Wireless LAN Controller (WLC) - Design und Funktionen - Häufig gestellte Fragen

Inhalt

Einleitung

Dieses Dokument enthält Informationen zu den am häufigsten gestellten Fragen (FAQs) zum Design und den Funktionen eines Wireless LAN Controllers (WLC).

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Häufig gestellte Fragen zum Design

Frage: Wie konfiguriere ich den Switch für die Verbindung mit dem WLC?

A. Konfigurieren Sie den Switch-Port, mit dem der WLC verbunden ist, als IEEE 802.1Q-Trunk-Port. Stellen Sie sicher, dass nur die erforderlichen VLANs auf dem Switch zulässig sind. In der Regel werden das Management und die AP-Manager-Schnittstelle des WLC nicht markiert. Das bedeutet, dass sie das native VLAN des verbundenen Switches annehmen. Das ist nicht nötig. Sie können diesen Schnittstellen ein separates VLAN zuweisen. Weitere Informationen finden Sie im Abschnitt *Configure the Switch for the WLC (Switch für WLC konfigurieren)* unter Wireless LAN Controller and Lightweight Access Point Basic Configuration Example.

F. Tunnelt der gesamte Netzwerkverkehr von und zu einem WLAN-Client über einen Wireless LAN Controller (WLC), nachdem der Access Point (AP) beim Controller registriert wurde?

A. Wenn der WAP einem WLC beitritt, wird ein CAPWAP-Tunnel (Control and Provisioning of Wireless Access Points) zwischen den beiden Geräten gebildet. Der gesamte Datenverkehr, der den gesamten Client-Datenverkehr einschließt, wird über den CAPWAP-Tunnel gesendet.

Die einzige Ausnahme besteht darin, dass sich ein Access Point im Hybrid-REAP-Modus befindet. Die Hybrid-REAP-Zugangspunkte können den Client-Datenverkehr lokal schalten und eine Client-Authentifizierung lokal durchführen, wenn die Verbindung zum Controller unterbrochen wird. Wenn sie mit dem Controller verbunden sind, können sie auch Datenverkehr an diesen zurücksenden.

Frage: Kann ich Lightweight Access Points (LAPs) in einer Zweigstelle und einen Cisco Wireless LAN Controller (WLC) in meinem Hauptsitz installieren? Läuft LWAPP/CAPWAP über ein WAN?

Antwort: Ja, die WLCs können von den APs aus über das WAN verteilt werden. LWAPP/CAPWAP funktioniert über ein WAN, wenn die LAPs im Modus Remote Edge AP (REAP) oder Hybrid Remote Edge AP (H-REAP) konfiguriert sind. In beiden Modi kann der Access Point über einen Remote-Controller gesteuert werden, der über eine WAN-Verbindung verbunden ist. Der Datenverkehr wird lokal an die LAN-Verbindung überbrückt, sodass kein unnötiger lokaler Datenverkehr über die WAN-Verbindung gesendet werden muss. Dies ist einer der größten Vorteile von WLCs in Ihrem Wireless-Netzwerk.

Hinweis: Diese Modi werden nicht von allen Lightweight APs unterstützt. Der H-REAP-Modus wird beispielsweise nur in den LAPs 1131, 1140, 1242, 1250 und AP801 unterstützt. Der REAP-Modus wird nur auf dem 1030 AP unterstützt, der 1010- und der 1020-AP unterstützen REAP jedoch nicht. Bevor Sie diese Modi implementieren, überprüfen Sie, ob die LAPs diese unterstützen. Cisco IOS® Software-APs (autonome APs), die in LWAPP umgewandelt wurden, unterstützen REAP nicht.

F. Wie funktionieren die REAP- und H-REAP-Modi?

A. Im **REAP**-Modus wird der gesamte Steuerungs- und Verwaltungsverkehr, einschließlich des Authentifizierungsverkehrs, zurück an den WLC getunnelt. Der gesamte Datenverkehr wird jedoch lokal im LAN der Außenstelle weitergeleitet. Wenn die Verbindung zum WLC unterbrochen wird, werden alle WLANs mit Ausnahme des ersten WLAN (WLAN1) terminiert. Alle Clients, die derzeit diesem WLAN zugeordnet sind, werden beibehalten. Damit sich die neuen Clients innerhalb der Ausfallzeit erfolgreich authentifizieren und den Service auf diesem WLAN empfangen können, konfigurieren Sie die Authentifizierungsmethode für dieses WLAN entweder als WEP oder als WPA-PSK, sodass die Authentifizierung lokal am REAP erfolgt. Weitere Informationen zur REAP-Bereitstellung finden Sie im REAP-Bereitstellungsleitfaden in der Außenstelle.

Im **H-REAP-**Modus tunnelt ein Access Point den Steuerungs- und Verwaltungsdatenverkehr einschließlich des Authentifizierungsdatenverkehrs zurück zum WLC. Der Datenverkehr von einem WLAN wird lokal in der Außenstelle überbrückt, wenn das WLAN mit lokalem H-REAP-Switching konfiguriert ist, oder der Datenverkehr wird zurück an den WLC gesendet. Wenn die Verbindung zum WLC unterbrochen wird, werden alle WLANs mit Ausnahme der ersten acht WLANs terminiert, die mit lokalem H-REAP-Switching konfiguriert wurden. Alle Clients, die derzeit diesen WLANs zugeordnet sind, bleiben erhalten. Damit sich die neuen Clients innerhalb der Ausfallzeiten erfolgreich authentifizieren und den Service auf diesen WLANs empfangen können, konfigurieren Sie die Authentifizierungsmethode für dieses WLAN entweder als WEP, WPA PSK oder WPA2 PSK, sodass die Authentifizierung lokal bei H-REAP erfolgt.

Weitere Informationen zu H-REAP finden Sie im H-REAP Design and Deployment Guide.

Frage: Was ist der Unterschied zwischen Remote-Edge-AP (REAP) und Hybrid-REAP (H-REAP)?

A. REAP unterstützt kein IEEE 802.1Q VLAN Tagging. Daher werden mehrere VLANs nicht unterstützt. Der Datenverkehr aller Service Set Identifiers (SSIDs) endet im gleichen Subnetz, aber H-REAP unterstützt IEEE 802.1Q VLAN Tagging. Der Datenverkehr von jeder SSID kann in ein eindeutiges VLAN segmentiert werden.

Wenn die Verbindung zum WLC unterbrochen wird, d. h. im Standalone-Modus, dient REAP nur einem WLAN, d. h. dem ersten WLAN. Alle anderen WLANs sind deaktiviert. Bei H-REAP werden bis zu 8 WLANs innerhalb der Ausfallzeiten unterstützt.

Ein weiterer wesentlicher Unterschied besteht darin, dass Datenverkehr im REAP-Modus nur lokal überbrückt werden kann. Es kann nicht zurück zur Zentrale geschaltet werden, aber im H-REAP-Modus haben Sie die Möglichkeit, den Verkehr zurück zur Zentrale zu schalten. Der Datenverkehr von WLANs, die mit lokalem H-REAP-Switching konfiguriert sind, wird lokal geswitcht. Der Datenverkehr von anderen WLANs wird zurück zur Zentrale geleitet.

Weitere Informationen zu REAP finden Sie unter Konfigurationsbeispiel für einen Remote-Edge-Access Point (REAP) mit Lightweight Access Points und Wireless LAN Controllern (WLCs).

Weitere Informationen zu H-REAP finden Sie unter Configuring Hybrid REAP (Konfigurieren von Hybrid-REAP).

Frage: Wie viele WLANs werden auf dem WLC unterstützt?

A. Seit der Softwareversion 5.2.157.0 kann WLC bis zu 512 WLANs für Lightweight Access Points steuern. Jedes WLAN hat eine eigene WLAN-ID (1 bis 512), einen eigenen Profilnamen und eine WLAN-SSID und kann mit eindeutigen Sicherheitsrichtlinien versehen werden. Der Controller stellt bis zu 16 WLANs für jeden verbundenen Access Point zur Verfügung. Sie können jedoch bis zu 512 WLANs auf dem Controller erstellen und diese WLANs dann selektiv (unter Verwendung von Access Point-Gruppen) auf verschiedenen Access Points veröffentlichen, um das Wireless-Netzwerk besser zu verwalten.

Hinweis: Die Cisco Controller 2106, 2112 und 2125 unterstützen nur bis zu 16 WLANs.

Hinweis: Detaillierte Informationen zu den Richtlinien für die Konfiguration von WLANs auf WLCs finden Sie im Abschnitt Creating WLANs (Erstellen von WLANs) im Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0.

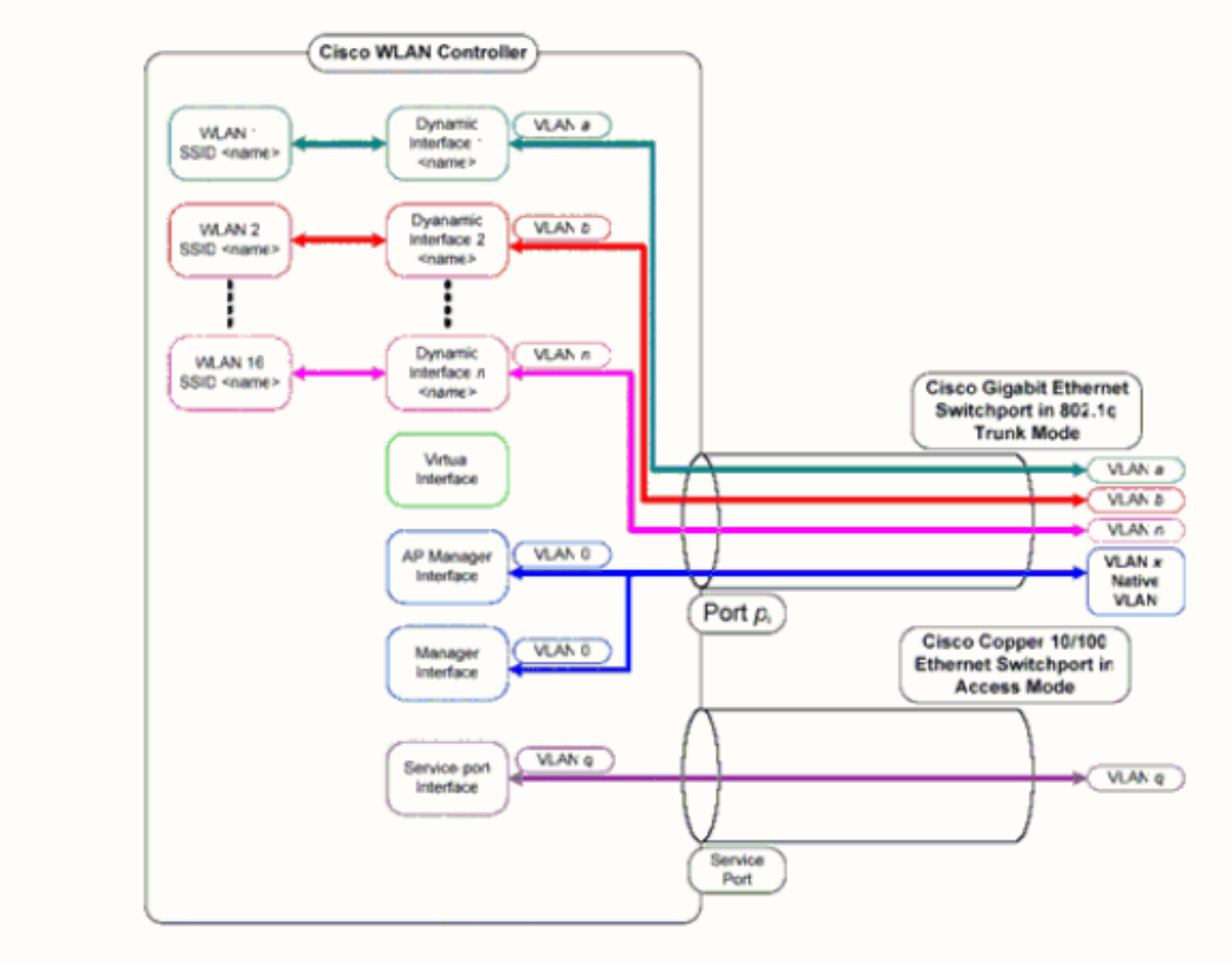
Frage: Wie kann ich VLANs auf meinem Wireless LAN Controller (WLC) konfigurieren?

Antwort: Im WLC sind die VLANs mit einer Schnittstelle verknüpft, die in einem eindeutigen IP-Subnetz konfiguriert ist. Diese Schnittstelle ist einem WLAN zugeordnet. Die Clients, die diesem WLAN zugeordnet sind, gehören dann zum VLAN der Schnittstelle und erhalten eine IP-Adresse aus dem Subnetz, zu dem die Schnittstelle gehört. Um VLANs auf dem WLC zu konfigurieren, führen Sie das Verfahren im Konfigurationsbeispiel VLANs auf Wireless LAN-Controllern aus.

Frage: Wir haben zwei WLANs mit zwei verschiedenen dynamischen Schnittstellen bereitgestellt. Jede Schnittstelle verfügt über ein eigenes VLAN, das sich vom VLAN der Management-Schnittstelle unterscheidet. Dies scheint zu funktionieren, aber wir haben die Trunk-Ports nicht bereitgestellt, um die von unseren WLANs verwendeten VLANs zuzulassen. Kennzeichnet der Access Point (AP) die Pakete mit dem Management-Schnittstellen-VLAN?

A. Der WAP kennzeichnet Pakete nicht mit der Verwaltungsschnittstelle VLAN. Der WAP kapselt die Pakete der Clients in das LWAPP/CAPWAP-Protokoll (Lightweight AP Protocol) ein und leitet

sie dann an den WLC weiter. Der WLC entfernt dann den LWAPP/CAPWAP-Header und leitet die Pakete mit dem entsprechenden VLAN-Tag an das Gateway weiter. Der VLAN-Tag hängt vom WLAN ab, zu dem der Client gehört. Der WLC hängt vom Gateway ab, das die Pakete an ihr Ziel weiterleitet. Um Datenverkehr für mehrere VLANs weiterleiten zu können, müssen Sie den Uplink-Switch als Trunk-Port konfigurieren. In diesem Diagramm wird die Funktionsweise von VLANs mit Controllern erläutert:



Frage: Welche IP-Adresse des WLC wird für die Authentifizierung beim AAA-Server verwendet?

A. Der WLC verwendet die IP-Adresse der Management-Schnittstelle für jeden Authentifizierungsmechanismus (Layer 2 oder Layer 3), der einen AAA-Server umfasst. Weitere Informationen zu Ports und Schnittstellen auf dem WLC finden Sie im Abschnitt *Configuring Ports and Interfaces (Konfigurieren von Ports und Schnittstellen) im* Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0.

Frage: Ich habe zehn Cisco Lightweight Access Points (LAPs) der Serie 1000 und zwei Wireless LAN Controller (WLCs) im selben VLAN. Wie kann ich sechs LAPs für die Verbindung mit dem WLC1 und die anderen vier LAPs für die Verbindung mit dem WLC2 registrieren?

Antwort: LWAPP/CAPWAP ermöglicht dynamische Redundanz und Lastenausgleich. Wenn Sie

beispielsweise mehr als eine IP-Adresse für Option 43 angeben, sendet ein LAP LWAPP/CAPWAP-Erkennungsanforderungen an jede der IP-Adressen, die der WAP empfängt. In die WLC-LWAPP/CAPWAP-Erkennungsantwort bettet der WLC folgende Informationen ein:

- Informationen zur aktuellen LAP-Last, definiert als die Anzahl der LAPs, die zum jeweiligen Zeitpunkt mit dem WLC verbunden sind
- Die LAP-Kapazität
- Die Anzahl der mit dem WLC verbundenen Wireless Clients

Der LAP versucht dann, dem am wenigsten ausgelasteten WLC beizutreten, dem WLC mit der größten verfügbaren LAP-Kapazität. Wenn ein LAP einem WLC beitritt, ermittelt er darüber hinaus die IP-Adressen der anderen WLCs in der Mobilitätsgruppe von seinem verbundenen WLC.

Sobald ein LAP einem WLC beitritt, können Sie ihn im Rahmen des nächsten Neustarts dazu bringen, einem bestimmten WLC beizutreten. Hierzu weisen Sie einem LAP einen primären, sekundären und tertiären WLC zu. Beim Neustart des LAP wird nach dem primären WLC gesucht, der unabhängig von der Last auf dem WLC diesem beitritt. Wenn der primäre WLC nicht antwortet, sucht er nach dem sekundären und, falls keine Antwort erfolgt, nach dem tertiären WLC. Weitere Informationen zur Konfiguration des primären WLC für eine LAP finden Sie im Abschnitt *Weisen Sie primäre, sekundäre und tertiäre Controller für den Lightweight Access Point* im Konfigurationsbeispiel *WLAN Controller Failover for Lightweight Access Points (WLAN-Controller-Failover für Lightweight Access Points) zu*.

Frage: Welche Funktionen werden von den Wireless LAN Controllern (WLCs) der Serie 2100 nicht unterstützt?

A. Diese Hardwarefunktionen werden von den Controllern der Serie 2100 nicht unterstützt:

- Service-Port (separate 10/100-Mbit/s-Ethernet-Schnittstelle für Out-of-Band-Management)

Die folgenden Softwarefunktionen werden von den Controllern der Serie 2100 nicht unterstützt:

- VPN-Terminierung (z. B. IPSec und L2TP)
- Terminierung von Gast-Controller-Tunneln (die Erstellung von Gast-Controller-Tunneln wird unterstützt)
- Liste der externen Webserver für Webauthentifizierung
- Layer-2-LWAPP
- Spanning Tree
- Port-Spiegelung
- Kranit
- Festung
- AppleTalk
- QoS-Bandbreitenverträge pro Benutzer
- IPv6-Passthrough
- Link Aggregation (LAG)
- Multicast-Unicast-Modus
- Kabelgebundener Gastzugriff

Frage: Welche Funktionen werden von den Controllern der Serie 5500 nicht unterstützt?

A. Diese Softwarefunktionen werden auf den Controllern der Serie 5500 nicht unterstützt:

- Statische AP-Manager-Schnittstelle**Hinweis:** Bei Controllern der Serie 5500 müssen Sie keine AP-Manager-Schnittstelle konfigurieren. Die Management-Schnittstelle agiert standardmäßig als AP-Manager-Schnittstelle, und die Access Points können über diese Schnittstelle verbunden werden.
- Asymmetrisches Mobility-Tunneling
- Spanning Tree Protocol (STP)
- Port-Spiegelung
- Unterstützung für Layer 2 Access Control List (ACL)
- VPN-Terminierung (z. B. IPSec und L2TP)
- VPN-Passthrough-Option
- Konfiguration von 802.3 Bridging, AppleTalk und Point-to-Point Protocol over Ethernet (PPPoE)

F. Welche Funktionen werden in Mesh-Netzwerken nicht unterstützt?

A. Diese Controller-Funktionen werden in Mesh-Netzwerken nicht unterstützt:

- Unterstützung mehrerer Länder
- Lastbasierte CAC (Mesh-Netzwerke unterstützen nur bandbreitenbasierte oder statische CACs)
- Hohe Verfügbarkeit (schneller Heartbeat- und primärer Erkennungs-Join-Timer)
- EAP-FASTv1- und 802.1X-Authentifizierung
- Verbindungspriorität des Access Points (Mesh-Access Points haben eine feste Priorität.)
- Lokal bedeutsames Zertifikat
- Standortbasierte Services

F. Wie lange sind die vom Hersteller installierten Zertifikate (MICs) auf einem Wireless LAN Controller und die Zertifikate der Lightweight APs gültig?

A. Die Gültigkeitsdauer eines MIC auf einem WLC beträgt 10 Jahre. Die gleiche Gültigkeitsdauer von 10 Jahren gilt für die Zertifikate des Lightweight AP ab Erstellung (ob es sich um ein MIC oder ein selbstsigniertes Zertifikat (SSC) handelt).

Frage: Ich habe zwei Wireless LAN Controller (WLCs) mit den Namen WLC1 und WLC2, die zur Ausfallsicherung in derselben Mobilitätsgruppe konfiguriert sind. Mein Lightweight Access Point (LAP) ist derzeit bei WLC1 registriert. Wenn WLC1 ausfällt, startet der für WLC1 registrierte AP während des Übergangs zum verbleibenden WLC (WLC2) neu? Verliert der WLAN-Client während dieses Failovers außerdem die WLAN-Verbindung mit der LAP?

A. Ja, die LAP hebt die Registrierung von WLC1 auf, startet neu und registriert sie dann erneut bei WLC2, wenn WLC1 ausfällt. Da die LAP neu startet, verlieren die zugehörigen WLAN-Clients die Verbindung zur neu startenden LAP. Weitere Informationen finden Sie unter AP Load Balancing und AP Fallback in Unified Wireless Networks.

Frage: Ist das Roaming vom LWAPP-Modus (Lightweight Access Point Protocol)

abhängig, für den der Wireless LAN Controller (WLC) konfiguriert ist? Kann ein WLC, der im Layer-2-LWAPP-Modus betrieben wird, ein Layer-3-Roaming durchführen?

A. Solange die Mobilitätsgruppierung auf den Controllern korrekt konfiguriert ist, sollte das Client-Roaming problemlos funktionieren. Das Roaming wird durch den LWAPP-Modus nicht beeinflusst (entweder Layer 2 oder Layer 3). Es wird jedoch empfohlen, soweit möglich Layer-3-LWAPP zu verwenden.

Hinweis: Der Layer-2-Modus wird nur von den Cisco WLCs der Serien 410x und 440x und den Cisco Access Points der Serie 1000 unterstützt. Layer-2-LWAPP wird von den anderen Wireless LAN-Controllern und Lightweight Access Point-Plattformen nicht unterstützt.

F. Welcher Roaming-Prozess wird durchgeführt, wenn ein Client beschließt, zu einem neuen Access Point (AP) oder Controller zu roamen?

A. Dies ist die Ereignissequenz, die auftritt, wenn ein Client zu einem neuen Access Point wechselt:

1. Der Client sendet über den LAP eine Neuzuordnungsanforderung an den WLC.
2. WLC sendet die Mobilitätsnachricht an andere WLCs in der Mobilitätsgruppe, um herauszufinden, mit welchem WLC der Client zuvor verbunden war.
3. Der ursprüngliche WLC antwortet mithilfe der Mobilitätsnachricht mit Informationen wie der MAC-Adresse, der IP-Adresse, der QoS, dem Sicherheitskontext usw. über den Client.
4. Der WLC aktualisiert seine Datenbank mit den bereitgestellten Client-Details; der Client durchläuft dann ggf. den Neuauthentifizierungsprozess. Die neue LAP, der der Client aktuell zugeordnet ist, wird zusammen mit weiteren Details in der Datenbank des WLC aktualisiert. Auf diese Weise wird die Client-IP-Adresse für Roaming zwischen WLCs beibehalten, was ein nahtloses Roaming ermöglicht.

Weitere Informationen zum Roaming in einer einheitlichen Umgebung finden Sie im Abschnitt *Configuring Mobility Groups (Konfigurieren von Mobilitätsgruppen) im* Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0.

Hinweis: Der Wireless-Client sendet während der Neuzuweisung keine Authentifizierungsanfrage (802.11). Der Wireless-Client sendet die Zuordnung einfach sofort aus. Anschließend erfolgt die 802.1x-Authentifizierung.

F. Welche Ports muss ich für die LWAPP/CAPWAP-Kommunikation zulassen, wenn im Netzwerk eine Firewall vorhanden ist?

A. Sie müssen diese Ports aktivieren:

- Aktivieren Sie diese UDP-Ports für LWAPP-Datenverkehr:Daten - 12222Steuerung - 12223
- Aktivieren Sie diese UDP-Ports für CAPWAP-Datenverkehr:Daten - 5247Steuerung - 5246
- Aktivieren Sie diese UDP-Ports für den Mobilitätsverkehr:16666 - Sicherer Modus16667 - Ungesicherter Modus

Mobility- und Datennachrichten werden in der Regel über EtherIP-Pakete ausgetauscht. **Das IP-Protokoll 97** muss auf der Firewall zugelassen werden, um EtherIP-Pakete zuzulassen. Wenn Sie **ESP** verwenden, um Mobilitätspakete zu kapseln, müssen Sie **ISAKMP** durch die Firewall

zulassen, wenn Sie den **UDP-Port 500** öffnen. Sie müssen auch das **IP-Protokoll 50** öffnen, damit die verschlüsselten Daten die Firewall passieren können.

Diese Ports sind optional (abhängig von Ihren Anforderungen):

- TCP 161 und 162 für SNMP (für das Wireless Control System [WCS])
- UDP 69 für TFTP
- TCP 80 und/oder 443 für HTTP oder HTTPS für GUI-Zugriff
- TCP 23 und/oder 22 für Telnet oder Secure Shell (SSH) für CLI-Zugriff

Frage: Unterstützen die Wireless LAN-Controller SSHv1 und SSHv2?

A. Wireless LAN-Controller unterstützen nur SSHv2.

Frage: Wird Reverse-ARP (RARP) von Wireless LAN-Controllern (WLCs) unterstützt?

A. Das Reverse Address Resolution Protocol (RARP) ist ein Link Layer-Protokoll, das zum Abrufen einer IP-Adresse für eine bestimmte Link Layer-Adresse, z. B. eine Ethernet-Adresse, verwendet wird. RARP wird von WLCs mit der Firmware-Version 4.0.217.0 oder höher unterstützt. RARP wird von keiner der früheren Versionen unterstützt.

Frage: Kann ich den internen DHCP-Server auf dem Wireless LAN Controller (WLC) verwenden, um den Lightweight Access Points (LAPs) IP-Adressen zuzuweisen?

A. Die Controller enthalten einen internen DHCP-Server. Dieser Server wird in der Regel in Zweigstellen verwendet, die noch nicht über einen DHCP-Server verfügen. Um auf den DHCP-Service zuzugreifen, klicken Sie in der WLC-GUI auf das Menü **Controller (Controller)** und anschließend links auf der Seite auf die Option **Internal DHCP Server (Interner DHCP-Server**). Weitere Informationen zur Konfiguration des DHCP-Bereichs auf dem WLC finden Sie im Abschnitt *Configuring DHCP (Konfigurieren* von *DHCP) im* Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0.

Der interne Server stellt DHCP-Adressen für Wireless-Clients, LAPs, Appliance-Mode-APs an der Management-Schnittstelle und DHCP-Anfragen bereit, die von LAPs weitergeleitet werden. WLCs bieten Geräten im Upstream des kabelgebundenen Netzwerks niemals Adressen an. Die DHCP-Option 43 wird auf dem internen Server nicht unterstützt. Daher muss der Access Point eine alternative Methode zum Auffinden der IP-Adresse der Verwaltungsschnittstelle des Controllers verwenden, z. B. lokale Subnetz-Broadcast-, DNS-, Priming- oder Over-the-Air-Erkennung.

Hinweis: WLC-Firmware-Versionen vor 4.0 unterstützen keinen DHCP-Service für LAPs, es sei denn, die LAPs sind direkt mit dem WLC verbunden. Die interne DHCP-Serverfunktion wurde nur verwendet, um Clients, die eine Verbindung zum Wireless LAN-Netzwerk herstellen, IP-Adressen zur Verfügung zu stellen.

F. Was bedeutet das Feld "DHCP erforderlich" unter einem WLAN?

A. DHCP erforderlich ist eine Option, die für ein WLAN aktiviert werden kann. Alle Clients, die mit diesem WLAN verbunden sind, müssen über DHCP IP-Adressen erhalten. Clients mit statischen

IP-Adressen dürfen keine Verbindung mit dem WLAN herstellen. Diese Option befindet sich auf der Registerkarte Advanced (Erweitert) eines WLAN. Der WLC lässt den Datenverkehr zu/von einem Client nur zu, wenn seine IP-Adresse in der MSCB-Tabelle des WLC vorhanden ist. WLC zeichnet die IP-Adresse eines Clients während seiner DHCP-Anfrage oder DHCP-Erneuerung auf. Dies erfordert, dass ein Client seine IP-Adresse bei jeder erneuten Zuordnung zum WLC erneuert, da der Eintrag jedes Mal aus der MSCB-Tabelle gelöscht wird, wenn der Client die Zuordnung als Teil des Roaming-Prozesses oder des Sitzungs-Timeouts aufhebt. Der Client muss sich erneut authentifizieren und dem WLC erneut zuordnen, der wiederum den Client-Eintrag in der Tabelle erstellt.

F. Wie funktioniert Cisco Centralized Key Management (CCKM) in einer LWAPP/CAPWAP-Umgebung?

A.: Während der ersten Client-Zuordnung handelt der WAP oder WLC einen paarweisen Master Key (PMK) aus, nachdem der WLAN-Client die 802.1x-Authentifizierung bestanden hat. Der WLC oder WDS AP speichert den PMK für jeden Client im Cache. Wenn ein Wireless-Client eine Zuweisung herstellt oder Roaming durchführt, wird die 802.1x-Authentifizierung übersprungen und der PMK sofort validiert.

Die einzige spezielle Implementierung des WLC im CCKM besteht darin, dass WLCs Client-PMK über Mobilitätspakete wie UDP 16666 austauschen.

Frage: Wie lege ich die Duplexeinstellungen für den Wireless LAN Controller (WLC) und die Lightweight Access Points (LAPs) fest?

A. Cisco Wireless-Produkte funktionieren am besten, wenn sowohl Geschwindigkeit als auch Duplex verhandelt werden, Sie können jedoch die Duplexeinstellungen für den WLC und die LAPs festlegen. Um die AP-Geschwindigkeits-/Duplexeinstellungen festzulegen, können Sie die Duplexeinstellungen für die LAPs auf dem Controller konfigurieren und diese dann an die LAPs weiterleiten.

configure ap ethernet duplex <auto/half/full> speed <auto/10/100/1000> <all/Cisco AP Name> ist der Befehl zum Festlegen der Duplexeinstellungen über die CLI. Dieser Befehl wird nur in Version 4.1 und höher unterstützt.

Um die Duplexeinstellungen für die physischen WLC-Schnittstellen festzulegen, verwenden Sie den physischen **Konfigurationsmodus des Ports {all | Port} {100h | 100 f | 10h | 10f}** Befehl.

Mit diesem Befehl werden die angegebenen oder alle 10/100BASE-T Ethernet-Ports an der Vorderseite für dedizierten Betrieb mit 10 Mbit/s oder 100 Mbit/s, Halbduplex oder Vollduplex festgelegt. Beachten Sie, dass Sie die Autoübertragung mit dem Befehl **config port autoneg disable** deaktivieren müssen, bevor Sie einen physischen Modus auf dem Port manuell konfigurieren. Beachten Sie außerdem, dass der Befehl **config port autoneg** die Einstellungen überschreibt, die mit dem Befehl **config port physicalmode** vorgenommen wurden. Standardmäßig sind alle Ports auf Auto-Negotiation eingestellt.

Hinweis: Es ist nicht möglich, die Geschwindigkeitseinstellungen an den Glasfaser-Ports zu ändern.

Frage: Gibt es eine Möglichkeit, den Namen des Lightweight Access Point (LAP) zu verfolgen, wenn dieser nicht beim Controller registriert ist?

A. Wenn Ihr Access Point vollständig ausgefallen und nicht für den Controller registriert ist, können Sie den LAP nicht über den Controller verfolgen. Die einzige verbleibende Möglichkeit besteht darin, auf den Switch zuzugreifen, an dem diese APs angeschlossen sind. Den Switch-Port, an dem sie angeschlossen sind, finden Sie mithilfe des folgenden Befehls:

```
show mac-address-table address
```

Daraus ergibt sich die Portnummer des Switches, mit dem dieser AP verbunden ist. Führen Sie dann den folgenden Befehl aus:

```
show cdp nei detail
```

Die Ausgabe dieses Befehls gibt auch den LAP-Namen an. Diese Methode ist jedoch nur möglich, wenn der Access Point hochgefahren und mit dem Switch verbunden ist.

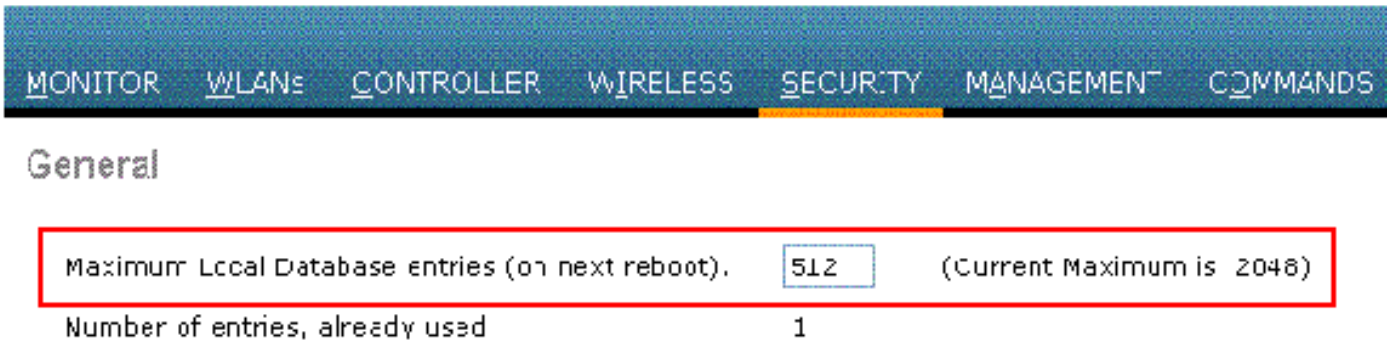
Frage: Ich habe für meinen Controller 512 Benutzer konfiguriert. Gibt es eine Möglichkeit, die Anzahl der Benutzer am Wireless LAN Controller (WLC) zu erhöhen?

A. Die lokale Benutzerdatenbank ist auf maximal 2048 Einträge auf der Seite **Sicherheit > Allgemein** beschränkt. Diese Datenbank wird von lokalen Managementbenutzern (einschließlich Lobby-Botschaftern), Netzbenutzern (einschließlich Gastbenutzern), MAC-Filtereinträgen, Einträgen in der Berechtigungsliste des Access Points und Einträgen in der Ausschlussliste gemeinsam genutzt. Zusammen genommen dürfen diese Benutzertypen die konfigurierte Datenbankgröße nicht überschreiten.

Verwenden Sie den folgenden CLI-Befehl, um die lokale Datenbank zu erweitern:

```
<Cisco Controller>config database size ?
<count>  Enter the maximum number of entries (512-2048)
```

Hinweis: Sie müssen die Konfiguration speichern und das System zurücksetzen (mit dem Befehl **reset system**), damit die Änderung wirksam wird.

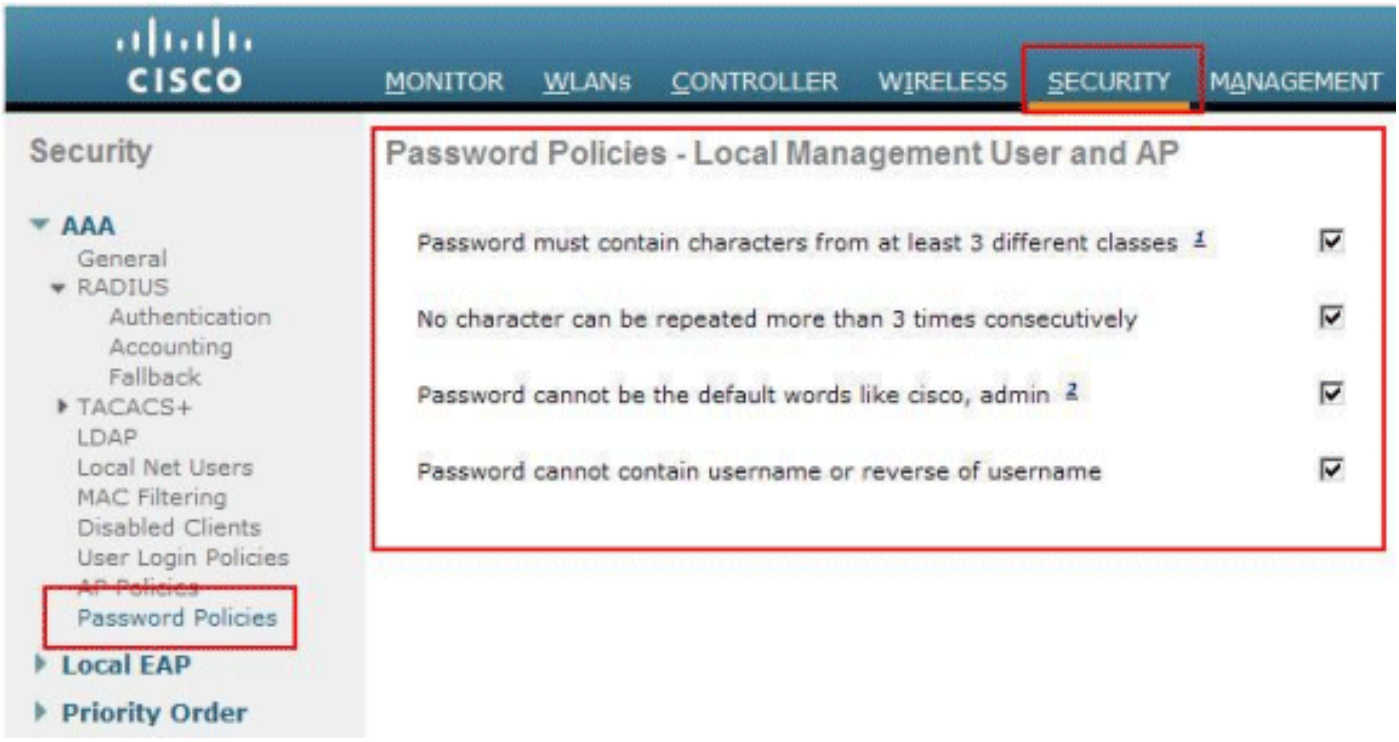


Frage: Wie kann ich eine Richtlinie für sichere Passwörter für WLCs durchsetzen?

A. Mit WLCs können Sie eine Richtlinie für sichere Kennwörter definieren. Dies kann entweder

über die CLI oder die GUI erfolgen.

Gehen Sie in der GUI zu **Security > AAA > Password Policies**. Diese Seite verfügt über eine Reihe von Optionen, die ausgewählt werden können, um ein sicheres Kennwort durchzusetzen. Hier ein Beispiel:



Verwenden Sie dazu die Befehlszeile von WLC: **config switchconfig strong-pwd** *{case-check | Konsekutivprüfung | Standardprüfung | Überprüfung des Benutzernamens | alle Prüfungen} {enable | disable}*-Befehl:

- **case-check**: Überprüft dreimal hintereinander das Auftreten desselben Zeichens.
- **konsekutives Prüfen** - Überprüft, ob die Standardwerte oder deren Varianten verwendet werden.
- **default-check** - Überprüft, ob entweder der Benutzername oder die Umkehrung verwendet wird.
- **all-checks** - Aktiviert/deaktiviert alle Prüfungen auf sichere Passwörter.

Frage: Wie wird die passive Client-Funktion auf Wireless LAN-Controllern verwendet?

A. Passive Clients sind Wireless-Geräte, z. B. Waagen und Drucker, für die eine statische IP-Adresse konfiguriert ist. Diese Clients übertragen keine IP-Informationen wie IP-Adresse, Subnetzmaske und Gateway-Informationen, wenn sie eine Verbindung zu einem Access Point herstellen. Wenn passive Clients verwendet werden, kennt der Controller die IP-Adresse daher nur, wenn er DHCP verwendet.

WLCs fungieren derzeit als Proxy für ARP-Anfragen. Nach Empfang einer ARP-Anforderung antwortet der Controller mit einer ARP-Antwort, anstatt die Anforderung direkt an den Client weiterzuleiten. Dieses Szenario hat zwei Vorteile:

- Das Upstream-Gerät, das die ARP-Anforderung an den Client sendet, weiß nicht, wo sich der Client befindet.
- Die Stromversorgung von batteriebetriebenen Geräten wie Mobiltelefonen und Druckern bleibt erhalten, da diese nicht auf alle ARP-Anfragen reagieren müssen.

Da der Wireless Controller keine IP-bezogenen Informationen über die passiven Clients besitzt, kann er nicht auf ARP-Anfragen reagieren. Das aktuelle Verhalten lässt keine Übertragung von ARP-Anforderungen an passive Clients zu. Jede Anwendung, die versucht, auf einen passiven Client zuzugreifen, schlägt fehl.

Die passive Client-Funktion ermöglicht den Austausch von ARP-Anfragen und -Antworten zwischen kabelgebundenen und Wireless-Clients. Wenn diese Funktion aktiviert ist, kann der Controller ARP-Anfragen von kabelgebundenen an Wireless-Clients weiterleiten, bis der gewünschte Wireless-Client den Status "RUN" erreicht.

Weitere Informationen zum Konfigurieren der passiven Client-Funktion finden Sie im Abschnitt Verwenden der grafischen Benutzeroberfläche zum Konfigurieren passiver Clients im Konfigurationshandbuch für Cisco Wireless LAN-Controller, Version 7.0.116.0.

Frage: Wie kann ich den Client so einrichten, dass er sich alle drei Minuten oder innerhalb eines bestimmten Zeitraums erneut beim RADIUS-Server authentifiziert?

A. Dazu kann der Sitzungs-Timeout-Parameter auf dem WLC verwendet werden. Standardmäßig wird der Sitzungs-Timeout-Parameter für 1800 Sekunden konfiguriert, bevor eine erneute Authentifizierung erfolgt.

Ändern Sie diesen Wert auf 180 Sekunden, damit sich der Client nach drei Minuten erneut authentifiziert.

Um auf den Sitzungs-Timeout-Parameter zuzugreifen, klicken Sie in der GUI auf das Menü **WLANs**. Es zeigt die Liste der im WLC konfigurierten WLANs an. Klicken Sie auf das WLAN, zu dem der Client gehört. Wechseln Sie zur Registerkarte **Erweitert**, und finden Sie den Parameter *Sitzungszeitüberschreitung aktivieren*. Ändern Sie den Standardwert in 180, und klicken Sie auf **Apply** (Anwenden), damit die Änderungen wirksam werden.

Wenn das Attribut "Session-Timeout" zusammen mit dem Wert "Termination-Action" von RADIUS-Request in einem Access-Accept gesendet wird, gibt es die maximale Anzahl an Sekunden an, die der Dienst vor der erneuten Authentifizierung bereitgestellt wird. In diesem Fall wird das Session-Timeout-Attribut verwendet, um die ReAuthPeriod-Konstante innerhalb des Reauthentication-Timer-Zustandscomputers von 802.1X zu laden.

Frage: Ich habe einen Gast-Tunneling-Ethernet-over-IP (EoIP)-Tunnel, der zwischen meinem Wireless LAN Controller (WLC) der Serie 4400, der als Anker-WLC fungiert, und mehreren Remote-WLCs konfiguriert ist. Kann der WLC Subnetz-Broadcasts durch den EoIP-Tunnel vom kabelgebundenen Netzwerk an Wireless-Clients weiterleiten, die den Remote-Controllern zugeordnet sind?

A. Nein, der WLC 4400 leitet IP-Subnetz-Broadcasts nicht über den EoIP-Tunnel von der kabelgebundenen Seite an die Wireless-Clients weiter. Diese Funktion wird nicht unterstützt. Cisco unterstützt kein Tunneling von Subnetz-Broadcast oder Multicast in der Gastzugriffstopologie. Da das Gast-WLAN den Client-Point of Presence zu einem sehr

spezifischen Ort im Netzwerk zwingt, meist außerhalb der Firewall, kann das Tunneling von Subnetz-Broadcast ein Sicherheitsproblem darstellen.

Frage: Welche Differentiated Services Code Point (DSCP)-Werte werden in einer Konfiguration mit Wireless LAN Controller (WLC) und LWAPP (Lightweight Access Point Protocol) für Sprachdatenverkehr übergeben? Wie wird QoS auf dem WLC implementiert?

A. Die WLANs der Cisco Unified Wireless Network (UWN)-Lösung unterstützen vier QoS-Ebenen:

- Platin/Sprache
- Gold/Video
- Silver/Best Effort (Standard)
- Bronze/Hintergrund

Sie können das Sprach-Datenverkehrs-WLAN so konfigurieren, dass es Platin-QoS verwendet, das WLAN mit niedriger Bandbreite so konfigurieren, dass es Bronze-QoS verwendet, und den gesamten anderen Datenverkehr zwischen den anderen QoS-Ebenen zuweisen. Weitere Informationen finden Sie unter Zuweisen eines QoS-Profils zu einem WLAN.

Frage: Werden Linksys Ethernet Bridges in einer Cisco Wireless Unified Solution unterstützt?

A. Nein, der WLC unterstützt nur Cisco WGB-Produkte. Linksys WGB werden nicht unterstützt. Obwohl die Cisco Wireless Unified Solution die Linksys WET54G- und WET11B-Ethernet-Bridges nicht unterstützt, können Sie diese Geräte in einer Konfiguration der Wireless Unified Solution verwenden, wenn Sie die folgenden Richtlinien verwenden:

- Schließen Sie nur ein Gerät an die WET54G oder WET11B an.
- Aktivieren Sie die MAC-Klonfunktion auf der WET54G oder WET11B, um das angeschlossene Gerät zu klonen.
- Installieren Sie die neuesten Treiber und Firmware auf Geräten, die mit der WET54G oder der WET11B verbunden sind. Diese Richtlinie ist besonders wichtig für JetDirect-Drucker, da frühere Firmware-Versionen Probleme mit DHCP verursachen.

Hinweis: Bridges anderer Anbieter werden nicht unterstützt. Die genannten Schritte können auch für andere Drittanbieter-Bridges ausprobiert werden.

Frage: Wie speichere ich die Konfigurationsdateien auf dem Wireless LAN Controller (WLC)?

A. Der WLC enthält zwei Arten von Speicher:

- Volatile RAM-Kapazität - Hält die aktuelle, aktive Controller-Konfiguration
- Nonvolatile RAM (NVRAM) (Nichtflüchtiger RAM (NVRAM)): Enthält die Neustartkonfiguration

Wenn Sie das Betriebssystem im WLC konfigurieren, ändern Sie den flüchtigen RAM. Sie müssen die Konfiguration aus dem flüchtigen RAM in den NVRAM speichern, um sicherzustellen, dass der WLC in der aktuellen Konfiguration neu gestartet wird.

Es ist wichtig zu wissen, welchen Speicher Sie bei der Durchführung dieser Aufgaben ändern:

- Verwenden des Konfigurationsassistenten
- Löschen Sie die Controller-Konfiguration.
- Speichern von Konfigurationen
- Setzen Sie den Controller zurück.
- Melden Sie sich von der CLI ab.

Funktionen - FAQ

Frage: Wie lege ich den EAP-Typ (Extensible Authentication Protocol) auf dem Wireless LAN Controller (WLC) fest? Ich möchte mich über eine ACS-Appliance (Access Control Server) authentifizieren und erhalte einen EAP-Typ, der nicht unterstützt wird.

Antwort: Der WLC verfügt über keine eigenen Einstellungen für den EAP-Typ. Für LEAP (Light EAP), EAP Flexible Authentication via Secure Tunneling (EAP-FAST) oder Microsoft Protected EAP (MS-PEAP) müssen Sie nur IEEE 802.1x oder Wi-Fi Protected Access (WPA) konfigurieren (wenn Sie 802.1x mit WPA verwenden). Jeder EAP-Typ, der vom RADIUS-Back-End und vom Client unterstützt wird, wird über das 802.1x-Tag unterstützt. Die EAP-Einstellung auf dem Client und dem RADIUS-Server muss übereinstimmen.

Gehen Sie wie folgt vor, um EAP über die Benutzeroberfläche des WLC zu aktivieren:

1. Klicken Sie in der WLC-GUI auf **WLANs**.
2. Eine Liste der im WLC konfigurierten WLANs wird angezeigt. Auf ein WLAN klicken.
3. Klicken Sie unter **WLANs > Edit** auf die Registerkarte **Security (Sicherheit)**.
4. Klicken Sie auf **Layer 2**, und wählen Sie Layer 2 Security als 802.1x oder WPA+WPA2 aus. Sie können auch die 802.1x-Parameter konfigurieren, die im gleichen Fenster verfügbar sind. Anschließend leitet der WLC EAP-Authentifizierungspakete zwischen dem Wireless-Client und dem Authentifizierungsserver weiter.
5. Klicken Sie auf die **AAA**-Server, und wählen Sie den Authentifizierungsserver aus dem Dropdown-Menü für dieses WLAN aus. Es wird davon ausgegangen, dass der Authentifizierungsserver bereits global konfiguriert ist. Weitere Informationen zum Aktivieren der EAP-Option auf WLCs über die Befehlszeilenschnittstelle (CLI) finden Sie im Abschnitt *Using the CLI to Configure RADIUS (Verwenden der CLI zum Konfigurieren von RADIUS)* im Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0.

F. Was ändert sich bei einer schnellen SSID?

A. Schnelles SSID-Ändern ermöglicht Clients, sich zwischen SSIDs zu bewegen. Wenn der Client eine neue Zuordnung für eine andere SSID sendet, wird der Client-Eintrag in der Controller-Verbindungstabelle gelöscht, bevor der Client der neuen SSID hinzugefügt wird. Wenn die schnelle SSID-Änderung deaktiviert ist, erzwingt der Controller eine Verzögerung, bevor Clients zum Wechsel zu einer neuen SSID berechtigt sind. Informationen zum Aktivieren von Fast SSID Changing finden Sie im Abschnitt *Configuring Fast SSID Changing* im Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0.

Frage: Kann ich die Anzahl der Clients, die eine Verbindung zu einem Wireless-LAN herstellen können, begrenzen?

A. Sie können die Anzahl der Clients, die eine Verbindung mit einem WLAN herstellen können, begrenzen. Dies ist in Szenarien nützlich, in denen eine begrenzte Anzahl von Clients eine Verbindung mit einem Controller herstellen können. Die Anzahl der Clients, die Sie pro WLAN konfigurieren können, hängt von der Plattform ab, die Sie verwenden.

Im Abschnitt Configuring the Maximum Number of Clients per WLAN des Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0 finden Sie Informationen zu den Client-Limits pro WLAN für die verschiedenen Plattformen von Wireless LAN Controllern.

F. Was ist PKC und wie funktioniert es mit dem Wireless LAN Controller (WLC)?

A. PKC steht für proaktives Schlüssel-Caching. Es wurde als Erweiterung des 802.11i IEEE-Standards entwickelt.

PKC ist eine Funktion, die in Cisco Controllern der Serien 2006/410x/440x aktiviert wurde. Sie ermöglicht ordnungsgemäß ausgestatteten Wireless-Clients das Roaming ohne vollständige Neuauthentifizierung mit einem AAA-Server. Um PKC zu verstehen, müssen Sie zunächst die Schlüsselzwischenspeicherung verstehen.

Die Schlüsselzwischenspeicherung ist eine Funktion, die WPA2 hinzugefügt wurde. Dadurch kann eine Mobilstation die Master-Schlüssel (Pairwise Master Key [PMK]) zwischenspeichern, die sie durch eine erfolgreiche Authentifizierung mit einem Access Point (AP) erhält, und **sie in einer zukünftigen Verbindung mit demselben AP wiederverwenden**. Das bedeutet, dass sich ein bestimmtes Mobilgerät einmal mit einem bestimmten WAP authentifizieren und den Schlüssel für die zukünftige Verwendung zwischenspeichern muss. Das Key-Caching wird über einen Mechanismus durchgeführt, der als PMK Identifier (PMKID) bezeichnet wird. Dabei handelt es sich um einen Hash des PMK, einen String, die Station und die MAC-Adressen des AP. Die PMKID identifiziert die PMK eindeutig.

Selbst bei der Schlüsselzwischenspeicherung muss sich eine Wireless-Station bei jedem AP authentifizieren, von dem sie den Dienst beziehen möchte. Dies führt zu erheblichen Latenzzeiten und Overheads, die den Handoff-Prozess verzögern und die Unterstützung von Echtzeitanwendungen beeinträchtigen können. Um dieses Problem zu beheben, wurde PKC mit WPA2 eingeführt.

Mit PKC kann eine Station einen PMK wiederverwenden, den sie zuvor durch einen erfolgreichen Authentifizierungsprozess erhalten hat. Dadurch muss sich die Station beim Roaming nicht mehr bei neuen APs authentifizieren.

Bei einem Intra-Controller-Roaming berechnet der Client daher beim Wechsel eines Mobilgeräts von einem WAP zu einem anderen auf demselben Controller eine PMKID unter Verwendung des zuvor verwendeten PMK neu und stellt diese während des Zuordnungsprozesses dar. Der WLC durchsucht seinen PMK-Cache, um festzustellen, ob ein solcher Eintrag vorhanden ist. Wenn dies der Fall ist, umgeht es den 802.1x-Authentifizierungsprozess und initiiert sofort den WPA2-Schlüsselaustausch. Ist dies nicht der Fall, wird der standardmäßige 802.1X-Authentifizierungsprozess durchlaufen.

PKC ist mit WPA2 standardmäßig aktiviert. Wenn Sie WPA2 als Layer-2-Sicherheit in der WLAN-Konfiguration des WLC aktivieren, ist PKC daher auf dem WLC aktiviert. Konfigurieren Sie außerdem den AAA-Server und den Wireless-Client für die entsprechende EAP-Authentifizierung.

Die clientseitige Komponente sollte auch WPA2 unterstützen, damit PKC funktioniert. PKC kann

auch in einer Inter-Controller-Roaming-Umgebung implementiert werden.

Hinweis: PKC funktioniert nicht mit dem Aironet Desktop Utility (ADU) als Client-Komponente.

Frage: Was sind die Erklärungen für diese Timeout-Einstellungen auf dem Controller: Address Resolution Protocol (ARP) Timeout, User Idle Timeout und Session Timeout?

A. Das **ARP-Timeout** wird verwendet, um ARP-Einträge auf dem WLC für die vom Netzwerk empfangenen Geräte zu löschen.

The **User Idle Timeout (Benutzerstillstand-Timeout)**: Wenn ein Benutzer ohne Kommunikation mit dem LAP für die als User Idle Timeout (Benutzerstillstand-Timeout) eingestellte Zeit inaktiv ist, wird der Client vom WLC deauthentifiziert. Der Client muss sich erneut authentifizieren und dem WLC erneut zuordnen. Er wird in Situationen verwendet, in denen ein Client die zugehörige LAP verlassen kann, ohne die LAP zu benachrichtigen. Dies kann passieren, wenn der Akku auf dem Client ausfällt oder sich die Mitarbeiter des Clients entfernen.

Hinweis: Um über die WLC-GUI auf ARP und User Idle Timeout (Zeitüberschreitung bei Inaktivität des Benutzers) zuzugreifen, wechseln Sie zum Menü **Controller (Controller**). Wählen Sie auf der linken Seite **Allgemein** aus, um nach den Feldern ARP und Timeout bei Inaktivität für Benutzer zu suchen.

Das Sitzungstimeout ist die maximale Zeit für eine Clientsitzung mit dem WLC. Danach wird der Client vom WLC deinstalliert, und der Client durchläuft erneut den gesamten Authentifizierungsprozess (Re-Authentifizierung). Dies ist Teil einer Sicherheitsvorkehrung zum Rotieren der Verschlüsselungsschlüssel. Wenn Sie eine Extensible Authentication Protocol (EAP)-Methode mit Schlüsselverwaltung verwenden, erfolgt die erneute Eingabe in jedem regelmäßigen Intervall, um einen neuen Verschlüsselungsschlüssel abzuleiten. Ohne Schlüsselverwaltung ist dieser Timeout-Wert der Zeitpunkt, zu dem Wireless-Clients eine vollständige Neuauthentifizierung durchführen müssen. Das Sitzungs-Timeout bezieht sich auf das WLAN. Auf diesen Parameter kann über das Menü **WLANs > Edit** zugegriffen werden.

F. Was ist ein RFID-System? Welche RFID-Tags werden derzeit von Cisco unterstützt?

A. Funkfrequenzkennzeichnung (Radio Frequency Identification, RFID) ist eine Technologie, die Funkfrequenzkommunikation für eine Kommunikation mit relativ kurzer Reichweite nutzt. Ein grundlegendes RFID-System besteht aus RFID-Tags, RFID-Lesegeräten und der Verarbeitungssoftware.

Derzeit unterstützt Cisco RFID-Tags von AeroScout und Pango. Weitere Informationen zum Konfigurieren von AeroScout-Tags finden Sie unter WLC Configuration for AeroScout RFID Tags.

Frage: Kann ich die EAP-Authentifizierung lokal auf dem WLC durchführen? Gibt es ein Dokument, das diese lokale EAP-Funktion erklärt?

Antwort: Ja, die EAP-Authentifizierung kann lokal auf dem WLC durchgeführt werden. Local EAP ist eine Authentifizierungsmethode, die es Benutzern und Wireless-Clients ermöglicht, sich lokal auf dem WLC zu authentifizieren. Es wurde für den Einsatz in Außenstellen entwickelt, die die Verbindung zu Wireless-Clients aufrechterhalten möchten, wenn das Backend-System ausfällt

oder der externe Authentifizierungsserver ausfällt. Wenn Sie lokalen EAP aktivieren, dient der WLC als Authentifizierungsserver. Weitere Informationen zur Konfiguration eines WLC für die lokale EAP-Fast-Authentifizierung finden Sie unter Lokale EAP-Authentifizierung auf dem Wireless LAN-Controller mit EAP-FAST und LDAP-Server-Konfigurationsbeispiel.

Frage: Was ist die WLAN-Änderungsfunktion? Wie konfiguriere ich diese Funktion? Werden die Werte für die WLAN-Außerkraftsetzung von den LAPs beibehalten, wenn ein Failover zum Backup-WLC erfolgt?

A.: Mithilfe der WLAN-Änderungsfunktion können wir WLANs aus den WLANs auswählen, die auf einem WLC konfiguriert sind und auf individueller LAP-Basis aktiv genutzt werden können. Gehen Sie wie folgt vor, um eine WLAN-Außerkraftsetzung zu konfigurieren:

1. Klicken Sie in der WLC-GUI auf das Menü **Wireless**.
2. Klicken Sie auf der linken Seite auf die Option **Radios,** und wählen Sie **802.11 a/n** oder **802.11 b/g/n aus**.
3. Klicken Sie im Dropdown-Menü rechts auf den Link **Configure (Konfigurieren)**, der dem Namen des Access Points entspricht, für den Sie die WLAN-Außerkraftsetzung konfigurieren möchten.
4. Wählen Sie im Dropdown-Menü "WLAN Override" die Option **Enable** aus. Das Menü WLAN Override (WLAN-Außerkraftsetzung) ist das letzte Element auf der linken Seite des Fensters.
5. Die Liste aller auf dem WLC konfigurierten WLANs wird angezeigt.
6. Aktivieren Sie in dieser Liste die **WLANs**, die auf der LAP angezeigt werden sollen, und klicken Sie auf **Apply (Anwenden)**, damit die Änderungen wirksam werden.
7. Speichern Sie Ihre Konfiguration, nachdem Sie diese Änderungen vorgenommen haben.

Die WAPs behalten die WLAN-Überschreibungswerte bei, wenn sie bei anderen WLCs registriert werden, vorausgesetzt, dass die WLAN-Profile und SSIDs, die Sie überschreiben möchten, für alle WLCs konfiguriert sind.

Hinweis: In der Controller-Software-Version 5.2.157.0 wurde die WLAN-Änderungsfunktion sowohl in der grafischen Benutzeroberfläche (GUI) als auch in der CLI des Controllers entfernt. Wenn der Controller für WLAN-Übersteuerung konfiguriert ist und Sie ein Upgrade auf die Controller-Software Version 5.2.157.0 durchführen, löscht der Controller die WLAN-Konfiguration und sendet alle WLANs. Sie können festlegen, dass nur bestimmte WLANs übertragen werden, wenn Sie Access Point-Gruppen konfigurieren. Jeder Access Point kündigt nur die aktivierten WLANs an, die zu seiner Access Point-Gruppe gehören.

Hinweis: Access Point-Gruppen ermöglichen nicht die Übertragung von WLANs über eine Funkschnittstelle des Access Point.

Frage: Wird IPv6 von den Cisco Wireless LAN Controllern (WLCs) und Lightweight Access Points (LAPs) unterstützt?

A. Derzeit unterstützen die Controller der Serien 4400 und 4100 nur IPv6-Client-Passthrough. Native IPv6-Unterstützung wird nicht unterstützt.

Um IPv6 auf dem WLC zu aktivieren, aktivieren Sie auf der Seite WLAN > Edit (WLAN > Bearbeiten) das Kontrollkästchen **IPv6 Enable (IPv6 aktivieren)** in der WLAN-SSID-Konfiguration.

Außerdem ist der Ethernet Multicast Mode (EMM) erforderlich, um IPv6 zu unterstützen. Wenn Sie

EMM deaktivieren, verlieren Client-Geräte, die IPv6 verwenden, die Verbindung. Um EMM zu aktivieren, gehen Sie zur Seite Controller > General (Controller > Allgemein), und wählen Sie im Dropdown-Menü Ethernet Multicast Mode (Ethernet-Multicast-Modus) die Option **Unicast** oder **Multicast aus**. Dadurch wird Multicast entweder im Unicast- oder im Multicast-Modus aktiviert. Wenn Multicast als Multicast-Unicast aktiviert ist, werden Pakete für jeden AP repliziert. Dies kann prozessorintensiv sein, verwenden Sie es daher mit Vorsicht. Multicast wird aktiviert, da Multicast die vom Benutzer zugewiesene Multicast-Adresse verwendet, um ein herkömmlicheres Multicast an die Access Points (APs) zu senden.

Hinweis: IPv6 wird von den 2006-Controllern nicht unterstützt.

Außerdem gibt es die Cisco Bug-ID CSCsg78176, die bei Verwendung der Funktion zum Überschreiben von AAA die Verwendung von IPv6-Passthrough verhindert.

Frage: Unterstützt der Cisco Wireless LAN Controller (WLC) der Serie 2000 die Web-Authentifizierung für Gastbenutzer?

A. Die Webauthentifizierung wird von allen Cisco WLCs unterstützt. Die Webauthentifizierung ist eine Layer-3-Authentifizierungsmethode, die verwendet wird, um Benutzer mit einfachen Authentifizierungsdaten zu authentifizieren. Es ist keine Verschlüsselung erforderlich. Gehen Sie wie folgt vor, um diese Funktion zu aktivieren:

1. Klicken Sie in der GUI auf das Menü **WLAN**.
2. Klicken Sie auf ein **WLAN**.
3. Wechseln Sie zur Registerkarte **Sicherheit**, und wählen Sie **Layer 3 aus**.
4. Aktivieren Sie das Kontrollkästchen **Webrichtlinie**, und wählen Sie **Authentifizierung aus**.
5. Klicken Sie auf **Apply**, um die Änderungen zu speichern.
6. Um eine Datenbank auf dem WLC zu erstellen, für die Benutzer authentifiziert werden sollen, gehen Sie zum Menü **Security (Sicherheit)** in der GUI, wählen Sie **Local Net User (Lokaler Net-Benutzer)** aus, und führen Sie die folgenden Aktionen aus: Definieren Sie den Gastbenutzernamen und das Passwort, das der Gast für die Anmeldung verwenden soll. Bei diesen Werten wird die Groß- und Kleinschreibung berücksichtigt.Wählen Sie die verwendete WLAN-ID aus.**Hinweis:** Ausführliche Informationen finden Sie im Konfigurationsbeispiel für die Web-Authentifizierung des Wireless LAN-Controllers.

Frage: Kann der WLC im Wireless-Modus verwaltet werden?

A. WLC kann nach der Aktivierung über den Wireless-Modus verwaltet werden. Weitere Informationen zum Aktivieren des Wireless-Modus finden Sie im Abschnitt *Enabling Wireless Connections to the GUI and CLI* des Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0.

Frage: Was ist Link Aggregation (LAG)? Wie aktiviere ich die LAG auf Wireless LAN-Controllern (WLCs)?

A.: Die LAG bündelt alle Ports am WLC in einer einzigen EtherChannel-Schnittstelle. Das System sorgt für ein dynamisches Management von Datenverkehrslastausgleich und Port-Redundanz mit der LAG.

Im Allgemeinen sind mit der Schnittstelle am WLC mehrere Parameter verknüpft, darunter die IP-

Adresse, das Standard-Gateway (für das IP-Subnetz), der primäre physische Port, der sekundäre physische Port, der VLAN-Tag und der DHCP-Server. Wenn die LAG nicht verwendet wird, wird jede Schnittstelle in der Regel einem physischen Port zugeordnet. Mehrere Schnittstellen können jedoch auch einem einzelnen WLC-Port zugeordnet werden. Bei Verwendung der LAG ordnet das System die Schnittstellen dynamisch dem aggregierten Port-Channel zu. Dies hilft bei der Port-Redundanz und beim Lastenausgleich. Beim Ausfall eines Ports wird die Schnittstelle dynamisch dem nächsten verfügbaren physischen Port zugeordnet, und die LAPs werden auf die Ports verteilt.

Wenn die LAG auf einem WLC aktiviert ist, leitet der WLC Daten-Frames auf demselben Port weiter, auf dem sie empfangen wurden. Der WLC nutzt den benachbarten Switch zum Lastenausgleich des Datenverkehrs über den EtherChannel. Der WLC führt keinen eigenen EtherChannel-Lastenausgleich durch.

Frage: Welche Modelle von Wireless LAN Controllern (WLCs) unterstützen Link Aggregation (LAG)?

A.: Die Cisco Controller der Serie 5500 unterstützen die LAG in Softwareversion 6.0 oder höher, die Cisco Controller der Serie 4400 unterstützen die LAG in Softwareversion 3.2 oder höher, und die LAG wird automatisch auf den Controllern im Cisco WiSM und im Catalyst 3750G Integrated Wireless LAN Controller Switch aktiviert. Ohne LAG unterstützt jeder Port des Verteilungssystems an einem Cisco Controller der Serie 4400 bis zu 48 Access Points. Bei aktivierter LAG unterstützt der logische Port eines Cisco 4402 Controllers bis zu 50 Access Points, der logische Port eines Cisco 4404 Controllers bis zu 100 Access Points und der logische Port des Catalyst 3750G Integrated Wireless LAN Controller Switch und jedes Cisco WiSM Controllers bis zu 150 Access Points.

Die Cisco WLCs 2106 und 2006 unterstützen die LAG nicht. Ältere Modelle wie der Cisco WLC der Serie 4000 unterstützen die LAG nicht.

Frage: Was ist die automatische Ankermobilitätsfunktion in Unified Wireless Networks?

A. Auto-Anker-Mobilität (oder Gast-WLAN-Mobilität) wird verwendet, um den Lastenausgleich und die Sicherheit für Roaming-Clients in Ihren WLANs (WLANs) zu verbessern. Unter normalen Roaming-Bedingungen werden Client-Geräte in ein WLAN eingebunden und dort mit dem ersten Controller verbunden, den sie kontaktieren. Wenn ein Client zu einem anderen Subnetz wechselt, richtet der Controller, zu dem der Client wechselt, eine Fremdsitzung für den Client mit dem Anker-Controller ein. Mithilfe der automatischen Ankermobilitätsfunktion können Sie einen Controller oder eine Gruppe von Controllern als Ankerpunkte für Clients in einem WLAN angeben.

Hinweis: Der Mobilitätsanker darf nicht für die Layer-3-Mobilität konfiguriert werden. Der Mobilitätsanker wird nur für das Gast-Tunneling verwendet.

Frage: Kann ein Cisco 2006 Wireless LAN Controller (WLC) als Anker für ein WLAN konfiguriert werden?

A.: Ein Cisco WLC der Serie 2000 kann nicht als Anker für ein WLAN festgelegt werden. Ein WLAN, das auf einem Cisco WLC der Serie 2000 erstellt wird, kann jedoch auf einem Cisco WLC der Serie 4100 und einem Cisco WLC der Serie 4400 aufbauen.

F. Welche Art von Mobility Tunneling verwendet der Wireless LAN Controller?

A. Die Controller-Software-Versionen 4.1 bis 5.1 unterstützen sowohl asymmetrisches als auch symmetrisches Mobility Tunneling. Die Controller-Software Version 5.2 oder höher unterstützt nur das symmetrische Mobility Tunneling, das jetzt standardmäßig immer aktiviert ist.

Beim asymmetrischen Tunneling wird der Client-Datenverkehr zum kabelgebundenen Netzwerk direkt über den Fremdcontroller geleitet. Das asymmetrische Tunneling wird unterbrochen, wenn bei einem Upstream-Router die RPF (Reverse Path Filtering) aktiviert ist. In diesem Fall wird der Client-Datenverkehr am Router verworfen, da die RPF-Prüfung sicherstellt, dass der Pfad zurück zur Quelladresse mit dem Pfad übereinstimmt, von dem das Paket stammt.

Wenn das symmetrische Mobility Tunneling aktiviert ist, wird der gesamte Client-Datenverkehr an den Anker-Controller gesendet und kann dann die RPF-Prüfung erfolgreich bestehen. Symmetrisches Mobility Tunneling ist auch in folgenden Situationen nützlich:

- Wenn bei einer Firewall-Installation im Client-Paketpfad Pakete verworfen werden, weil die Quell-IP-Adresse nicht mit dem Subnetz übereinstimmt, in dem die Pakete empfangen werden, ist dies nützlich.
- Wenn sich das Gruppen-VLAN des Access Points auf dem Anker-Controller von dem VLAN der WLAN-Schnittstelle des ausländischen Controllers unterscheidet: In diesem Fall kann während Mobilitätsereignissen Client-Datenverkehr über ein falsches VLAN gesendet werden.

Frage: Wie greifen wir auf den WLC zu, wenn das Netzwerk ausgefallen ist?

A. Wenn das Netzwerk ausgefallen ist, kann der Service-Port auf den WLC zugreifen. Diesem Port wird eine IP-Adresse in einem völlig anderen Subnetz als anderen Ports des WLC zugewiesen. Dies wird als Out-of-Band-Management bezeichnet. Weitere Informationen finden Sie im Abschnitt *Configuring Ports and Interfaces (Konfigurieren von Ports und Schnittstellen) im* Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0.

Frage: Unterstützen die Cisco Wireless LAN Controller (WLCs) die Failover- (oder Redundanzfunktion)?

A. Ja, wenn Sie zwei oder mehr WLCs in Ihrem WLAN-Netzwerk haben, können Sie diese für Redundanz konfigurieren. Im Allgemeinen wird eine LAP mit dem konfigurierten primären WLC verbunden. Wenn der primäre WLC ausfällt, wird der LAP neu gestartet und einem anderen WLC in der Mobilitätsgruppe hinzugefügt. Failover ist eine Funktion, bei der die LAP eine Abfrage nach dem primären WLC durchführt und sich in den primären WLC einwählt, sobald dieser funktionsfähig ist. Weitere Informationen finden Sie im Konfigurationsbeispiel zum WLAN-Controller-Failover für Lightweight Access Points.

Frage: Was nutzen Zugriffskontrolllisten (ACLs) vor der Authentifizierung in Wireless LAN Controllern (WLCs)?

A. Wie der Name schon sagt, können Sie mit einer Pre-Authentication-Zugriffskontrollliste den Client-Datenverkehr von und zu einer bestimmten IP-Adresse zulassen, noch bevor der Client sich authentifiziert. Wenn ein externer Webserver für die Webauthentifizierung verwendet wird, benötigen einige der WLC-Plattformen eine Pre-Authentication-ACL für den externen Webserver (Cisco Controller der Serie 5500, Cisco Controller der Serie 2100, Cisco Controller der Serie 2000

und das Controller-Netzwerkmodul). Für die anderen WLC-Plattformen ist die ACL vor der Authentifizierung nicht obligatorisch. Es empfiehlt sich jedoch, eine Pre-Authentication-ACL für den externen Webserver zu konfigurieren, wenn externe Web-Authentifizierung verwendet wird.

Frage: Ich habe ein MAC-gefiltertes WLAN und ein vollständig offenes WLAN in meinem Netzwerk. Wählt der Client standardmäßig das offene WLAN? Oder wird der Client automatisch mit der WLAN-ID verknüpft, die auf dem MAC-Filter festgelegt ist? Warum gibt es eine "Schnittstelle"-Option für einen MAC-Filter?

A. Der Client kann mit jedem WLAN verbunden werden, mit dem der Client für die Verbindung konfiguriert ist. Die Schnittstellenoption im MAC-Filter bietet die Möglichkeit, den Filter auf ein WLAN oder eine Schnittstelle anzuwenden. Wenn mehrere WLANs mit derselben Schnittstelle verbunden sind, können Sie den MAC-Filter auf die Schnittstelle anwenden, ohne einen Filter für jedes einzelne WLAN erstellen zu müssen.

Frage: Wie kann ich die TACACS-Authentifizierung für Managementbenutzer auf dem Wireless LAN Controller (WLC) konfigurieren?

A. Ab WLC Version 4.1 wird TACACS auf den WLCs unterstützt. Weitere Informationen zur Konfiguration von TACACS+ für die Authentifizierung von Verwaltungsbenutzern des WLC finden Sie unter Konfigurieren von TACACS+.

Frage: Was geschieht mit der Einstellung für einen überhöhten Authentifizierungsfehler in einem Wireless LAN Controller (WLC)?

A. Diese Einstellung ist eine der Clientausschlussrichtlinien. Der Client-Ausschluss ist eine Sicherheitsfunktion auf dem Controller. Die Richtlinie wird verwendet, um Clients auf eine Blacklist zu setzen, um illegalen Zugriff auf das Netzwerk oder Angriffe auf das Wireless-Netzwerk zu verhindern.

Wenn diese Richtlinie für exzessive Web-Authentifizierungsfehler aktiviert ist und die Anzahl der fehlgeschlagenen Web-Authentifizierungsversuche eines Clients 5 übersteigt, geht der Controller davon aus, dass der Client die maximale Anzahl von Web-Authentifizierungsversuchen überschritten hat, und listet den Client auf einer schwarzen Liste auf.

Gehen Sie wie folgt vor, um diese Einstellung zu aktivieren oder zu deaktivieren:

1. Gehen Sie in der WLC-GUI zu **Security > Wireless Protection Policies > Client Exclusion Policies**.
2. Aktivieren bzw. deaktivieren Sie **Excessive Web Authentication Failures**.

F. Ich habe meinen autonomen Access Point (AP) in den Lightweight-Modus umgewandelt. Im LWAPP-Modus (Lightweight AP Protocol) mit dem AAA-RADIUS-Server für die Client-Abrechnung wird der Client normalerweise anhand der IP-Adresse des WLC mit der RADIUS-Abrechnung nachverfolgt. Ist es möglich, die RADIUS-Abrechnung auf der Grundlage der MAC-Adresse des diesem WLC zugeordneten AP und nicht der IP-Adresse des WLC einzurichten?

Antwort: Ja, dies ist mit der WLC-seitigen Konfiguration möglich. Führen Sie diese Schritte aus:

1. In der Controller-GUI gibt es unter **Security > Radius Accounting** ein Dropdown-Feld für den Anrufstations-ID-Typ. Wählen Sie die **AP-MAC-Adresse aus**.
2. Überprüfen Sie dies anhand des LWAPP-AP-Protokolls. Dort sehen Sie das Feld mit der Stations-ID des angerufenen Teilnehmers, in dem die MAC-Adresse des AP angezeigt wird, dem der jeweilige Client zugeordnet ist.

Frage: Wie ändern Sie den Wert des Handshake-Timeouts für Wi-Fi Protected Access (WPA) auf einem Wireless LAN Controller (WLC) über die CLI? Ich weiß, dass ich dies auf Cisco IOS® Access Points (APs) mit dem Befehl dot11 wpa handshake timeout *value* tun kann, aber wie führst du das auf einem WLC aus?

A. Die Möglichkeit, das WPA-Handshake-Timeout über die WLCs zu konfigurieren, wurde in Softwareversion 4.2 und höher integriert. Bei früheren WLC-Softwareversionen ist diese Option nicht erforderlich.

Mit diesen Befehlen kann das WPA-Handshake-Timeout geändert werden:

```
    config advanced eap eapol-key-timeout <value>
    config advanced eap eapol-key-retries <value>
```

Die Standardwerte spiegeln weiterhin das aktuelle Verhalten der WLCs wider.

```
   - the default value for eapol-key-timeout is 1 second.
   - the default value for eapol-key-retries is 2 retries
```

Hinweis: Auf IOS-APs kann diese Einstellung mit dem Befehl **dot11 wpa handshake** konfiguriert werden.

Sie können die anderen EAP-Parameter auch mit den Optionen unter dem Befehl **config advanced eap** konfigurieren.

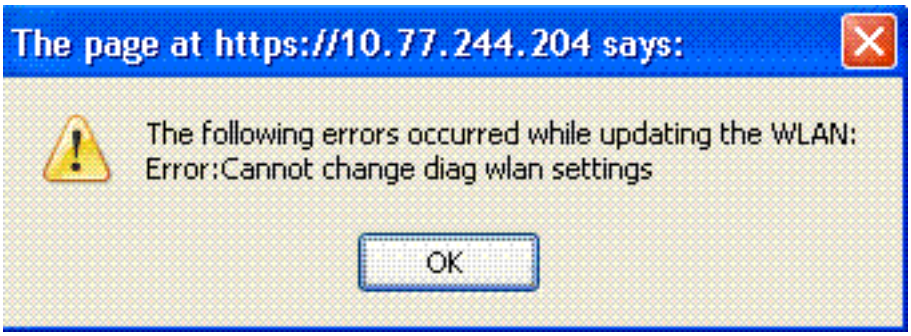
```
(Cisco Controller) >config advanced eap ?

eapol-key-timeout
   Configures EAPOL-Key Timeout in seconds.
eapol-key-retries
   Configures EAPOL-Key Max Retries.
identity-request-timeout
   Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries
   Configures EAP-Identity-Request Max Retries.
key-index
   Configure the key index used for
   dynamic WEP(802.1x) unicast key (PTK).
max-login-ignore-identity-response
   Configure to ignore the same username count
   reaching max in the EAP identity response
request-timeout
   Configures EAP-Request Timeout in seconds.
request-retries
   Configures EAP-Request Max Retries.
```

Frage: Welchen Zweck hat die Diagnosekanalfunktion auf der Seite WLAN > Edit > Advanced (WLAN > Bearbeiten > Erweitert)?

A. Mit der Diagnosekanalfunktion können Sie Probleme bei der Client-Kommunikation mit einem WLAN beheben. Der Client und die Access Points können einem definierten Testsatz unterzogen werden, um die Ursache von Kommunikationsschwierigkeiten zu ermitteln, mit denen der Client konfrontiert wird, und um dann Korrekturmaßnahmen zu ermöglichen, damit der Client im Netzwerk betriebsbereit ist. Sie können den Diagnosekanal über die grafische Benutzeroberfläche (GUI) oder die Kommandozeile (CLI) des Controllers aktivieren und die Diagnosetests über die Kommandozeile (CLI) oder das WCS durchführen.

Der Diagnosekanal kann nur zum Testen verwendet werden. Wenn Sie versuchen, die Authentifizierung oder Verschlüsselung für das WLAN bei aktiviertem Diagnosekanal zu konfigurieren, wird dieser Fehler angezeigt:



Frage: Wie viele AP-Gruppen können maximal auf einem WLC konfiguriert werden?

A. Diese Liste zeigt die maximale Anzahl von AP-Gruppen, die Sie auf einem WLC konfigurieren können:

- Maximal 50 Access Point-Gruppen für Cisco Controller der Serie 2100 und Controller-Netzwerkmodule
- Maximal 300 Access Point-Gruppen für Cisco Controller der Serie 4400, Cisco WiSM und Cisco 3750G Wireless LAN Controller Switch
- Maximal 500 Access Point-Gruppen für Cisco Controller der Serie 5500

Zugehörige Informationen

- Wireless LAN Controller (WLC) – Häufig gestellte Fragen
- Häufig gestellte Fragen zu Wireless LAN Controller (WLC)-Fehlern und -Systemmeldungen
- Lightweight Access Point - Häufig gestellte Fragen
- Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 7.0.116.0
- IPv6-Unterstützung auf dem Wireless LAN Controller
- Support für Wireless-Produkte
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.