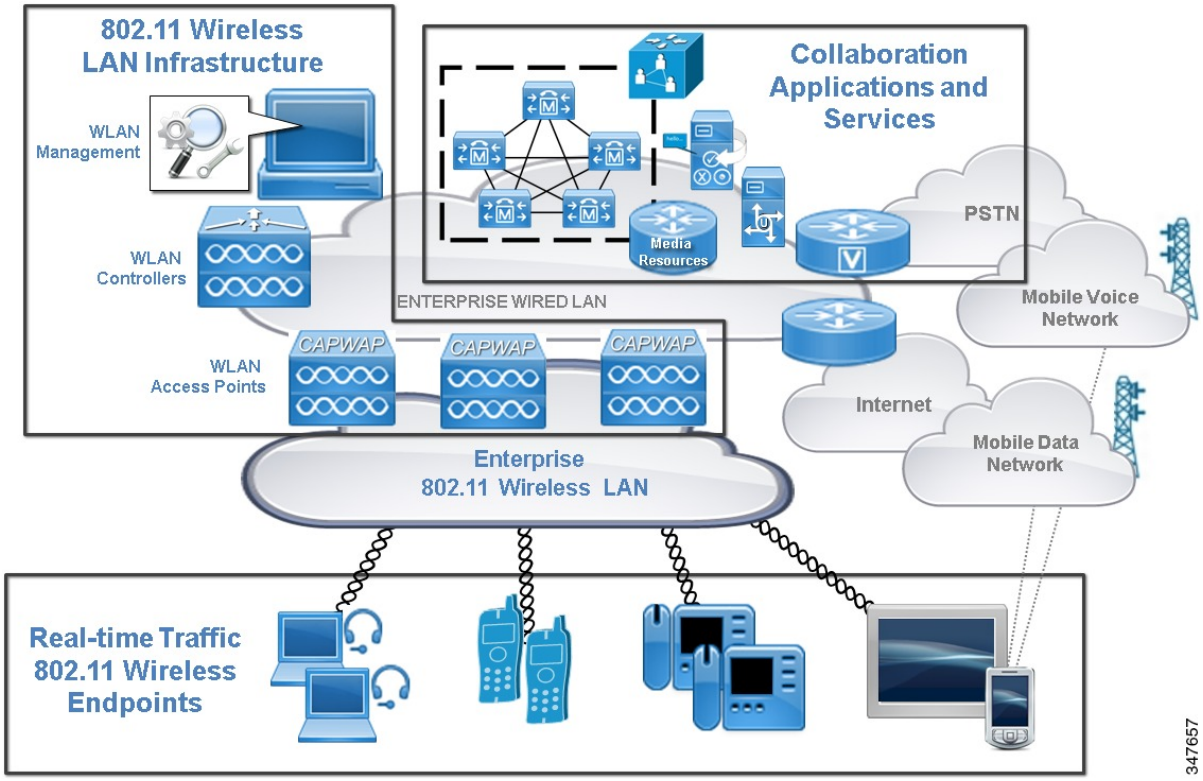
RToWLAN solution architecture overview

The overall architecture for an RToWLAN solution deployment (see Figure 2: RToWLAN solution architecture overview, on page 5) consists of the following three main components:

- **802.11 Wireless LAN infrastructure:** The wireless infrastructure enables the 802.11 wireless LAN for endpoint or client attachment. This infrastructure includes the WLAN controller, access points, and management applications.
- **Collaboration applications and services:** Collaboration applications enable real-time traffic services, including voice and video calling. These applications and services include call control, PSTN gateways, media resources, voicemail, and instant messaging and presence.
- **Real-time traffic capable 802.11 wireless endpoints:** Wireless endpoints consume and generate real-time traffic over the 802.11 WLAN. These endpoints include wireless-enabled desktop and mobile software applications and clients as well as wireless IP phone hardware.

All of these components are involved in enabling RToWLAN applications and delivering real-time services wirelessly.

Figure 2: RToWLAN solution architecture overview



See Figure 2: RToWLAN solution architecture overview, on page 5 above and subsequent discussions within this chapter do not include information about basic network services that are provided by typical enterprise applications and servers. These network services are assumed to be present, and considerations related to the following are not discussed except in cases that are directly related to RToWLAN:

- Network-based device and user authentication and identification services, including certificate authority servers, two-factor authentication supplicants, identity stores like directory servers, and any other applications or components that provide security services.
- Network time and IP address resolution and assignment, including network time services (NTP), domain name services (DNS), and dynamic IP address assignment (DHCP).
- Network routing, packet forwarding and queuing, quality of service, and admission control.

Enterprise 802.11 wireless LAN solution infrastructure

The enterprise 802.11 wireless LAN (WLAN) network is essential for RToWLAN solutions, because the wireless infrastructure provides the network that transports real-time traffic that connected real-time traffic capable wireless devices generate and consume. The following table lists the 802.11 wireless network infrastructure components:

Table 1: 802.11 Wireless Network Infrastructure Components

802.11 wireless network infrastructure components	Description
Wireless LAN access points	The wireless LAN access point provides wireless network access to wireless devices that enables the devices and clients to communicate with wired network components. The access points not only provide wireless device network connectivity, but they also serve as the demarcation point between the wired and wireless networks. The wireless LAN controllers manage the access points that are registered to them.
Wireless LAN controllers	The wireless LAN controller (WLC) is a network infrastructure device that performs the central management role in the wireless network. WLCs make it easier to manage wireless LAN deployments by centralizing access point configuration and management, radio frequency monitoring, and client association and authentication. After the wireless access points register to a WLC, the wireless access points tunnel all management and client traffic to the WLC. The WLC is also responsible for switching traffic between wireless clients and the wired portion of the network.
Wireless management	Wireless LAN management applications and services provide a robust wireless life-cycle management tool that enables network administrators to successfully plan, deploy, monitor, troubleshoot, and report on wireless networks.

You must design the enterprise WLAN network to meet the needs of the users, applications, and endpoints. The WLAN coverage must provide enough bandwidth on the Wi-Fi channels to support quality application performance. To design enough bandwidth into WLAN coverage areas for the users, you must understand the Wi-Fi performance capabilities of the endpoints. Wireless endpoints and mobile client devices are available in different varieties, and not all wireless clients have the same capabilities. You must perform detailed wireless infrastructure planning for the WLAN deployment to be successful.

For a successful wireless network deployment, you must conduct a thorough wireless site survey to ensure that the radio frequency configuration and design are optimized to provide necessary bandwidth and throughput to endpoints in motion throughout the deployment. In addition, the site survey helps you identify the sources of interference so that they can be eliminated. A site survey seeks to verify the following basic radio frequency design principles:

- **Adjacent channel cell separation:** Same channel or adjacent channel can cause interference, which reduces network throughput and leads to increased packet loss. Through site survey, you can verify that adjacent channel cells are separated appropriately.
- **Nonadjacent channel cell overlap:** Nonadjacent channel cells should be overlapped to ensure that wireless endpoints can seamlessly transition or roam between access points and wireless channel cells. Through site survey, you can verify that nonadjacent channel cells are overlapped sufficiently.
- **Channel cell coverage for all desired areas of service:** If wireless network coverage is expected in stairwells, between buildings, or on building perimeters, you can verify through site survey that access

points and antennas are located properly to provide appropriate wireless channel coverage in all required locations.

- **Channel cell density:** Appropriate channel cell density must be provided such that the required number of endpoints are supported with necessary network bandwidth and throughput provided on WLAN channels to support quality real-time application and service performance.
- **Wireless interference identification and mitigation:** Wireless interference caused by improper AP and antenna placement, physical structures and characteristics of the deployment area, and poor radio frequency design must be identified during a site survey. Further, sources of interference such as cordless phones, personal wireless network devices, sulphur plasma lighting systems, microwave ovens as well as high-power electrical devices such as transformers, heavy-duty electric motors, refrigerators, elevators and elevator equipment, and any other power devices that could cause electromagnetic interference (EMI) must be considered when you plan a WLAN deployments. You must mitigate these interference sources by adjusting access point locations and antenna direction, radio frequency configuration and AP power levels, or by removing or eliminating these interference sources.

Today, controllers and access points are purpose-built for particular use cases and levels of scale. In a home environment, a limited number of mobile client devices share the same WLAN channel radio frequencies at the same time. Hence, bandwidth is not a concern. However, in an enterprise environment, many devices are connected to a Wi-Fi channel. With inadequate bandwidth, voice calls may become inaudible, video calls may become unwatchable, and in some cases, the application fails.

Related Topics

Real-Time Traffic over WLAN Radio Frequency Design
Cisco wireless products
Enterprise Mobility Design Guide

Enterprise collaboration solution applications and services

After the enterprise wired and wireless LAN is planned and deployed, you must deploy the enterprise collaboration applications, services, and endpoints on top of this infrastructure. The enterprise collaboration deployment must be properly designed to ensure that required components, applications, and services are available and that the infrastructure provides sufficient capacity and reliability.

Collaboration systems enable a large number of features and services, including voice and video calling; messaging, including voicemail and instant messaging (IM), presence and availability; media resources, including conferencing and music on hold, and directory integration. These features and services are often deployed in tandem, which provides a comprehensive collaboration solution for enterprises and their workers.

The enterprise call control platform, which is considered central to the collaboration system, is responsible for providing voice and video calling services (for example, Cisco Unified Communications Manager). The collaboration system also relies on several components and applications, including the following:

- **Gateways:** Platforms with IP or TDM interfaces that provide external access to the PSTN as well as internal access to other call control platforms, applications, and devices.
- **Media Resources:** Hardware or software-based resources that are deployed throughout the network to enhance call flows with supplementary services like voice and video conferencing, music on hold, and transcoding.

- **Collaboration applications:** Applications that provide communication features and functions beyond traditional voice and video calling. These include voicemail, IM and presence, conferencing, information and document sharing, fixed mobile convergence, and directory integration.

Voice and video endpoints are also a key component of the collaboration system. Enterprise users communicate and collaborate with endpoints including desk phones, wireless phones, software clients, immersive video systems, and mobile clients for smartphones and tablets.

When deploying collaboration hardware, applications and services, and before enabling real-time traffic capable wireless endpoints, ensure that the required collaboration and communication applications and services are deployed and configured appropriately. You must consider the following factors:

- Device configuration

  Device configuration within the call control system including, location, user association, calling privileges, button layout, and other feature settings must be configured correctly for proper operation.

- Network service operations

  Devices must be capable of attaching to the network, retrieving or receiving their configuration from the call control system over the network, and connecting to and communicating with the collaboration infrastructure components.

- Dial plan

  The enterprise dial plan that is configured on the call control system is as fundamental to collaboration system operation as IP addressing and routing are to IP networking. You must implement the following dial plan configuration correctly to ensure that users are capable of making and receiving calls:

  - The numbering or assigning of directory or telephone numbers to devices
  - The dialing habits enabled and the classes of restriction applied to devices
  - The manipulation of called or calling numbers as configured for the device

- Intercomponent integration

  Enable and configure integrations between collaboration and communication infrastructure components to deliver additional features and services. For example, integrations between the call control platform and PSTN gateways or border controllers, the voicemail and IM or presence application servers, and directory or contact source platform must be put in place to enable additional services like PSTN access or IM and presence.

- Security

  Deploy security features as indicated by enterprise security policies to ensure that operations are secured. Specifically, if you plan to use functionality such as encrypted voice or video media or signaling, certificate-based trunk integrations, or digest authenticated devices, then you must deploy an appropriate configuration and infrastructure, including a certification authority server.

Use a nonwireless real-time traffic capable endpoint first to verify the preceding considerations and ensure that the required features and functions are working correctly before proceeding with deployment of RToWLAN wireless endpoints.

Related Topics

802.11 RToWLAN endpoints, on page 9
Cisco voice products

Cisco collaboration products
Cisco enterprise collaboration deployment design

802.11 RToWLAN endpoints

After you design and implement the enterprise WLAN infrastructure and collaboration applications and services, you must deploy the RToWLAN-capable devices and clients on top of this overall infrastructure.

Note Consider the RToWLAN endpoint selection during the WLAN infrastructure design and implementation phase, particularly during the site survey. If you design the WLAN infrastructure without consideration for the specific RToWLAN endpoints that will be deployed on this infrastructure, the result will be issues such as packet loss, excessive delay, and poor voice and video quality.

RToWLAN endpoints are categorized into two categories:

- Hardware-based wireless IP phones
- Software-based clients for wireless devices

Hardware-based wireless IP phones

The hardware-based wireless IP phones are purpose-built wireless IP voice and video phones that are designed specifically to provide voice and video calling functionality.

Hardware-based wireless IP phones fall into two subcategories:

- **Desktop WLAN Phones (or Fixed WLAN Phones):** IP desk phones connect to the network wirelessly but remain stationary because they are powered from a wall outlet. For example, Cisco Desktop Collaboration Experience DX650.
- **Mobile WLAN Phones:** Wireless IP phones are battery powered and are connected to the network wirelessly, which enables them to move throughout the enterprise while maintaining an active network connection. For example, Cisco Unified Wireless IP Phone 7925G.

Software-based clients for wireless devices

The software-based clients for wireless devices run on multifunction wireless devices that are capable of generating many types of traffic and performing many types of operations. The multifunction wireless device runs a collaboration software application that enables voice and video calling as well as other collaboration features.

Software-based clients running on wireless devices fall into two subcategories:

- Desktop computing platforms

  These devices connect to the network wirelessly, but depending on the platform, they may or may not remain stationary. Desktop computers rely on power from a wall outlet, while laptop computers are battery powered, and can therefore move around while maintaining an active wireless connection to the network. These devices typically run Microsoft Windows or Apple Mac operating systems, so the collaboration software client must support these operating systems.

  For example, Cisco Jabber for Windows.

- Mobile computing platforms

  Smartphones and tablets are examples of these types of devices. They are battery powered, and when wirelessly connected, they can move throughout the enterprise while actively maintaining connection to the network. These devices typically run Android or Apple iOS operating systems, so the collaboration software client must support these operating systems.

  For example, Cisco Jabber for Android.

Endpoint selection and WLAN site survey

You must understand the WLAN performance capabilities on the endpoints to design enough bandwidth into WLAN coverage areas for the users. Wireless endpoints and mobile client devices are available in different varieties, and not all wireless clients have the same capabilities.

Site surveys are one of the basic requirements when you deploy a WLAN, and you must always consider the Wi-Fi capabilities of the client devices or endpoints. Most smartphones and tablets support 802.11. However, generally, the smartphones and tablets have fewer antennas and lower data rates than laptops. In addition, most are not purpose-built for the enterprise WLAN market. Almost all smartphones and tablets support enterprise security policies. However, many of them do not support Wi-Fi protocols and features like 802.11e WMM for QoS and bandwidth control for audio and video calls. Consider these limitations before you start the survey process.

Smartphones and tablets generally have subpar access point to access point roaming logic. Most consumer or nonenterprise Wi-Fi endpoints perform poorly when they roam between access points. Client roaming can be unpredictable, and it is common for an endpoint without enterprise roaming logic to travel the same path repeatedly without repeating the same roam times in milliseconds or seconds. Nonenterprise Wi-Fi endpoints often repeatedly roam to the same access points in a high-density deployment rather than using other access points that may provide better throughput. It is important to test and understand the capabilities of the devices that are to be used in your facilities before you start the survey process.

Cisco WLAN controllers provide parameters to help nonenterprise clients roam. These parameters include minimum received signal strength indication (RSSI), hysteresis of decibels (dB), scan threshold in decibels per milliwatt (dBm), and transition time. The settings of these parameters need to be tested on-site with different mobile clients, because mobile clients behave differently.

Related Topics

Enterprise collaboration solution applications and services, on page 7
Real-Time Traffic over WLAN Radio Frequency Design
Cisco IP phones
Cisco Jabber

RToWLAN solution deployment considerations

This section describes important factors that you must consider when you design and implement an RToWLAN solution.

Hardware and software selection

When you select the hardware and software for an RToWLAN solution deployment, you must consider feature sets, standards and capabilities that are supported, and compatibility of the hardware and software. It is important to ensure that the selected wireless and collaboration infrastructure and the devices that are deployed

on that infrastructure deliver the required features and capabilities, whether you are selecting wireless LAN controllers and access points, collaboration platforms and applications, or the endpoint devices.

As a general rule, you should choose products that support a rich set of advanced network and application features, and at the same time, meet approved wireless and collaboration protocol standards to ensure interoperability and compatibility with a wide variety of systems. For example, when you choose wireless infrastructure components, consider full support for 802.11 wireless standards (802.11a, 802.11g, and the newer 802.11n and 802.11ac wireless access standards, as well as advanced wireless standards like 802.11e and 802.11r) as minimal requirements. Support for these standards ensures that necessary bandwidth with minimal delay and best effort treatment are provided for real-time traffic like voice and video.

When you design collaboration and communications infrastructure, a system that provides advanced capabilities (location and availability awareness, fixed mobile convergence, voice and video over IP, dual-mode device support, and so on) is needed to deliver the appropriate feature set that mobile workers require with RToWLAN deployments.

Voice and video over WLAN

It is critical that you plan and deploy a finely tuned, QoS-enabled, and highly available WLAN network to enable voice and video calling and other real-time traffic applications to ensure a successful RToWLAN solution deployment.

Because the 802.11 RToWLAN endpoints rely on the WLAN infrastructure for carrying both critical call signaling and real-time voice and video media traffic, you must deploy a WLAN network that is optimized for both data and real-time media traffic. A poorly deployed WLAN network results in a large amount of interference and diminished capacity, leading to poor RToWLAN application and service performance. In the case of voice and video calling, issues include not only poor call quality but in some cases dropped or missed calls. The poor application performance renders the WLAN deployment unusable for making and receiving calls or using other real-time applications.

Another basic requirement is that you must conduct a WLAN radio frequency (RF) site survey before, during, and after deploying an RToWLAN solution. This ensures that cell boundaries, configuration and feature settings, capacity, and redundancy are optimized to support RToWLAN applications and services. The site survey must verify that the WLAN RF design minimizes same-channel interference and also provides sufficient radio signal levels and nonadjacent channel overlap which helps to maintain acceptable real-time traffic throughput and voice and video quality as the RToWLAN endpoint device moves or roams from one location to another.

With appropriate site survey and careful planning, the wireless infrastructure conforms to the following collaboration and unified communications application minimum network requirements:

- Average IP packet loss for collaboration or other communications application traffic of less than or equal to one percent.
- Average end-to-end delay variation or jitter for collaboration or other communications application traffic of less than or equal to 30 ms.
- Average one-way packet delay for collaboration or other communications application traffic of less than or equal to 150 ms.

Note If you implement an RToWLAN network that is intended to carry voice or video traffic where the one-way delay exceeds 150 ms, it introduces issues not only with the quality of the voice and video calls but also with call setup and media cut-through times. These problems occur because several call signaling messages must be exchanged between each endpoint and the call control platform to establish the call.

While conducting a site survey and carefully planning an RToWLAN network ensures a successful deployment on the 2.4 GHz WLAN band (802.11b/g/n), Cisco recommends that you use the 5 GHz WLAN band (802.11a/n/ac) whenever possible for RToWLAN endpoint connectivity. 5 GHz WLANs enable higher density device deployments and provide better traffic throughput and less interference than 2.4 GHz WLANs. Higher density, higher throughput, and less interference are important network characteristics for RToWLAN applications and services, that include voice and video calling. In addition, with the prevalence of Bluetooth headsets and other Bluetooth peripherals, interference on enterprise 2.4 GHz WLANs is hard to avoid. When you use the 5 GHz band for RToWLAN deployments, Bluetooth interference is not a concern.

Note In dual-band WLANs (WLANs with both 2.4 GHz and 5 GHz bands), devices can roam between 802.11b/g/n and 802.11a/n with the same service set identifier (SSID), provided the RToWLAN endpoint is capable of supporting both bands. However, with some devices, a dual-band WLAN can cause gaps in the real-time traffic path. To avoid these gaps, use only one band for real-time traffic applications and services.

Quality of Service

One critical component for successful RToWLAN solution deployments is to implement Quality of Service (QoS) at the network and application layer. QoS ensures that different types of network traffic are given access to specific amounts of bandwidth or are given priority over other traffic as they traverse the network. You can use a variety of methods to provide different levels of network throughput and access based on traffic type.

For real-time traffic, QoS methods fall into the following two categories:

- Packet marking

  Packet marking determines how packets are queued as they ingress and egress network interfaces along the traffic path. Based on packet marking, certain types of traffic are allocated more or less bandwidth or can be transmitted more quickly and more often. Generally, when traversing the network, real-time media traffic is given priority treatment in all transmit queues along the network path. Real-time signaling traffic that is used to set up calls or facilitate application features is allocated dedicated bandwidth amounts based on the expected overhead of this signaling and other control plane traffic. Real-time signaling and other non-media traffic must never be assigned to priority traffic queues.

- Packet queuing

  Packet marking may or may not be performed at the application or endpoint level, but most IP networks are capable of marking or re-marking traffic flows as they traverse the network. Marking or re-marking of traffic flows by the network is usually based on IP port numbers or IP addresses. The client application or device performs the packet marking at the endpoint level based on specific application requirements or based on standardized marking guidelines (for example, voice media should be marked as Layer 2 802.11 WLAN User Priority 6, and Layer 3 IP packet marking should be Class of Service of 5, Differentiated Services Code Point of 0x46, or Per-Hop Behavior Expedited Forwarding).

802.11 WLAN packet marking at layer 2 (User Priority, or UP) presents challenges for many RToWLAN applications and endpoints. While some applications and endpoints do mark RToWLAN traffic flows at Layer 2 according to standard guidelines, many endpoint devices, particularly multifunction mobile devices, may not support Layer 2 802.11 UP marking. Unless endpoint devices are fully 802.11e and WMM compliant, and the operating system supports UP values as marked by applications, you cannot rely on Layer 2 QoS marking to provide improved RToWLAN traffic throughput on the wireless network.

Packet marking at Layer 3 is more common in RToWLAN applications and endpoints. Many applications and endpoints mark RToWLAN traffic flows at Layer 3. When the application and endpoints are marking traffic according to recommended guidelines, existing wired network QoS policy should not be modified, because real-time traffic automatically receives appropriate treatment based on standard QoS policy (priority treatment for voice and dedicated bandwidth for video and control plane traffic).

While correct packet marking is important, whether by application or endpoint, it is also important that you trust that the correct packet marking is applied to the correct type of traffic by the application or endpoint. If the packet marking of even some network traffic generated by an RToWLAN endpoint cannot be trusted, then administrators can decide to rely on network-based packet re-marking for all traffic. In this case, all traffic is re-marked according to enterprise policy based on traffic type (port number or protocol) and IP address to ensure that network priority queuing and dedicated bandwidth are applied to traffic flows. As a general rule, you must not trust the packet marking from RToWLAN endpoints unless the enterprise has complete control over the endpoints and the applications that are running on those devices. Besides re-marking packets for untrusted devices or applications, administrators can also enable network-based policing and rate limiting to ensure that untrusted devices or applications do not consume too much network bandwidth.

In some deployments, RToWLAN endpoints securely connect to the enterprise network to utilize RToWLAN applications and services. Because these connections traverse the Internet, there is no end-to-end QoS on the IP path. All packet marking is ignored and all traffic is treated as best effort. RToWLAN application performance cannot be guaranteed over these types of connections.

Security

When you deploy wireless endpoints, consider the security mechanisms that are used to control access to the network and to protect the network traffic. Wireless LAN infrastructure and RToWLAN endpoints support a wide range of authentication and encryption protocols, including WPA, WPA2, EAP-FAST, and PEAP. Generally, the authentication and encryption method that you choose for securing the wireless LAN should align with the IT security policies that are supported by both the WLAN infrastructure and the RToWLAN endpoint devices that you deploy.

An authentication and encryption method that supports fast rekeying such as Proactive Key Caching (PKC) or Cisco Centralized Key Management (CCKM) is important for real-time traffic solution deployments. It is critical because it ensures that active voice and video calls and other RToWLAN applications can maintain connectivity and operations as the RToWLAN endpoint is roaming from one access point in the network to another.

Another important security consideration is seamless attachment to the WLAN network. The endpoints must automatically attach to the WLAN network without user intervention to maximize the utilization of RToWLAN applications and services. Certificate-based identity and authentication facilitates an excellent user experience by eliminating user intervention (after initial provisioning) for network connection and minimizing authentication delay. However, deployments where enterprise security policy requires two-factor authentication or one-time passwords, user intervention is required for network attachment. In such cases, access to RToWLAN applications and services gets delayed.

Remote secure attachment

With appropriate security infrastructure and configuration in place, 802.11 RToWLAN endpoints are able to connect to the enterprise from remote locations using public or private 802.11 WLAN networks or Wi-Fi hot spots. While this securely enables RToWLAN application and service delivery for remote attached endpoints, you must consider whether to deliver RToWLAN applications and services over these types of remote connections.

The two key reasons that makes it problematic to enable RToWLAN applications and services over remote secure connections are as follows:

- Nonenterprise 802.11 WLAN

  Public and private 802.11 WLAN networks like wireless hot spots that are found at coffee shops and airports are typically not optimized for real-time traffic applications and do not deliver enterprise-class security or performance. Acceptable RToWLAN solution performance (voice and video quality, connection reliability, and so on) can never be guaranteed over nonenterprise class 802.11 WLANs.

- Internet traversal

  Because remote connections result in real-time traffic traversing the Internet between the enterprise and the endpoint, RToWLAN application performance, including voice and video quality, may be poor. Connectivity across the Internet is never guaranteed and always best effort. There is no end-to-end QoS on the IP path and all packet marking is ignored. All traffic is treated as best-effort. Acceptable RToWLAN solution performance can never be guaranteed over these Internet-based network connections.

Related Topics

Real-Time Traffic over WLAN Radio Frequency Design
Real-Time Traffic over WLAN Quality of Service
Real-time Traffic over WLAN Security
Real-time Traffic over WLAN Roaming

RToWLAN solution high availability

High availability is another important factor to consider while planning and deploying RToWLAN. Along with stringent network and radio frequency design requirements for successful deployments of real-time traffic applications and services, you must also consider redundancy and failover for WLAN infrastructure and real-time applications, services, and endpoints.

You must implement the wired network infrastructure in a redundant fashion so that the IP path from the network edge through the data centers and to all locations within the enterprise network infrastructure is maintained even in cases of hardware or service failure. With redundant physical network connections and appropriate network routing and switching configuration, hardwired RToWLAN components, such as call control platforms and other applications servers, are still able to communicate on the network even when components or portions of the network becomes unavailable.

The WLAN infrastructure must be deployed in a resilient manner to ensure continued network connectivity for endpoints even in scenarios where an access point, wireless LAN controller, or authentication system fails. By providing highly available network connectivity, real-time applications and services can continue to function despite isolated infrastructure outages.

Similarly, real-time traffic applications and services as well as the endpoints that service them must be highly available. In the case of real-time voice and video services as provided by Cisco call control, it is imperative that given the failure of a primary call control platform that other platforms or components can continue to

provide these services to endpoints and their users. In addition to network services redundancy, the endpoints and the real-time traffic applications that run on them must be able to automatically fail over to backup service nodes and remain operational.

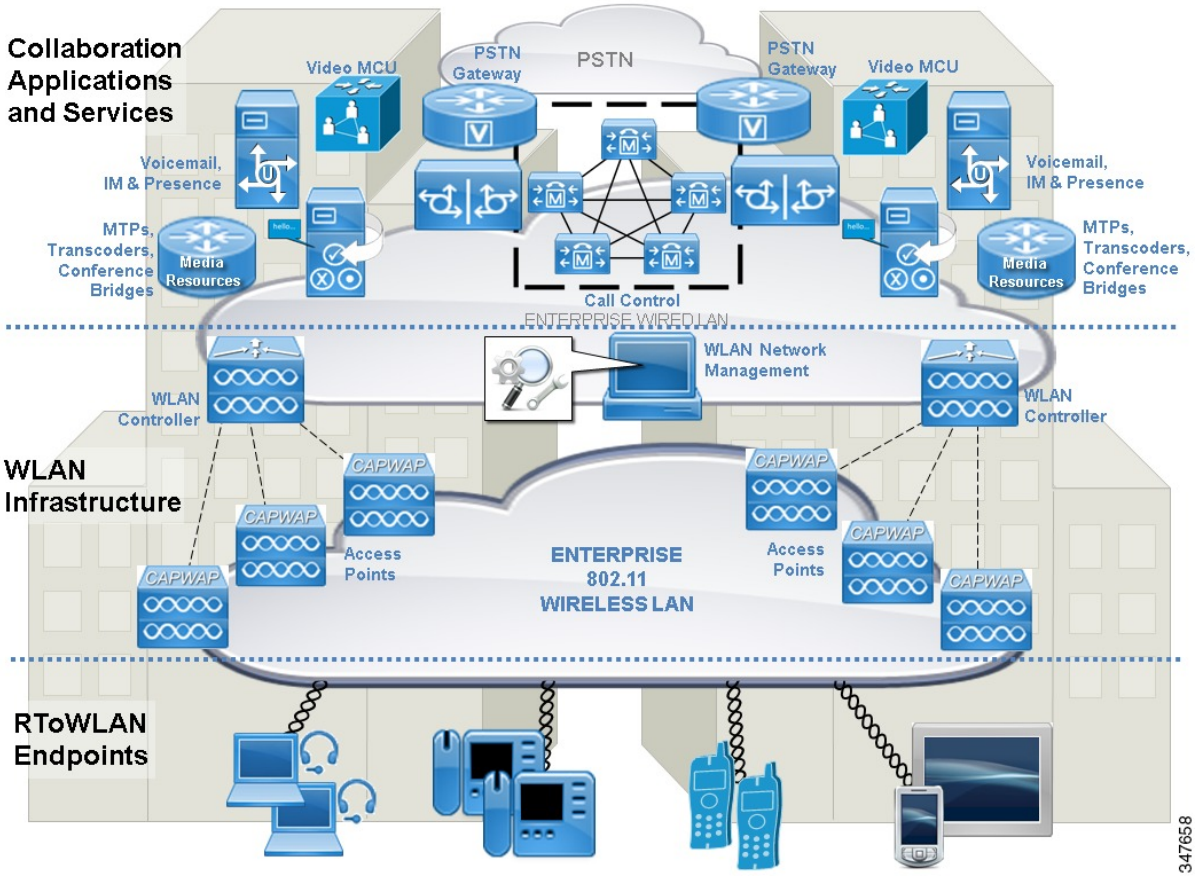
High availability considerations for RToWLAN solutions deployments, in some cases, dictates the physical characteristics of the enterprise network or deployment.

Single-site or campus RToWLAN deployment

In a single-site or campus deployment, the RToWLAN solution is implemented and operated within a single location or a group of locations within close proximity. The primary consideration for this deployment is to provide resiliency to network connectivity and RToWLAN services like voice and video calling.

Figure 3: RToWLAN single-site deployment, on page 15 shows a single-site or campus deployment that relies on duplication of key components and services to ensure high availability across the RToWLAN solution.

Figure 3: RToWLAN single-site deployment



Note The preceding figure does not show the wired network infrastructure redundancy but you must assume that it exists.

It also shows a split data center between two buildings in a campus location with duplication of all key components and services, which are as follows:

- Wireless network components: Multiple WLAN controllers and access points.

  Deploying redundant wireless network infrastructure components ensures that wireless network connectivity for RToWLAN endpoints is highly available. It also ensures that the devices can continually have access to network-based RToWLAN applications and services both when stationary and when moving or roaming within a location.

- Collaboration components: Multiple call control platforms or nodes, media resources (conference bridges, media control units, and so on), PSTN gateways or border controllers, and application servers.

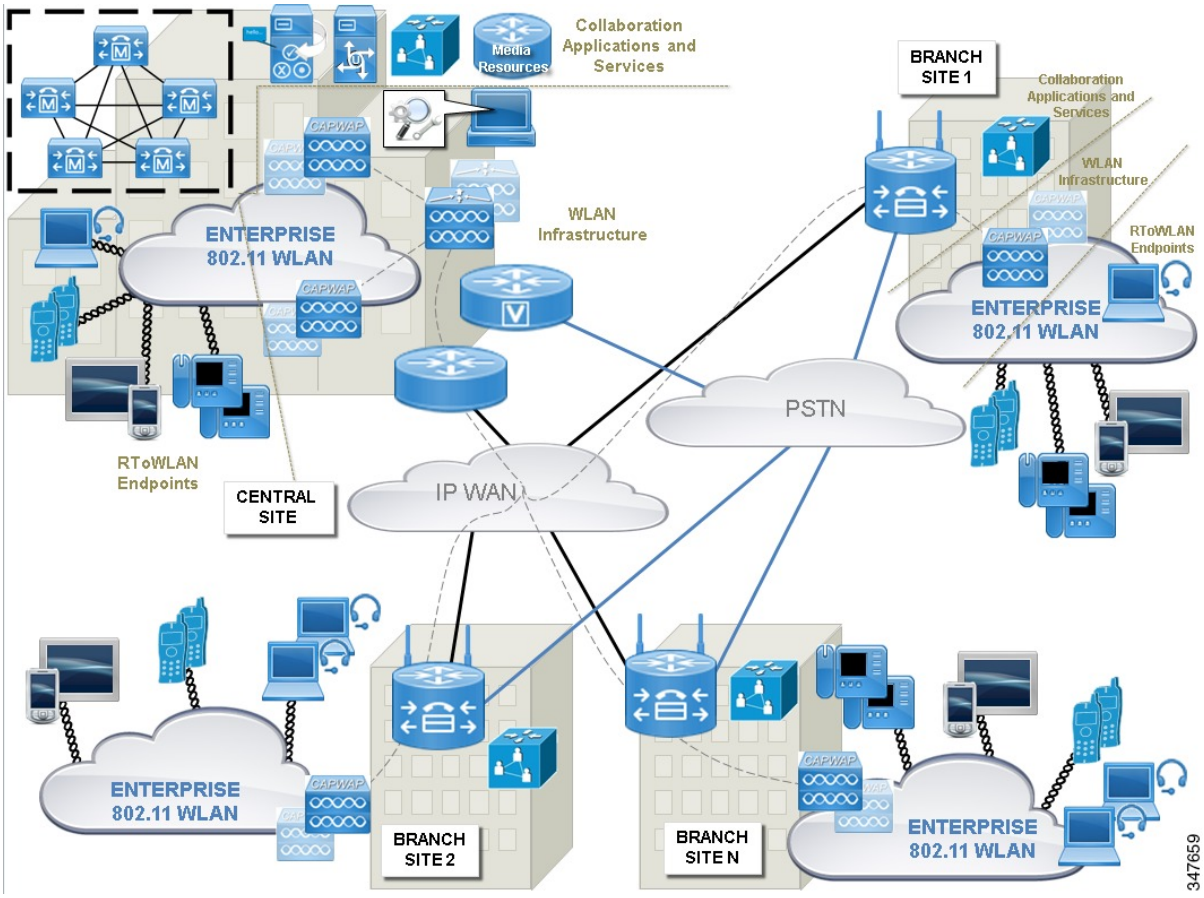
  Deploying redundant call control platforms, media resources, PSTN connections, and application servers ensures that RToWLAN applications and services are highly available and that RToWLAN endpoints can continually use these applications and services.

Distributed RToWLAN deployment

In a distributed deployment, the RToWLAN solution is implemented and operated at multiple sites or locations, and RToWLAN devices are distributed throughout the network. In these type of deployments, providing resiliency to network connectivity and RToWLAN services like voice and video calling is still the primary consideration. However, there are specific considerations apply for distributed deployments, related to site interconnectivity.

Figure 4: RToWLAN Distributed Deployment, on page 17shows that with distributed deployments, key WLAN and collaboration components and services must be replicated locally at each site to provide persistent network connectivity and persistent access to RToWLAN applications and services across the enterprise.

Figure 4: RToWLAN Distributed Deployment



Access points (APs) are deployed redundantly throughout the enterprise at each site based on density and site survey requirements. In the case of wireless LAN controllers (WLCs), you have two high availability deployment options:

- Central site WLCs control and manage APs at all locations providing centralized management and control.

  In the case of IP network failures between a branch and the central site, the local APs at the branch continue to service local RToWLAN endpoint devices, providing network connectivity and authentication services with cached credentials from the central site. This type of high availability scheme works best for smaller branch sites with a limited number of APs and wireless devices.

- Local WLCs deployed at each branch site control and manage APs at the local site.

  In the case of IP network failures between a branch and the central site, all WLAN network services continue to be provided locally. It is also possible to leverage centralized authentication services in this type of deployment, with the local site WLC caching credentials from the central site to provide local authentication services during IP network outages. This type of high availability is better suited for larger

branch sites with many APs and wireless devices. Even in the case of distributed or local WLCs, in most deployments, the overall WLAN network management component and application typically remain centralized as shown in Figure 4: RToWLAN Distributed Deployment, on page 17.

Note In deployments where branch sites vary in size or the required service level at each location differs, it is possible to have hybrid deployments, where some locations rely on centralized management and control of wireless APs and other locations rely on distributed or local control.

Figure 4: RToWLAN Distributed Deployment, on page 17 depicts both WLC high availability deployment options. The gray dashed lines between the central site WLC and all APs including the branch site APs represent centralized WLC control. Each branch site location router is capable of providing local WLC capabilities, as indicated by the wireless antennas.

Collaboration call control platforms and other components must also be replicated at each enterprise site to provide persistent access to RToWLAN applications and services. Figure 4: RToWLAN Distributed Deployment, on page 17 shows the replication of critical collaboration components including call control, PSTN connectivity, and media resources as represented by the voice enabled router and the media control unit (MCU) at each branch site. As with WLC high availability for distributed deployments, collaboration call control can also be centralized within the central site or distributed at all locations. Figure 4: RToWLAN Distributed Deployment, on page 17 depicts centralized call control with distributed backup call control provided at each branch site in the case of IP network failures between the branch and central site.

Another important consideration for RToWLAN deployments and distributed multisite deployments is RToWLAN device mobility. In a multisite deployment, movement between locations is common, because of the mobile nature of most RToWLAN endpoints. The collaboration call-control platform should dynamically track the location of RToWLAN endpoints as they move between enterprise sites. Based on the IP address of the device or other identifying information, the call control application should determine the devices location and adjust call routing, PSTN egress point, and codec and media resource selection as appropriate.

Another important consideration with distributed RToWLAN deployments is call admission control. Call admission control is a collaboration call control feature that ensures that bandwidth between enterprise sites is not oversubscribed by voice or video call traffic. Oversubscription of bandwidth on the connections between sites leads to poor voice and video quality, delayed call set up, and even dropped calls. Given the limited bandwidth and throughput that is available on links between enterprise sites which are usually lower speed, call admission control ensures that sufficient bandwidth is available on the IP path to setup and maintain a quality voice or video call. If sufficient bandwidth is not available, the call control system denies the call setup or reroutes the call using the local site PSTN connection. While call admission control is not unique to RToWLAN, it is an important consideration in distributed multisite collaboration deployments.

RToWLAN solution capacity planning

RToWLAN deployment scalability is a major design consideration when you implement real-time traffic applications and services. Failure to provide sufficient network and call processing capacity may result in service or functionality outages that prevent endpoints from associating, authenticating, registering, making or receiving voice and video calls, or leveraging other collaboration applications.

The WLAN infrastructure must provide sufficient client attachment as well as bandwidth capacity to ensure endpoints are able to actively connect to the WLAN and successfully make high-quality voice and video calls. In particular, the number of simultaneous voice or video bidirectional traffic streams per WLAN channel cell

is a critical capacity consideration, which, along with the number of associated endpoints, ultimately determines deployment device densities and potential user call rates.

Apart from WLAN infrastructure endpoint and bandwidth capacity, you must also consider the capacity of the collaboration system, which enables real-time traffic applications and services. With Cisco call control, each call control platform or node has a finite endpoint and call volume capacity. Likewise, media resource platforms and MCUs have finite call or session capacity. You must deploy sufficient endpoint and call volume capacity by adding the appropriate number of call control application nodes to provide services for the required number RToWLAN endpoint users.