Real-time Traffic over WLAN Security

The security of a wireless LAN (WLAN) system is always a critical consideration in every WLAN deployment. Control of the WLAN access depends on the principles of authentication, authorization, and accounting (AAA), augmented by encryption to ensure privacy. This chapter focuses on the authentication and encryption aspects of WLAN security for RToWLAN deployments.

For more information about WLAN security, see the *Enterprise Mobility Design Guide* at http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob73dg/emob73.html.

Real-Time Traffic over WLAN security overview

WLAN traffic is visible to any WLAN device within the radio frequency (RF) range of the WLAN infrastructure because the 802.11 wireless LANs is a shared network access medium.

The shared network access of WLANs creates the following challenges:

- How to provide privacy for users and devices of the WLAN from unauthorized users or devices.
- How to provide privacy for authorized users and devices of the WLAN from each other.
- How to provide privacy for multicast and broadcast WLAN traffic.
- How to differentiate between user and devices on the WLAN.

Each generation of WLAN security has addressed these challenges in different ways. But the key mechanisms are based on the same strategies that are used to secure communication over any untrusted medium—authentication and encryption.

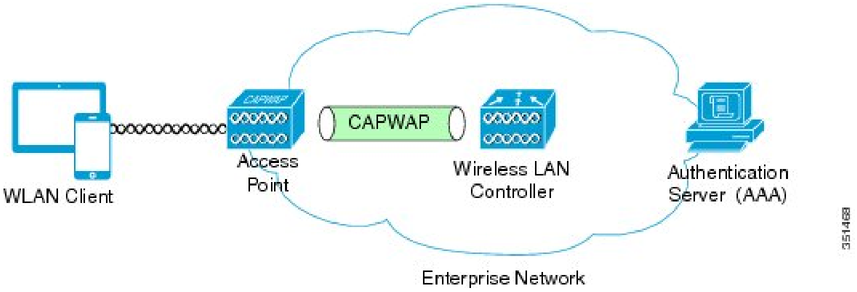
802.11 security schemes

There are several 802.11 security schemes that you can implement when you deploy a real-time traffic enabled WLAN. The type of security scheme or schemes that the network administrator uses depends on the capabilities and features that are supported by the WLAN network infrastructure and the specific RToWLAN client devices that will be deployed.

The following figure shows the basic components of WLAN security. The components that are required to implement secure network attachment and encrypted traffic for wireless network traversal include the following:

- Wireless client device
- Wireless access point (AP)
- Wireless LAN Controller (WLC)
- Authentication or AAA server

Figure 1: Secure Wireless LAN Topology



The best practice to deploy RToWLAN-capable client devices and RToWLAN services is that the security mechanisms that are enabled on the WLAN should provide user and device authentication and traffic encryption to ensure the following:

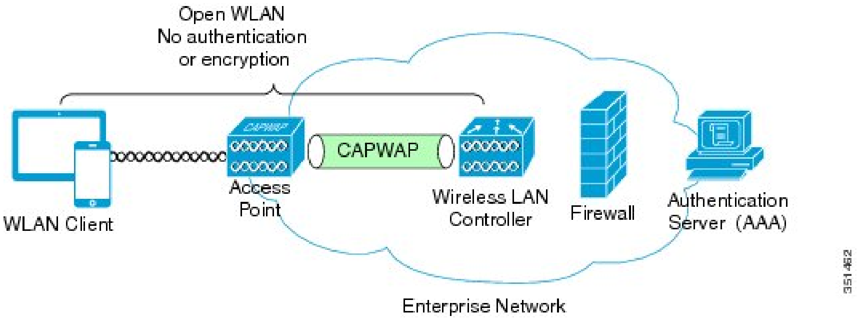
- Only authorized users and their devices are given access to the network.
- Real-time traffic flows are protected from interception and eavesdropping.

Open security scheme

An open security scheme provides no encryption or authentication for client device access to the WLAN.

The following figure shows an open WLAN security topology.

Figure 2: Open Wireless LAN Security Topology



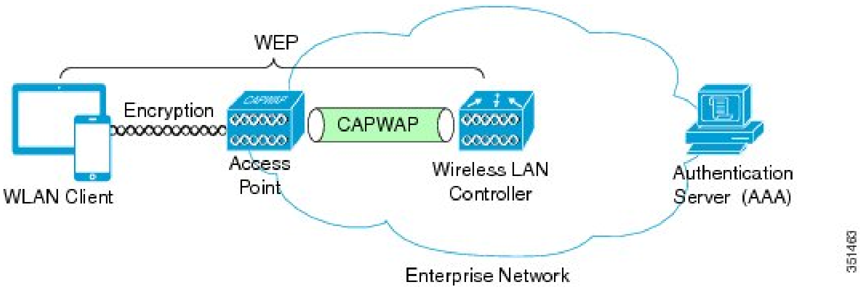
WLAN is open for attachment by all 802.11-capable devices. This security scheme is generally considered undesirable when deploying an enterprise WLAN, because the network is not protected from unauthorized access, and user and client traffic is not protected from interception and eavesdropping. However, despite the lack of encryption and authentication, open WLAN service set identifiers (SSIDs) are useful in some deployments when providing guest access for basic Internet connectivity or to onboard personal or noncorporate devices in bring-your-own-device (BYOD) scenarios.

In the case of BYOD deployments, the open network provides initial WLAN access for all clients and devices prior to identifying and onboarding authorized users and devices through additional network management and security services such that they have access to secured WLAN SSIDs or other areas of the enterprise network. You must take care to segment these open WLAN SSID networks from the rest of the secured enterprise network to prevent unauthorized access when you implement an open security scheme in these scenarios.

Wired Equivalent Privacy

A Wired Equivalent Privacy (WEP) security scheme provides encryption through a common shared key with minimal, if any, user or device authentication for client device access to the WLAN. The following figure shows a WEP security topology where WEP encryption occurs between the WLAN client device and the WLAN infrastructure AP and WLC.

Figure 3: WEP Wireless LAN Security Topology



The original 802.11 standard defined the WEP encryption mechanism but did not define an authentication mechanism. The level of authentication that was offered in the original 802.11 standard was at a group level that required everyone in the group to have the same static encryption key. This key was used to encrypt unicast, multicast, and broadcast traffic. WLAN security solutions further augmented this group authentication by authenticating the client MAC address. However, the solution of authenticating the client MAC address is not considered a significant improvement in security for the following reasons:

- It does not provide any additional per-user privacy, because the WEP key is still shared by all users.
- It is difficult to manage the WEP keys, because if one or multiple WEP keys need to be changed, you must update all the devices.
- It offers a weak level of authentication, because the 802.11 MAC addresses are sent unencrypted and the MAC address identifies the WLAN client devices rather than the users.
- It is difficult to administer MAC address authentication for large groups of users because you must maintain the database of the client device MAC addresses.

The original WEP encryption method with or without MAC address authentication that was implemented with the 802.11 standard were based on static configuration. While, the introduction of a dynamic WEP mechanism was an improvement over static WEP key implementations, issues in the WEP encryption mechanism means that the security of both static and dynamic WEP may be compromised. The issues of the WEP encryption mechanism itself is based on the fact that the WEP key can be derived by monitoring the client traffic.

Wi-Fi Protected Access

The weaknesses in WEP and the demand for a solution drove the Wi-Fi Alliance to develop WLAN security improvements through the 802.11i workgroup. These improvements are defined as Wi-Fi Protected Access (WPA). WPA addressed the main weakness in WEP encryption by replacing it with the Temporal Key Integrity Protocol (TKIP). While there are slight differences between WPA and the related sections of the 802.11i standard, these differences are transparent to users. The sections from the 802.11i standard that are used by WPA primarily address the need to secure the WLAN while maintaining sufficient backward compatibility with WEP to prevent the need to upgrade or replace currently deployed hardware. Because TKIP reuses the core encryption engine of WEP (RC4), it allows WPA to be implemented in the majority of systems through a software or firmware upgrade. WPA also attempts to address the absence of an authentication mechanism which was missing in the original WEP definition and further provides improvement over MAC address authentication that is sometimes used in combination with WEP.

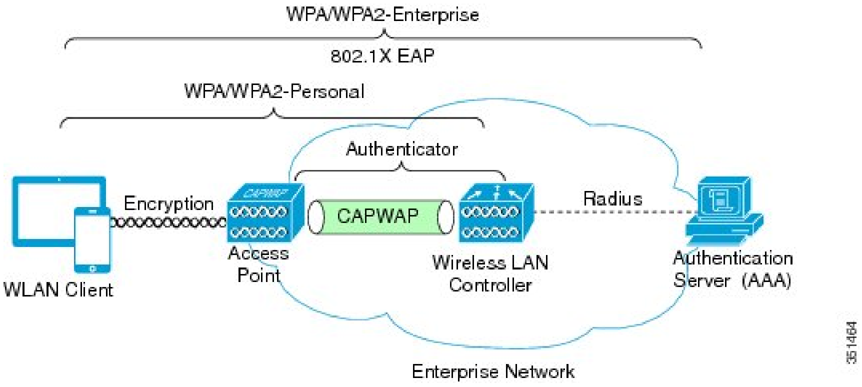
Wi-Fi Protected Access 2

The security features that were developed in WPA were based on the recommendations of the 802.11i workgroup that was tasked with replacing original security features that were defined in the 802.11 standard. While the security changes from 802.11i that were adopted by WPA are important, the key component in 802.11i standard was the incorporation of the Advanced Encryption Standard (AES) into WLAN security that aligns its encryption mechanism with the latest industry standard for encryption. The underlying mechanism of AES-Counter Mode CBC-MAC (AES-Counter Mode describes the encryption mechanism, and CBC-MAC describes frame protection mechanism) is very different to those of WPA and WEP, and generally requires hardware upgrades to be supported. WPA2 introduces support for AES. The hardware requirements that are required to support AES encryption in WPA2 mean that migration from WPA is almost always dependent on a hardware upgrade or replacement. In many cases, it is easier to update the network infrastructure than to update the WLAN client infrastructure, and a complete migration to WPA2 is dependent on a generational change in the WLAN client infrastructure. Also, when you consider whether to migrate from WPA to WPA2, keep in mind that currently there are no known serious security exposures in WPA.

WPA and WPA2: Enterprise and Personal

The following figure shows the two different security schemes that the WPA and WPA2 define, WPA/WPA2-Personal and WPA/WPA2-Enterprise.

Figure 4: WPA /WPA2 Wireless LAN Security Topology



- **WPA/WPA2-Personal:**

  WPA/WPA2-Personal uses the same cryptographic tools as WPA/WPA2-Enterprise but relies on a shared key to authenticate the WLAN clients. The shared key mechanism of authentication that is used in WPA-Personal does not provide a per-user or per-device authentication. Therefore, every device and every AP that is part of that WLAN SSID uses the same shared key. On the other hand, the key that is used for encryption is unique per user and per session because of randomizing during the initial four-way cryptographic handshake, but the shared key that is used to authenticate is the same for everyone. The primary advantage of WPA/WPA2-Personal in an RToWLAN deployment is that it does not require the use of an AAA server, and this can be an advantage in smaller deployments or multisite deployments with one or more branch sites that are separate from a central or larger regional site.

  Note When you rely on WPA/WPA2-Personal security scheme, make sure that you use strong keys, because tools are available that can successfully perform a dictionary attack on WPA/WPA2-Personal.

- **WPA/WPA2-Enterprise:**

  WPA/WPA2-Enterprise uses the same base WPA frame protection and cryptographic features as WPA/WPA2-Personal, but adds 802.1X with Extensible Authentication Protocol (EAP)-based authentication to the scheme. 802.1X with EAP-based authentication requires utilization of an AAA authentication server.

WPA/WPA2-Enterprise versus WPA/WPA2-Personal

Generally, the use of WPA/WPA2-Enterprise is preferred over WPA/WPA2-Personal for enterprise RToWLAN deployments. WPA/WPA2-Personal is generally targeted more for home-user or small-office deployments. Shared key security systems do not provide the authentication features that are typically required for the enterprise, and can introduce operational issues due to the overhead in updating the shared keys if an RToWLAN client device is lost, stolen, or is part of a regular key rotation regime.

The reward for successfully cracking, guessing, or stealing the shared key is very high, because this key is used for all users and devices. This does not mean that you can not use WPA/WPA2-Personal for RToWLAN deployments. You must balance the enterprise security requirement for an AAA authentication server against the RToWLAN handset requirements and characteristics of the RToWLAN deployment. Real-time traffic services and applications are usually expected to be highly available, and high availability may be difficult to achieve in branch and remote environments that are dependent on a centralized authentication system. You can address this issue by distributing authentication databases to branches through local AAA authentication servers or the embedded AAA services of a Wireless LAN Controller; or by deploying RToWLAN on a WLAN system leveraging WPA/WPA2-Personal, given the lack of dependency on centralized authentication.

Related Topics

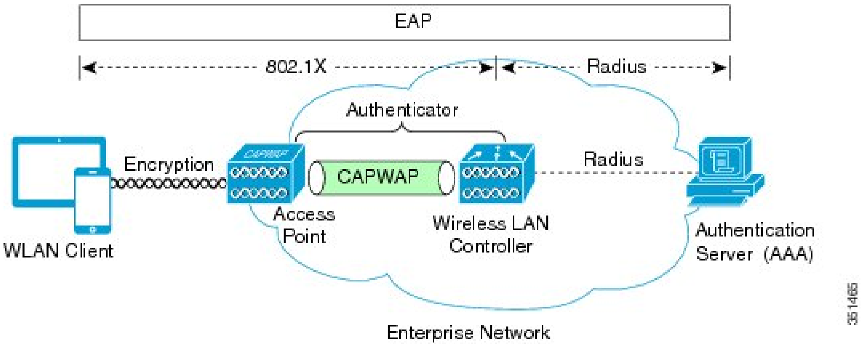
802.1X and Extensible Authentication Protocol, on page 6

802.11 encryption, on page 9

802.1X and Extensible Authentication Protocol

In order to provide enterprise-level WLAN security, 802.1X and Extensible Authentication Protocol (EAP) authentication mechanisms were implemented to provide mutual authentication of WLANs and WLAN client devices. The following figure shows the basic 802.1X and EAP authentication secure topology.

Figure 5: 802.1X and EAP Wireless LAN Security Topology



802.1X is an IEEE standard for port-based network access control and was adopted by the 802.11i security standard workgroup. The 802.1X standard provides authenticated access to 802.11 wireless LAN networks using the following logic:

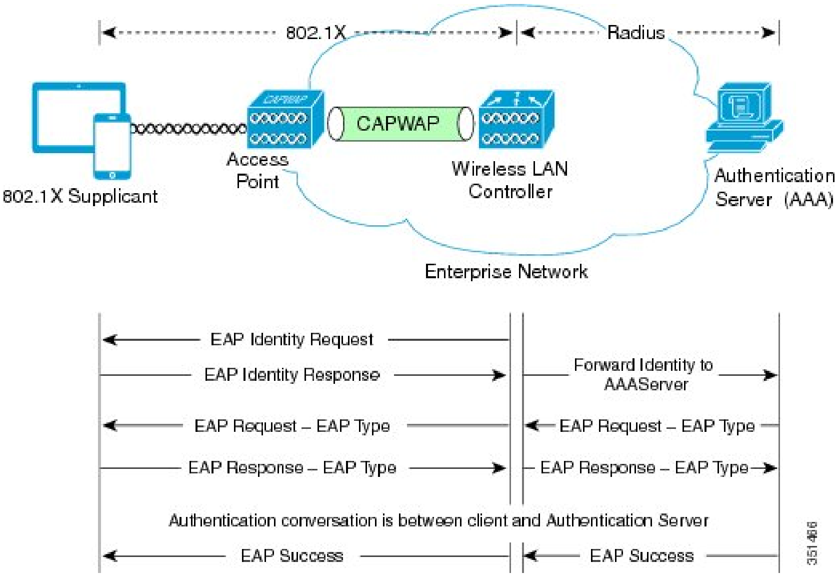
- A virtual port is created at the AP during the 802.11 association process for each WLAN client device.
- The AP then blocks all data frames on this virtual port except for 802.1X-based traffic.
- EAP authentication packets are carried in 802.1X traffic frames and are passed by the AP and Wireless LAN Controller to the AAA authentication server.
- Assuming EAP authentication is successful, the authentication server sends an EAP success message back to the Wireless LAN Controller and AP, which in turn pass the message on to the WLAN client device.
- The AP then allows data traffic (including voice and video) from the WLAN client device to flow through the virtual port.

- Before the virtual port opens to allow data traffic, data link encryption is established between the client device and the AP.

During the authentication process, a unique per-user per-session shared key is derived, and a portion of this key is used as a per-session encryption key.

The EAP authentication process supports a number of protocols, and which protocol is used ultimately depends on the capabilities of the WLAN client device supplicant and the WLAN infrastructure. Regardless of the EAP type that is used, all protocols generally behave as shown in the example EAP flow in the following figure.

Figure 6: EAP Protocol Flow



EAP as defined by RFC 3748 supports four packet types as part of the EAP authentication process:

- **EAP request:**

  The request packet that is sent by the authenticator (in the preceding figure, it is the Wireless LAN Controller and AP in combination) to the 802.1X supplicant (in the preceding figure, it is the WLAN client device). Each EAP request has a specific type that indicates what is being requested. In the example in the preceding figure, the first EAP request is for the WLAN client device identity, while the second EAP request is for the EAP type to be used for the authentication. A sequence number allows the authenticator and the peer to match an EAP response to each EAP request.

- **EAP response:**

  The response packet is sent by the WLAN client device to the AP and in turn to the Wireless LAN Controller, and uses a sequence number to match the initiating EAP request. In the case of an identity or type response, the response is forwarded by the Wireless LAN Controller to the authentication server.

- **EAP success:**

  Assuming that the WLAN client device or user has provided appropriate credentials during the authentication conversation, as shown in the preceding figure, the AAA server sends an EAP success packet to the Wireless LAN Controller, which in turn relays it through the AP to the WLAN client device.

- **EAP failure:**

  If the appropriate credentials are not provided at the WLAN client device or some other failure occurs, the AAA server sends an EAP failure packet to the Wireless LAN Controller, which relays it through the AP to the WLAN client device, resulting in failure of the authentication.

Common RToWLAN EAP supplicant types

This section describes the following common RToWLAN EAP supplicant types:

- EAP-FAST
- EAP-TLS
- PEAP

EAP-FAST

The EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) protocol was meant as a replacement for pre-802.11i Cisco proprietary Lightweight EAP (LEAP). LEAP was specifically designed to consider the limited processing power of application-specific or purpose-built devices, such as RToWLAN IP handsets. Given the security issues of LEAP, where weak passwords (less than ten characters) could be derived through analysis of the LEAP authentication transactions, EAP-FAST was designed to address these security issues while at the same time maintaining the “lightweight” nature of LEAP.

EAP-FAST is designed to provide the same tunneling protection as a tunneled authentication protocol such as EAP-Transport Layer Security (TLS), without requiring the Public Key Infrastructure (PKI) overhead associated with setting up the TLS tunnel that is used in EAP-TLS. Instead EAP-FAST typically relies on protected access credentials (PACs) for authenticating the tunnel between the client device and the authentication server. Although automatic PAC provisioning may be used, if the PAC is intercepted, it can be used to access user credentials. The use of manual PAC provisioning or optionally authentication server certificates during provisioning can help mitigate this potential issue.

As a tunneled protocol, EAP-FAST is capable of supporting multiple inner authentication mechanisms such as Microsoft Challenge-Handshake Authentication Protocol Version 2 (MSCHAPv2) or generic token card (GTC). The supported inner authentication mechanism depends on the RToWLAN client implementation.

EAP-TLS

The EAP-TLS protocol provides tunneled authentication protection relying on the PKI to authenticate both the WLAN client device and the WLAN network infrastructure. EAP-TLS uses certificates for both user and server authentication and for dynamic session key generation. It requires installation of both a client certificate and an authentication server certificate. EAP-TLS provides excellent security but requires client certificate management.

PEAP

Protected EAP (PEAP) uses TLS to protect authentication exchange between the WLAN client device and the authentication server. In the case of PEAP MSCHAPv2, MSCHAPv2 is used to encapsulate this authentication exchange across the tunnel. With PEAP GTC, a generic token card exchange protects the authentication process across the tunnel.

802.11 encryption

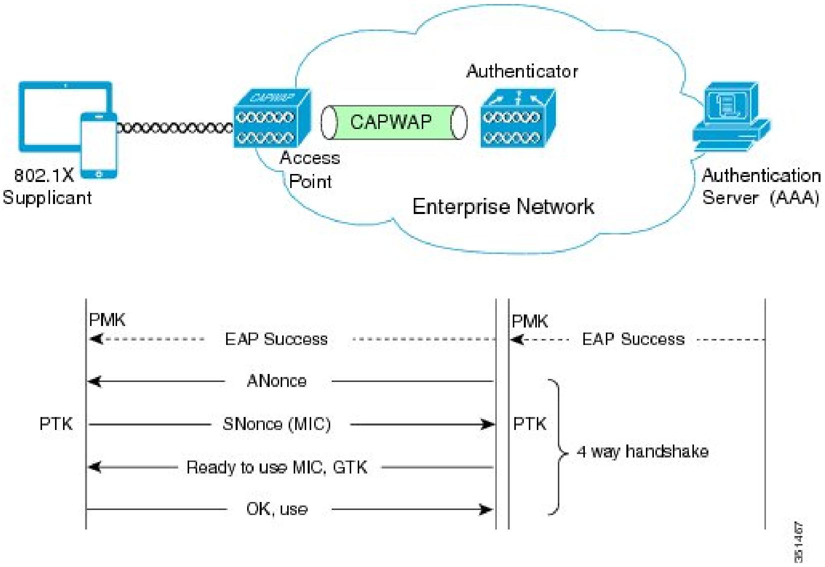
Encryption is a critical component of 802.11 WLAN security and is necessary for providing privacy over a local RF broadcast network. RToWLAN deployments should leverage TKIP or AES encryption as part of the WPA or WPA2 security mechanisms for securing network communication whenever WLAN client devices and infrastructure permit because of the superior security that these advanced mechanisms provide. WPA and WPA2 security mechanisms provide significant improvements over WEP encryption because of the encryption key derivation method.

The encryption key with WPA and WPA2 is derived using a four-way cryptographic handshake where the key shared between the WLAN client and the WLAN AP is not used directly for encryption, but instead used as the basis for the four-way handshake which derives the encryption key. This four-way handshake is used in both WPA/WPA2-Personal and WPA/WPA2-Enterprise.

The keys that are used for encryption are derived from the pair-wise master key (PMK) that has been mutually derived during the EAP authentication. This PMK is sent to the authenticator in the EAP success message, but is not forwarded to the supplicant because the supplicant has derived its own copy of the PMK.

The following figure shows the basic four-way handshake mechanism that is used in WPA/WPA2-Enterprise.

Figure 7: Four-Way Handshake for Deriving Wireless Encryption Keys with WPA/WPA-2 Enterprise



1. The authenticator sends an EAP over LAN (EAPOL)-Key frame that contains an authenticator nonce (ANonce), which is a random number that is generated by the authenticator.
   a. The supplicant generates a supplicant nonce (SNonce), which is a random number that is generated at the supplicant.
   b. The supplicant derives a pair-wise temporal key (PTK) from the ANonce and SNonce.
2. The supplicant sends an EAPOL-Key frame that contains the SNonce and a message integrity check (MIC).
3. The authenticator derives the PTK from the ANonce and SNonce and validates the MIC in the EAPOL-Key frame.

4 The authenticator sends an EAPOL-Key frame containing the group temporal key (GTK), the multicast, and the broadcast encryption keys if the validation is successful.

5 Upon validating the MIC from this frame, the supplicant installs its PTK and the GTK.

6 The supplicant sends an EAPOL-Key frame to confirm that the temporal keys are installed.

7 Upon validating the MIC from this frame, the authenticator installs the PTK for this client.

At this point, the supplicant and authenticator have verified that they both have a matching PMK, and both share the same PTK and GTK.

As shown in the preceding figure, with WPA/WPA2-Enterprise, the shared key that is used to generate the cryptographic key through the four-way handshake is derived during the 802.1X EAP authentication process. This EAP authentication process provides the AAA features that are missing in WPA/WPA2-Personal, allowing each user or device to be authenticated individually, a policy based on the authentication ID applied (authorization), and the collection of statistics based on authentication ID (accounting).

The difference between WPA/WPA2-Enterprise and the WPA/WPA2-Personal behavior is that the four-way handshake uses a shared key that is configured in the WLAN client device supplicant and the WLC. This shared key mechanism of authentication that is used in WPA-Personal does not provide a per-user or per-device authentication. Therefore, every device and every AP that is part of that WLAN SSID uses the same shared key. On the other hand, the key that is used for encryption, just as with WPA/WPA2-Enterprise, is unique per-user and per-session because of randomizing during the initial four-way cryptographic handshake.

Key caching and management

After an RToWLAN client device successfully authenticates with the WLAN network and establishes an encryption mechanism for traffic flows, it is able to securely send and receive traffic through the AP that it is associated with. However, what happens when the RToWLAN device moves or roams from one part of the WLAN network to another and must associate to another AP on the WLAN? In these situations, if the RToWLAN client device user is on an active voice or video call, it is important that the association of the client device to the new AP occurs as quickly as possible while at the same time maintaining implemented security authentication and encryption mechanisms. To facilitate this rapid reassociation and reauthentication, authentication and encryption keys must be managed and in some cases cached.

Related Topics

Real-time Traffic over WLAN Roaming

Additional 802.11 security mechanisms

RToWLAN network administrators should consider additional 802.11 WLAN security mechanisms to prevent unauthorized access or disruptive network attacks apart from secure client device WLAN association, authentication, and traffic encryption. For example, traditional wired network attack vectors such as MAC flooding, man-in-the-middle attacks, and DHCP snooping or starving should be mitigated with appropriate network management and wired and wireless LAN infrastructure security features. Likewise, wired and wireless intrusion prevention, detection, and mitigation are critical components for a successful RToWLAN deployment. In particular, the detection and mitigation or elimination of rogue access points and clients is critical to maintain healthy wireless LAN radio frequency deployments with minimal interference. Without rogue AP and client detection, proper radio frequency design can be compromised, resulting in poor wireless network throughput and capacity, unacceptable voice and video quality, and in some cases complete failure of real-time traffic applications and services.

Related Topics

Enterprise Mobility Design Guide

RToWLAN design considerations

An important aspect of the overall network design is to secure the wireless network for RToWLAN deployments. You must consider authentication and encryption method selection, scalability, and high availability aspects when you implement RToWLAN applications and services.

Authentication and encryption method selection

It is critical that you enable appropriate 802.11 security mechanisms for RToWLAN applications and services for a successful deployment. The most important considerations when you design a secure RToWLAN deployment are the capabilities of the WLAN infrastructure components such as access points, wireless LAN controllers, and the WLAN client devices themselves. Consider the following important factors:

- Always try to implement the strongest security mechanisms. WPA or WPA2-Enterprise security methods with 802.1X EAP authentication and TKIP or AES encryption is preferred over WEP or open authentication and encryption methods, provided the planned client devices and infrastructure are capable of supporting the stronger security methods. On the other hand, if the infrastructure or the target client devices do not support more secure mechanisms, then the network administrators must determine the most secure mechanism that can be supported based on the security policies and equipment standards of the organization.
- In the case of BYOD implementations where noncorporate-owned devices may be utilizing the WLAN infrastructure, it may be necessary to enable open authentication and nonencrypted connections to onboard these devices or simply to provide Internet-only guest access. In these cases, unsecure network access (at least initially) may be as critical as highly secure authentication and encryption methods.
- Another important consideration when selecting the security method or methods for an RToWLAN deployment is whether network attachment requires end-user intervention to complete the connection. The network administrator should strongly consider allowing voice and video-capable clients to attach to the enterprise network in the background (after initial provisioning), without user intervention. This ensures maximum utilization of the real-time traffic applications and services such as the enterprise voice and video telephony infrastructure. Specifically, the use of a certificate-based identity and authentication security mechanism like EAP-TLS helps facilitate an excellent user experience by minimizing network connection and authentication delay and ensuring quick WLAN device attachment. Failure to provide a fast, secure, and seamless network attachment mechanism for RToWLAN client devices may result in limited use of real-time traffic applications and services, because users delay or forget to intervene to complete the authentication process.
- Ultimately, the encryption and authentication methods that are used will be dictated by the client devices and the wireless infrastructure that will be deployed as well as the intended use cases for the RToWLAN deployment.

Scalability

While administrators generally prefer stronger security mechanisms, they must also consider the scalability of the security solution in terms of the number of users and the devices that will be deployed. In scenarios where large numbers of users or devices are deployed, it is important that the authentication servers or services are able to handle the authentication request load during the busiest times for wireless-client-device-network attachment.

For example, at the beginning of a work day, depending on the size of the deployment, the number of users who are attempting to connect their RToWLAN devices to the wireless network may exceed the authentication or credential database storage capacity of the authentication server. This results in failed or delayed authentication for at least some of the devices which can be problematic. In these situations, the administrators should seek to distribute authentication fulfillment and credential storage across multiple authentication servers. Ensure that sufficient capacity is available to handle the expected authentication load for successful RToWLAN deployments.

High availability

Another important aspect of securing RToWLAN deployments is to ensure that WLAN network security services are highly available. For example, in situations where an authentication server is required to secure the RToWLAN client device network attachment, it is important that the authentication server is available to authenticate the device when it attempts to connect. In the situation where the authentication server has failed or is not available due to a network issue, it is critical that a redundant authentication server is available to handle the authentication request.

Without highly available authentication services and server redundancy, RToWLAN client devices may not be able to connect to the WLAN network during a server failure. For example, in distributed network deployments with multiple sites where the authentication services for a branch location are provided through a centralized authentication server located in the central site, if there is a network failure between the branch location and the central site, the client devices that are located in the branch site will not be able to authenticate and connect to the WLAN unless a redundant authentication service is available at the local site or at another site that is reachable from the local site. Whenever possible, an RToWLAN deployment should be designed with highly available authentication services.