Draadloos LAN-controller (WLC) ontwerp en functies Veelgestelde vragen

Inhoud

Inleiding

Dit document biedt informatie over de meest gestelde vragen (FAQ) over het ontwerp en de functies die beschikbaar zijn met een Wireless LAN Controller (WLC).

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Veelgestelde vragen over ontwerpen

V. Hoe configureer ik de switch om verbinding te maken met de WLC?

A. Configureer de switch-poort waarop de WLC is aangesloten als een IEEE 802.1Q trunkpoort. Zorg ervoor dat alleen de benodigde VLAN's op de switch zijn toegestaan. Gewoonlijk, worden het beheer en de AP-Manager interface van WLC verlaten untagged. Dit betekent dat ze het native VLAN van de aangesloten switch overnemen. Dat is niet nodig. U kunt een afzonderlijk VLAN aan deze interfaces toewijzen. Raadpleeg voor meer informatie het *gedeelte Configure the Switch for the WLC*-sectie van Wireless LAN Controller en Lichtgewicht access point - basisconfiguratievoorbeeld.

Q. Wordt al netwerkverkeer van en naar een WLAN-clienttunnel via een draadloze LAN-controller (WLC) geregistreerd wanneer het access point (AP) is geregistreerd met de controller?

A. Wanneer AP zich bij een WLC aansluit, wordt een tunnel van de Controle en van de Provisioning van Draadloze Toegang Punten Protocol (CAPWAP) gevormd tussen de twee apparaten. Al het verkeer, dat al het cliëntverkeer omvat, wordt verzonden door de tunnel CAPWAP.

De enige uitzondering hierop is wanneer een AP zich in de hybride-REAP-modus bevindt. De hybride-REAP access points kunnen client-dataverkeer lokaal switches en client-verificatie lokaal uitvoeren wanneer hun verbinding met de controller verloren gaat. Wanneer zij met de controller zijn verbonden, kunnen zij ook verkeer terugsturen naar de controller.

V. Kan ik Lichtgewicht access points (LAP's) op een extern kantoor installeren en een Cisco draadloze LAN-controller (WLC) op mijn hoofdkantoor installeren? Werkt de LWAP/CAPWAP via een WAN?

A. Ja, u kunt WLCs over WAN van APs hebben. LWAP/CAPWAP werkt via een WAN wanneer de LAP's zijn geconfigureerd in de modus Remote Edge AP (REAP) of Hybrid Remote Edge AP (H-REAP). Beide modi kunnen een AP bedienen door een afstandsbediening die verbonden is via een WAN-verbinding. Het verkeer wordt lokaal overbrugd naar de LAN link, waardoor de noodzaak wordt vermeden om onnodig lokaal verkeer via de WAN-link te versturen. Dit is precies een van de grootste voordelen van het hebben van WLC's in uw draadloze netwerk.

Opmerking: niet alle lichtgewicht AP's ondersteunen deze modi. De H-REAP-modus wordt bijvoorbeeld alleen ondersteund in 1131, 140, 1242, 1250 en AP801 LAP's. De REAP-modus wordt alleen ondersteund op de 1030 AP, maar de 1010 en 1020 AP's ondersteunen de REAP niet. Voordat u deze modi gaat implementeren, controleert u of de LAP's deze ondersteunen. Cisco IOS®-softwarereleases (Autonome AP's) die naar WAP zijn geconverteerd, ondersteunen WAP niet.

V. Hoe werken de opties REAP en H-REAP?

A. In de **REAP-**modus wordt al het controle- en beheerverkeer, inclusief het verificatieverkeer, getunneld naar de WLC. Maar al het gegevensverkeer wordt lokaal geschakeld binnen het externe kantoor-LAN. Wanneer de verbinding met de WLC verloren gaat, worden alle WLAN's beëindigd, behalve het eerste WLAN (WLAN1). Alle clients die momenteel aan dit WLAN zijn gekoppeld, worden behouden. Om de nieuwe clients in de uitvaltijd de mogelijkheid te geven om de service op dit WLAN met succes te verifiëren en te ontvangen, configureert u de verificatiemethode voor dit WLAN als WEP of WPA-PSK, zodat de verificatie lokaal op het REAP wordt uitgevoerd. Raadpleeg voor meer informatie over de implementatie van REAP de REAP-implementatiegids bij de vestiging.

In de **H-REAP-**modus tunnelt een toegangspunt het controle- en beheerverkeer, dat het verificatieverkeer omvat, terug naar de WLC. Het gegevensverkeer van een WLAN wordt lokaal overbrugd in het externe kantoor als het WLAN is geconfigureerd met H-REAP lokale switching, of het gegevensverkeer wordt teruggestuurd naar de WLC. Wanneer de verbinding met de WLC verloren gaat, worden alle WLAN's beëindigd, behalve de eerste acht WLAN's die met H-REAP lokale switching zijn geconfigureerd. Alle clients die momenteel aan deze WLAN's zijn gekoppeld, worden behouden. Om de nieuwe clients in de uitvaltijd in staat te stellen om de service op deze WLAN's met succes te verifiëren en te ontvangen, configureert u de verificatiemethode voor dit WLAN als WEP, WPA PSK of WPA2 PSK, zodat de verificatie lokaal bij H-REAP wordt uitgevoerd.

Raadpleeg de H-REAP Design and Implementation Guide voor meer informatie over H-REAP.

V. Wat is het verschil tussen Remote-Edge AP (REAP) en Hybrid-REAP (H-REAP)?

A. REAP ondersteunt IEEE 802.1Q VLAN-tagging niet. Als zodanig ondersteunt het geen meerdere VLAN's. Het verkeer van alle serviceset-id's (SSID) eindigt op hetzelfde subnetknooppunt, maar H-REAP ondersteunt IEEE 802.1Q VLAN-tagging. Het verkeer van elke SSID kan aan uniek VLAN worden gesegmenteerd.

Wanneer de verbinding met de WLC verloren gaat, dat wil zeggen, in Standalone modus, REAP

dient slechts één WLAN, dat wil zeggen het Eerste WLAN. Alle andere WLAN's worden gedeactiveerd. In H-REAP worden tot 8 WLAN's ondersteund tijdens downtime.

Een ander belangrijk verschil is dat in de REAP-modus gegevensverkeer alleen lokaal kan worden overbrugd. Het kan niet worden teruggeschakeld naar het centraal kantoor, maar in H-REAP modus, hebt u de mogelijkheid om het verkeer terug naar het centraal kantoor te switches. Het verkeer van WLAN's die met H-REAP lokale switching zijn geconfigureerd, wordt lokaal geschakeld. Het gegevensverkeer van andere WLAN's wordt teruggeschakeld naar het hoofdkantoor.

Raadpleeg het configuratievoorbeeld van Remote-Edge AP (REAP) met lichtgewicht AP's en Wireless LAN Controllers (WLC's) voor meer informatie over REAP.

Raadpleeg Hybride WAP configureren voor meer informatie over H-WAP.

Q. Hoeveel WLAN's worden ondersteund op WLC?

A. Sinds softwareversie 5.2.157.0, kan WLC tot 512 WLANs voor lichtgewicht access points nu controleren. Elk WLAN heeft een afzonderlijke WLAN-id (1 tot en met 512), een afzonderlijke profielnaam en een WLAN-SSID en kan aan een uniek beveiligingsbeleid worden toegewezen. De controller publiceert maximaal 16 WLAN's naar elk aangesloten toegangspunt, maar u kunt maximaal 512 WLAN's op de controller maken en vervolgens selectief deze WLAN's (met behulp van access point groepen) naar verschillende access points publiceren om uw draadloze netwerk beter te beheren.

Opmerking: Cisco 2106-, 2112- en 2125-controllers ondersteunen alleen tot 16 WLAN's.

N.B.: Lees voor gedetailleerde informatie over de richtlijnen voor het configureren van WLAN's op WLC's de sectie Create WLAN's van de Cisco Wireless LAN Controller Configuration Guide, release 7.0.16.0.

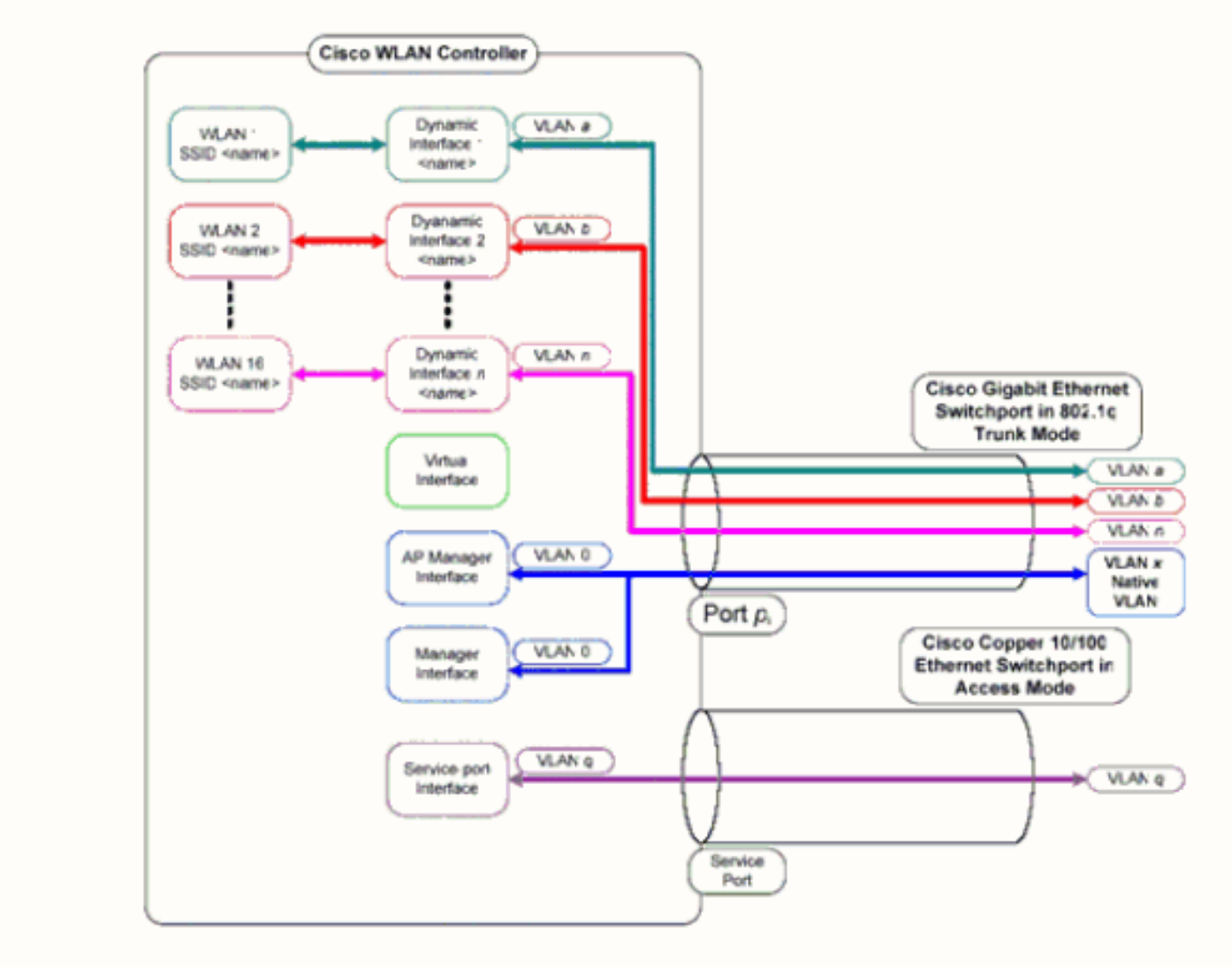
V. Hoe kan ik VLAN's configureren op mijn draadloze LAN-controller (WLC)?

A. In WLC, zijn VLANs gebonden aan een interface die in unieke IP-subnetwerkknooppunt wordt gevormd. Deze interface wordt toegewezen aan een WLAN. Vervolgens behoren de clients die met dit WLAN zijn geassocieerd tot het VLAN van de interface en worden aan deze client een IP-adres toegewezen van het subnetnetwerk waartoe de interface behoort. Voltooi de procedure in het configuratievoorbeeld van VLAN's op draadloze LAN-controllers om VLAN's op uw WLC te configureren.

Q. We hebben twee WLAN's met twee verschillende dynamische interfaces geleverd. Elke interface heeft zijn eigen VLAN, dat anders is dan de beheerinterface VLAN. Dit lijkt te werken, maar we hebben de trunkpoorten niet geprovisioneerd om de VLAN's toe te staan die onze WLAN's gebruiken. Codeert het access point (AP) de pakketten met de beheerinterface VLAN?

A. AP etiketteert geen pakketten met de beheersinterface VLAN. AP kapselt de pakketten van de cliënten in LichtgewichtAP Protocol (LWAP)/CAPWAP in, en gaat dan de pakketten over op WLC. De WLC stript vervolgens de LWAPP/CAPWAP-header en stuurt de pakketten door naar de gateway met de juiste VLAN-tag. De VLAN-tag hangt af van het WLAN waartoe de client behoort. De WLC hangt af van de gateway om de pakketten naar hun bestemming te leiden. Om verkeer

voor meerdere VLAN's te kunnen doorgeven, moet u de uplink-switch als een trunkpoort configureren. In dit diagram wordt uitgelegd hoe VLAN's met controllers werken:



V. Welk IP-adres van de WLC wordt gebruikt voor verificatie met de AAA-server?

A. WLC gebruikt het IP-adres van de beheerinterface voor elk verificatiemechanisme (Layer 2 of Layer 3) waarbij een AAA-server is betrokken. Raadpleeg voor meer informatie over poorten en interfaces op de WLC de sectie *Poorten en interfaces configureren* van de configuratiehandleiding voor Cisco draadloze LAN-controllers, release 7.0.16.0.

Q. Ik heb tien Cisco 1000 Series lichtgewicht access points (LAP's) en twee draadloze LAN-controllers (WLC's) in hetzelfde VLAN. Hoe kan ik zes LAPs registreren om aan WLC1 te associëren, en de andere vier LAPs om aan WLC2 te associëren?

A. De LWAP/CAPWAP maakt dynamische redundantie en taakverdeling mogelijk. Als u bijvoorbeeld meer dan één IP-adres voor optie 43 specificeert, stuurt een LAP LWAP/CAPWAP-detectieverzoeken naar elk van de IP-adressen die het AP ontvangt. In de WLC LWAPP/CAPWAP discovery response, voegt de WLC deze informatie in:

- Informatie over de huidige LAP-belasting, die is gedefinieerd als het aantal LAP's dat op dat moment is aangesloten op de WLC

- De LAP-capaciteit
- Het aantal draadloze clients dat is aangesloten op de WLC

De LAP probeert dan om zich bij de minst-geladen WLC aan te sluiten, die de WLC met de grootste beschikbare LAP capaciteit is. Bovendien, nadat een LAP zich aansluit bij een WLC, leert de LAP de IP-adressen van de andere WLC's in de mobiliteitsgroep van zijn aangesloten WLC.

Zodra een LAP zich aansluit bij een WLC, kunt u de LAP bij een specifieke WLC aansluiten binnen de volgende reboot. Om dit te doen, wees een primaire, secundaire en tertiaire WLC toe voor een LAP. Wanneer de LAP reboots, zoekt het de primaire WLC en sluit zich aan bij die WLC onafhankelijk van de lading op die WLC. Als de primaire WLC niet reageert, zoekt het naar de secundaire, en als er geen reactie is, naar de tertiaire. Voor meer informatie over hoe u de primaire WLC voor een LAP kunt configureren, raadpleegt u de *Toewijzen van primaire, secundaire en tertiaire controllers voor de lichtgewicht AP-*sectie van de WLAN-controller failover voor het lichtgewicht access points Configuration Voorbeeld.

V. Wat zijn de functies die niet worden ondersteund op de 2100 Series draadloze LAN-controllers (WLC's)?

A. Deze hardwarefuncties worden niet ondersteund door de 2100 Series controllers:

- Servicepoort (afzonderlijke out-of-band 10/100-Mb/s Ethernet-interface)

Deze softwarefuncties worden niet ondersteund door 2100 Series controllers:

- VPN-beëindiging (zoals IPsec en L2TP)
- Beëindiging van gastcontrollertunnels (de totstandkoming van gastcontrollertunnels wordt ondersteund)
- Webserverlijst voor externe webverificatie
- Layer 2 LWAPP
- Spanning Tree
- Poortmirroring
- Craniet
- vesting
- AppleTalk
- QoS-bandbreedtecontracten per gebruiker
- IPv6-doorgifte
- Link aggregation (LAG)
- Multicast-unicastmodus
- Bedrade gasttoegang

V. Welke functies worden niet ondersteund door 5500 Series controllers?

A. Deze softwarefuncties worden niet ondersteund door de 5500 Series controllers:

- Statische AP-Manager interface**Opmerking:** voor controllers uit de 5500 Series hoeft u geen AP-manager interface te configureren. De beheerinterface fungeert standaard als een AP-Manager interface en de access points kunnen zich op deze interface aansluiten.
- Asymmetrische mobiliteitstunneling
- STP-protocol (Spanning Tree Protocol)
- Poortmirroring

- Ondersteuning van Layer 2-toegangscontrolelijst (ACL)
- VPN-beëindiging (zoals IPSec en L2TP)
- Optie voor VPN-passthrough
- Configuratie van 802.3-overbrugging, AppleTalk en Point-to-Point Protocol over Ethernet (PPPoE)

V. Welke functies worden niet ondersteund op vermaasde netwerken?

A. Deze controllereigenschappen worden niet ondersteund op vermaasde netwerken:

- Ondersteuning voor meerdere landen
- Op lading gebaseerde CAC (mesh-netwerken ondersteunen alleen bandbreedte-gebaseerde of statische CAC.)
- Hoge beschikbaarheid (snelle hartslag en primaire ontdekking voegen timer)
- EAP-FASTv1- en 802.1X-verificatie
- Toegangspunt samenvoegen met prioriteit (mesh access points hebben een vaste prioriteit.)
- Lokaal relevant certificaat
- Locatiegebaseerde services

V. Wat is de geldigheidsperiode van door de fabrikant geïnstalleerde certificaten (MIC's) op een draadloze LAN-controller en van de lichtgewicht AP-certificaten?

A. De geldigheidsduur van een MIC op een WLC is 10 jaar. Dezelfde geldigheidsperiode van 10 jaar is van toepassing op de lichtgewicht AP's certificaten vanaf de oprichting (of het nu een MIC of een zelfondertekend certificaat (SSC) is).

Q. Ik heb twee draadloze LAN-controllers (WLC's) met de naam WLC1 en WLC2 geconfigureerd binnen dezelfde mobiliteitsgroep voor failover. My Lichtgewicht Access Point (LAP) is momenteel geregistreerd bij WLC1. Als WLC1 faalt, registreert de AP zich bij WLC1 rebooten tijdens de overgang naar de overlevende WLC (WLC2)? Verliest de WLAN-client tijdens deze failover ook WLAN-connectiviteit met de LAP?

A. Ja, de LAP verwijdert zich van WLC1, start opnieuw op en registreert vervolgens opnieuw bij WLC2 als WLC1 mislukt. Omdat de LAP-herstart, verliezen de bijbehorende WLAN-clients de connectiviteit met de herstartvertraging. Raadpleeg voor verwante informatie taakverdeling en terugvalmogelijkheden van AP in Unified Wireless Networks.

V. Is roaming afhankelijk van de Lichtgewicht access point protocol (LWAP) modus die de draadloze LAN controller (WLC) is geconfigureerd voor gebruik? Kan een WLC die in Layer 2 LWAPP-modus werkt Layer 3 roaming uitvoeren?

A. Zolang de mobiliteitsgroepering bij de controllers correct is geconfigureerd, moet client roaming werken prima. Het zwerven wordt niet beïnvloed door de LWAP-modus (Layer 2 of Layer 3). Het is echter aan te raden om Layer 3 LWAPP waar mogelijk te gebruiken.

Opmerking: Layer 2-modus wordt alleen ondersteund door de Cisco 410x- en 440x-Series WLC's en de Cisco 1000 Series access points. Layer 2 WAP wordt niet ondersteund door de andere

draadloze LAN-controller en lichtgewicht access point platforms.

V. Wat is het zwervende proces dat optreedt wanneer een client besluit te zwerven naar een nieuw access point (AP) of controller?

A. Dit is de opeenvolging van gebeurtenissen die voorkomt wanneer een cliënt aan nieuwe AP zwerft:

1. De client stuurt via de LAP een reassociatieverzoek naar de WLC.
2. WLC stuurt het mobiliteitsbericht naar andere WLC's in de mobiliteitsgroep om erachter te komen met welke WLC de client eerder was geassocieerd.
3. De oorspronkelijke WLC reageert met informatie, zoals het MAC-adres, IP-adres, QoS, Security context, etc. over de client via het mobiliteitsbericht.
4. De WLC werkt zijn database bij met de verstrekte clientgegevens; de client gaat dan door het reauthenticatieproces, indien nodig. De nieuwe LAP waarmee de client momenteel wordt geassocieerd wordt ook bijgewerkt samen met andere details in de database van de WLC. Op deze manier wordt het IP-adres van de klant behouden tussen WLC's, wat naadloos zwerven helpt te realiseren.

Raadpleeg voor meer informatie over zwerven in een geünificeerde omgeving de *sectie Configuration Mobility Groepen (Mobiliteitsgroepen configureren)* van de Cisco Wireless LAN-controllerconfiguratiegids, release 7.0.16.0.

Opmerking: de draadloze client stuurt geen (802.11) verificatieaanvraag tijdens de reassociatie. De draadloze client stuurt gewoon de reassociatie onmiddellijk uit. Vervolgens wordt de 802.1x-verificatie uitgevoerd.

V. Welke poorten moet ik toestaan voor LWAP/CAPWAP-communicatie wanneer er een firewall in het netwerk is?

A. U moet deze poorten inschakelen:

- Schakel deze UDP-poorten voor LWAP-verkeer in:Gegevens - 12222Controle - 12223
- Schakel deze UDP-poorten voor CAPWAP-verkeer in:Gegevens - 5247Controle - 5246
- Schakel deze UDP-poorten voor mobiliteitsverkeer in:16666 - Beveiligde modus16667 - onbeveiligde modus

Mobiliteit en databerichten worden meestal uitgewisseld via EtherIP-pakketten. **IP-protocol 97** moet op de firewall zijn toegestaan om EtherIP-pakketten toe te staan. Als u **ESP** gebruikt om mobiliteitspakketten in te kapselen, moet u **ISAKMP** via de firewall toestaan wanneer u **UDP poort 500** opent. U moet ook het **IP-protocol 50** openen om de versleutelde gegevens door de firewall te laten passeren.

Deze poorten zijn optioneel (afhankelijk van uw vereisten):

- TCP/IP-telefoon 161 en 162 voor SNMP (voor het draadloze controlesysteem [WCS])
- UDP 69 voor TFTP
- TCP/IPsec 800 en/of 443 TCP- of HTTPS-toegang voor GUI
- TCP/IPsec 23 en/of TCP/IPv 22 voor Telnet of Secure Shell (SSH) voor CLI-toegang

V. Ondersteuning van draadloze LAN-controllers voor zowel SSHv1 als SSHv2?

A. Draadloze LAN-controllers ondersteunen alleen SSHv2.

Q. Wordt Reverse ARP (RARP) ondersteund door Wireless LAN-controllers (WLC's)?

A. Reverse Address Resolution Protocol (RARP) is een protocol op de koppelingslaag dat wordt gebruikt om een IP-adres te verkrijgen voor een bepaald koppelingslaagadres, zoals een Ethernet-adres. RARP wordt ondersteund met WLC's met firmware versie 4.0.217.0 of hoger. RARP wordt niet ondersteund op een van de eerdere versies.

V. Kan ik de interne DHCP-server op de draadloze LAN-controller (WLC) gebruiken om IP-adressen toe te wijzen aan de Lichtgewicht access points (LAP's)?

A. De controllers bevatten een interne DHCP-server. Deze server wordt meestal gebruikt in filialen die nog geen DHCP-server hebben. Om tot de DHCP-service toegang te krijgen, klikt u op het menu **Controller** vanuit de WLC GUI; klik vervolgens op de optie **Interne DHCP-server** aan de linkerkant van de pagina. Raadpleeg de sectie *DHCP configureren* in de Cisco Wireless LAN Controller Configuration Guide, release 7.0.16.0 voor meer informatie over het configureren van het DHCP-bereik in de WLC.

De interne server biedt DHCP-adressen aan draadloze clients, LAP's, app-mode AP's op de beheerinterface en DHCP-verzoeken die worden doorgegeven vanuit LAP's. WLC's bieden nooit adressen aan apparaten stroomopwaarts in het bekabelde netwerk. DHCP-optie 43 wordt niet ondersteund op de interne server, dus het toegangspunt moet een andere methode gebruiken om het IP-adres van de beheerinterface van de controller te vinden, zoals lokale subnetuitzending, DNS, priming of detectie via de ether.

Opmerking: WLC firmware versies voor 4.0 ondersteunen DHCP-service niet voor LAP's, tenzij de LAP's direct zijn verbonden met de WLC. De interne DHCP-serverfunctie is alleen gebruikt om IP-adressen te leveren aan clients die verbinding maken met het draadloze LAN-netwerk.

V. Wat betekent het veld DHCP Required onder een WLAN?

A. DHCP Required is een optie die kan worden ingeschakeld voor een WLAN. Het vereist dat alle clients die met dat bepaalde WLAN geassocieerd zijn, IP-adressen verkrijgen via DHCP. Clients met statische IP-adressen mogen niet aan het WLAN koppelen. Deze optie staat in het tabblad Geavanceerd van een WLAN. WLC staat het verkeer aan/van een cliënt slechts toe als zijn IP adres in de MSCB- lijst van WLC aanwezig is. WLC registreert het IP-adres van een client tijdens het DHCP-verzoek of DHCP Verlengen. Dit vereist dat een client zijn IP-adres vernieuwt elke keer dat hij opnieuw aan de WLC associeert, omdat elke keer dat de client zich ontkoppelt als deel van zijn roamproces of sessietime-out, zijn ingang wordt gewist uit de MSCB-tabel. De client moet opnieuw authenticeren en opnieuw koppelen aan de WLC, die opnieuw de client in de tabel maakt.

V. Hoe werkt Cisco Centralized Key Management (CCKM) in een WAP/CAPWAP-omgeving?

A. Tijdens de aanvankelijke cliëntvereniging, bespreekt AP of WLC een paar-wijze hoofdsleutel (PMK) nadat de draadloze cliënt 802.1x authentificatie overgaat. De WLC of WDS AP slaat de PMK voor elke client in. Wanneer een draadloze client opnieuw koppelt of zwerft, wordt de 802.1x-

verificatie overgeslagen en wordt de PMK meteen gevalideerd.

De enige speciale implementatie van de WLC in CCKM is dat WLC's client PMK uitwisselen via mobiliteitspakketten, zoals UDP 16666.

V. Hoe stel ik de duplexinstellingen in op de draadloze LAN-controller (WLC) en de lichtgewicht access points (LAP's)?

A. Cisco Wireless-producten werken het beste wanneer zowel snelheid als duplex automatisch worden onderhandeld, maar u hebt de optie om de duplexinstellingen op de WLC en LAP's in te stellen. Om de instellingen AP speed/duplex in te stellen, kunt u de duplexinstellingen voor de LAP's op de controller configureren en ze vervolgens naar de LAP's drukken.

ap Ethernet duplex <auto/half/full>-snelheid configureren <auto/10/100/1000> <all/Cisco AP Name> is de opdracht om de duplexinstellingen in te stellen via de CLI. Deze opdracht wordt alleen ondersteund door versies 4.1 en hoger.

Om de duplexinstellingen voor de fysieke interfaces WLC te plaatsen, gebruik de **configuratiepoort physical mode {allen | haven} {100 uur | 100 septies | 10 nonies | 10f}** opdracht.

Met deze opdracht worden de gespecificeerde of alle 10/100BASE-T Ethernet-poorten op het voorpaneel ingesteld voor speciale 10 Mbps of 100 Mbps, half-duplex of full-duplex werking. Merk op dat u autonegotiation met het bevel van de **configuratiehaven** moet onbruikbaar maken alvorens u manueel om het even welke fysieke wijze op de haven vormt. Merk ook op dat het bevel van de **configuratiehaven autonoom** die instellingen met het bevel van de **configuratiehaven fysieke wijze** worden gemaakt met voeten treedt. Standaard zijn alle poorten ingesteld op automatisch onderhandelen.

Opmerking: de snelheidsinstellingen op de glasvezelpoorten kunnen niet worden gewijzigd.

Q. Is er een manier om de naam van het Lichtgewicht access point (LAP) te volgen wanneer het niet geregistreerd is bij de controller?

A. Als uw AP volledig neer en niet geregistreerd aan de controller is, is er geen manier waarop u de LAP door de controller kunt volgen. De enige manier waarop dit nog mogelijk is, is dat u toegang hebt tot de switch waarop deze AP's zijn aangesloten en dat u de switchpoort kunt vinden waarop ze zijn aangesloten met behulp van deze opdracht:

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

Dit geeft u het poortnummer op de switch waarop deze AP is aangesloten. Geef vervolgens deze opdracht uit:

```
show cdp nei detail
```

De output van dit bevel geeft ook de naam van de LAMP. Deze methode is echter alleen mogelijk wanneer het toegangspunt is ingeschakeld en is aangesloten op de switch.

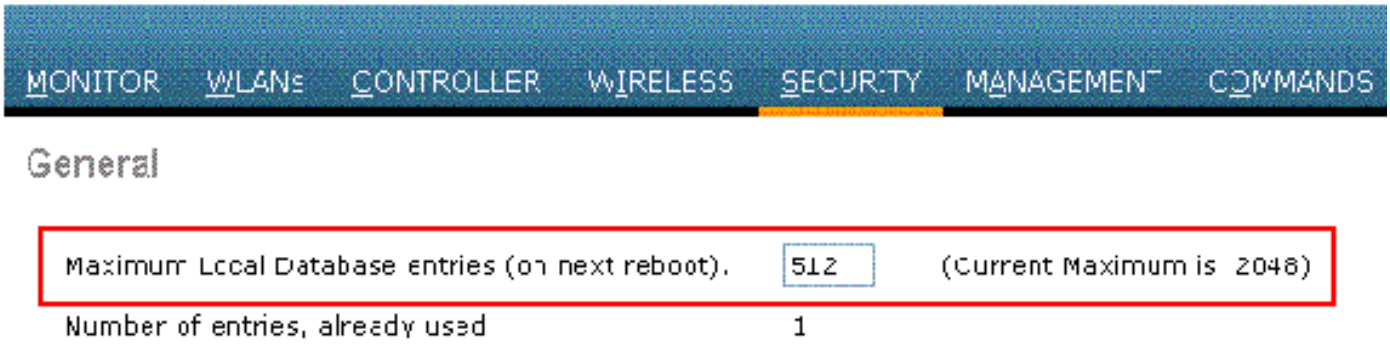
Q. Ik heb 512 gebruikers op mijn controller geconfigureerd. Is er een manier om het aantal gebruikers van de draadloze LAN-controller (WLC) te verhogen?

A. De lokale gebruikersdatabase is beperkt tot maximaal 2048 vermeldingen op de pagina **Security > General**. Deze database wordt gedeeld door lokale beheergebruikers (waaronder lobbyambassadeurs), netgebruikers (waaronder gastgebruikers), MAC-filtervermeldingen, vermeldingen in de toegangslijst en vermeldingen in de uitsluitingslijst. Samen, kunnen al deze types van gebruikers niet de gevormde gegevensbestandgrootte overschrijden.

Om de lokale database te vergroten, gebruikt u deze opdracht van de CLI:

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

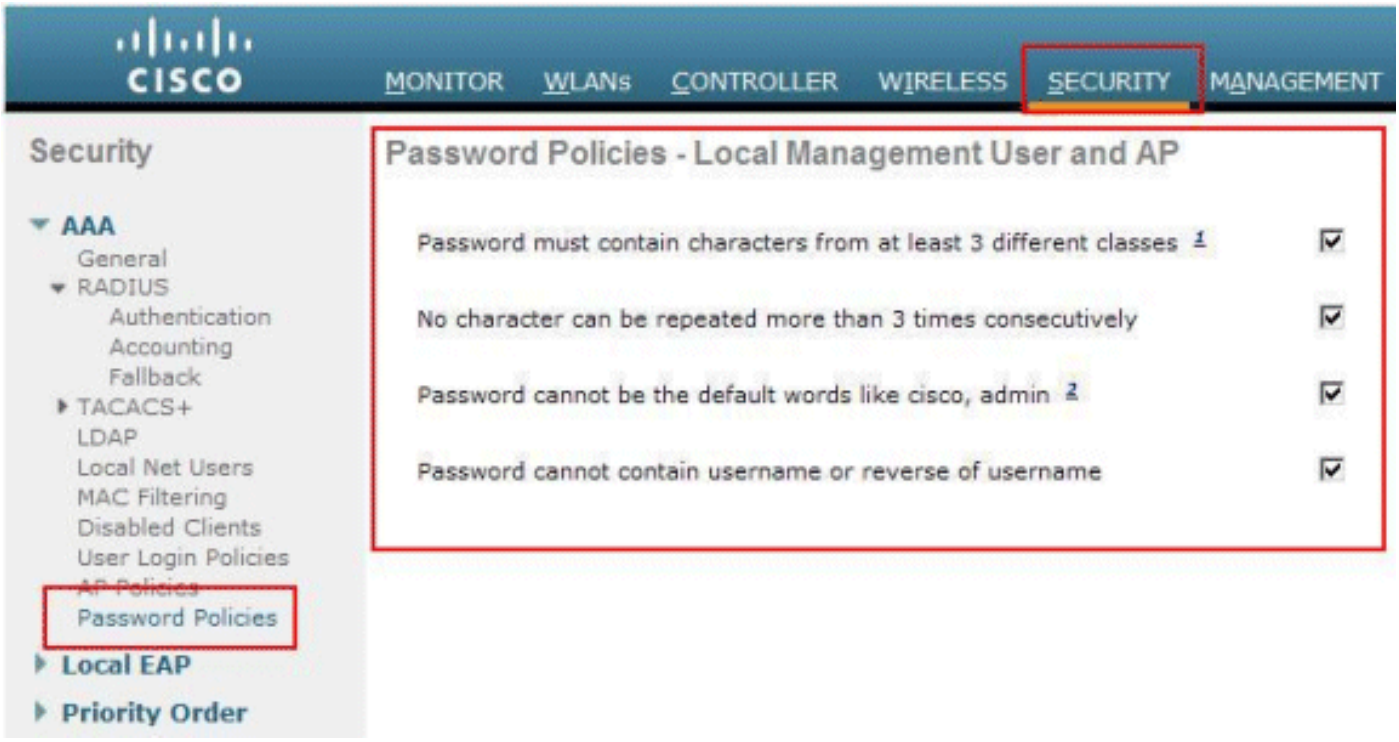
Opmerking: u moet de configuratie opslaan en het systeem opnieuw instellen (met de opdracht **Systeem opnieuw instellen**) voordat de wijziging van kracht kan worden.



V. Hoe kan ik een sterk wachtwoordbeleid op WLC's afdwingen?

A. WLCs staat u toe om een sterk wachtwoordbeleid te bepalen. Dit kan worden gedaan met de CLI of GUI.

In de GUI, ga naar **Beveiliging > AAA > Wachtwoordbeleid**. Deze pagina heeft een aantal opties die kunnen worden geselecteerd om een sterk wachtwoord af te dwingen. Hierna volgt een voorbeeld:



Om dit van de WLC CLI te doen, gebruik de **configuratie switchconfig strong-pwd** *{case-check | Controle achtereenvolgens | standaardcontrole | Gebruikersnaam controleren | all-check} {inschakelen | Uitschakelen}* opdracht:

- **case-check** - Controleert het voorkomen van hetzelfde teken driemaal na elkaar.
- **opeenvolgend-controle** - Controleert als de standaardwaarden of zijn varianten worden gebruikt.
- **default-check** - Controleert of de gebruikersnaam of het omgekeerde wordt gebruikt.
- **all-checks** - Schakelt alle sterke wachtwoordcontroles in/uit.

V. Hoe wordt de passieve clientfunctie gebruikt voor draadloze LAN-controllers?

A. Passieve clients zijn draadloze apparaten, zoals weegschalen en printers die zijn geconfigureerd met een statisch IP-adres. Deze clients verzenden geen IP-informatie zoals IP-adres, subnetmasker en gatewayinformatie wanneer ze aan een toegangspunt gekoppeld zijn. Wanneer passieve clients worden gebruikt, kent de controller het IP-adres dus nooit, tenzij ze de DHCP gebruiken.

WLC's fungeren momenteel als proxy voor ARP-verzoeken. Bij ontvangst van een ARP verzoek, reageert de controller met een ARP-antwoord in plaats van het verzoek rechtstreeks door te geven aan de client. Dit scenario heeft twee voordelen:

- Het upstream apparaat dat het ARP verzoek verstuurt naar de client zal niet weten waar de client zich bevindt.
- De macht voor batterij-bediende apparaten zoals mobiele telefoons en printers wordt bewaard omdat zij niet aan elke ARP verzoeken moeten gevolg geven.

Aangezien de draadloze controller geen IP-gerelateerde informatie over de passieve clients heeft, kan het niet reageren op ARP-verzoeken. Het huidige gedrag staat de overdracht van ARP verzoeken aan passieve cliënten niet toe. Elke toepassing die probeert toegang te krijgen tot een

passieve client zal falen.

De passieve cliënteigenschap laat de ARP verzoeken en de reacties toe om tussen getelegrafeerde en draadloze cliënten worden uitgewisseld. Deze eigenschap, wanneer toegelaten, staat het controlemechanisme toe om ARP verzoeken van getelegrafeerd aan draadloze cliënten over te gaan tot de gewenste draadloze cliënt aan de staat van de LOOPPAS krijgt.

Voor informatie over het configureren van de passieve clientfunctie raadpleegt u de sectie Gebruik van de GUI om passieve client te configureren in de configuratiehandleiding voor Cisco draadloze LAN-controllers, release 7.0.16.0.

V. Hoe kan ik de client zo instellen dat deze om de drie minuten of op een bepaalde periode opnieuw wordt geverifieerd met de RADIUS-server?

A. De sessie timeout parameter op de WLC kan worden gebruikt om dit te realiseren. In de standaardinstelling wordt de time-outparameter van de sessie ingesteld op 1800 seconden voordat er een nieuwe verificatie plaatsvindt.

Verander deze waarde in 180 seconden om de client na drie minuten opnieuw te verifiëren.

Klik op het menu **WLAN's** in de GUI om toegang te krijgen tot de parameter voor de sessietime-out. Het toont de lijst van WLAN's die in de WLC zijn geconfigureerd. Klik op het WLAN waartoe de client behoort. Ga naar het tabblad **Geavanceerd** en u vindt de parameter *Session Time-out inschakelen*. Verander de standaardwaarde in 180 en klik op **Toepassen** om de wijzigingen door te voeren.

Wanneer verzonden in een Access-Accept, samen met een Termination-Action-waarde van RADIUS-request, specificeert het Session-Time-out-kenmerk het maximale aantal seconden service dat wordt geboden voordat de verificatie wordt herhaald. In dit geval wordt het kenmerk Session-Time-out gebruikt om de ReAuthPeriod-constante te laden in de statusmachine van de verificatieteller van 802.1X.

Q. Ik heb een gast tunneling, Ethernet over IP (EoIP) tunnel, die tussen mijn draadloze LAN controller 4400 (WLC) wordt gevormd, die als anker WLC, en verscheidene verre WLCs dienst doet. Kan dit anker WLC voorwaartse subnetuitzendingen door de EoIP-tunnel van het bekabelde netwerk naar draadloze clients geassocieerd met de afstandscontrollers?

A. Nee, de WLC 4400 stuurt IP-subnetuitzendingen niet door van de bekabelde kant naar de draadloze clients in de EoIP-tunnel. Dit is geen ondersteunde functie. Cisco ondersteunt het tunnelen van subnetuitzending of multicast niet in topologie voor gasttoegang. Aangezien het gast WLAN het clientpunt van aanwezigheid afdwingt op een zeer specifieke locatie in het netwerk, meestal buiten de firewall, kan het tunnelen van subnetuitzending een beveiligingsprobleem zijn.

Q. Welke DSCP-waarden (Differentiated Services Code Point) worden in een installatie met Wireless LAN Controller (WLC) en Lichtgewicht Access Point Protocol (LWAP) doorgegeven voor spraakverkeer? Hoe wordt QoS geïmplementeerd op de WLC?

A. De Cisco Unified Wireless Network (UWN)-oplossing WLAN's ondersteunen vier niveaus van QoS:

- Platinum/spraak
- Goud/video
- Zilver/Beste Inspanning (standaard)
- Brons/achtergrond

U kunt het spraakverkeer WLAN configureren om Platinum QoS te gebruiken, het WLAN met lage bandbreedte toewijzen om Bronze QoS te gebruiken en al het andere verkeer tussen de andere QoS-niveaus toewijzen. Raadpleeg Een QoS-profiel toewijzen aan een WLAN voor meer informatie.

V. Worden Linksys Ethernet-bruggen ondersteund in een Cisco draadloze Unified Solution?

A. Nee, de WLC ondersteunt alleen Cisco WGB-producten. Linksys WGBs wordt niet ondersteund. Hoewel de Cisco Wireless Unified Solution de Linksys WET54G en WET11B Ethernet-bruggen niet ondersteunt, kunt u deze apparaten in een configuratie voor draadloze Unified oplossing gebruiken als u deze richtlijnen gebruikt:

- Sluit slechts één apparaat aan op de WET54G of WET11B.
- Schakel de MAC-kloonfunctie op de WET54G of WET11B in om het aangesloten apparaat te klonen.
- Installeer de nieuwste stuurprogramma's en firmware op apparaten die zijn aangesloten op de WET54G of WET11B. Deze richtlijn is vooral belangrijk voor JetDirect Printers omdat eerdere firmware versies problemen met DHCP veroorzaken.

Opmerking: andere bruggen van derden worden niet ondersteund. De genoemde stappen kunnen ook voor andere derdebruggen worden geprobeerd.

V. Hoe sla ik de configuratiebestanden op de draadloze LAN-controller (WLC) op?

A. De WLC bevat twee soorten geheugen:

- Vluchtig RAM: houdt de huidige, actieve controllerconfiguratie in
- Nonvolatile RAM (NVRAM)—Biedt de herstartconfiguratie

Wanneer u het besturingssysteem in de WLC configureert, wijzigt u het vluchtige RAM. U moet de configuratie van het vluchtige RAM in het NVRAM opslaan om ervoor te zorgen dat de WLC in de huidige configuratie opnieuw wordt opgestart.

Het is belangrijk om te weten welk geheugen u wijzigt wanneer u deze taken uitvoert:

- Gebruik de configuratiewizard.
- Schakel de controllerconfiguratie uit.
- Configuraties opslaan.
- Reset de controller.
- Uitloggen op de CLI.

Veelgestelde vragen over functies

V. Hoe stel ik het EAP-type (Extensible Verification Protocol) in op de draadloze LAN-controller (WLC)? Ik wil verificatie uitvoeren met een ACS-apparaat (Access Control Server) en ik krijg een EAP-type dat niet wordt ondersteund in de logbestanden.

A. Er is geen afzonderlijke instelling van het EAP-type op de WLC. Voor Light EAP (LEAP), EAP Flexible Verification via Secure Tunneling (EAP-FAST) of Microsoft Protected EAP (MS-PEAP) configureert u alleen IEEE 802.1x of Wi-Fi Protected Access (WPA) (als u 802.1x met WPA gebruikt). Elk EAP-type dat wordt ondersteund op de RADIUS-back-end en op de client, wordt ondersteund via de 802.1x-tag. De EAP-instelling op de client en de RADIUS-server moet overeenkomen.

Voltooi deze stappen om EAP via de GUI op de WLC in te schakelen:

1. Klik vanuit de WLC GUI op **WLAN's**.
2. Er wordt een lijst weergegeven van WLAN's die in de WLC zijn geconfigureerd. Klik op een WLAN.
3. Klik in **WLAN's > Bewerken** op het tabblad **Beveiliging**.
4. Klik op **Layer 2** en kies Layer 2 Security als 802.1x of WPA+WPA2. U kunt ook de parameters van 802.1x configureren die in hetzelfde venster beschikbaar zijn. Vervolgens stuurt de WLC EAP-verificatiepakketten door tussen de draadloze client en de verificatieserver.
5. Klik op de **AAA**-servers en kies de verificatieserver in het vervolgkeuzemenu voor dit WLAN. We gaan ervan uit dat de verificatieserver al globaal is geconfigureerd. Raadpleeg het gedeelte *Gebruik* van de *CLI* om *RADIUS* te *configureren* in de sectie Cisco Wireless LAN Controller Configuration Guide, release 7.0.16.0, voor informatie over het inschakelen van *de* EAP-optie op WLC's via *de* opdrachtregelinterface (CLI).

V. Wat is Fast SSID Changing?

A. Snel SSID veranderen staat cliënten toe om tussen SSIDs te bewegen. Wanneer de client een nieuwe associatie voor een andere SSID verstuurt, wordt de client-ingang in de controllerverbindingstabel gewist voordat de client aan de nieuwe SSID wordt toegevoegd. Wanneer Fast SSID Changing is uitgeschakeld, dwingt de controller een vertraging af voordat clients naar een nieuwe SSID mogen overstappen. Raadpleeg het gedeelte *Fast SSID Changing configureren* van de configuratiehandleiding voor draadloze LAN-controllers van Cisco, release 7.0.16.0, voor informatie over het inschakelen van Fast SSID Changing.

V. Kan ik een limiet instellen voor het aantal clients dat verbinding kan maken met een draadloos LAN?

A. U kunt een limiet instellen voor het aantal clients dat verbinding kan maken met een WLAN, wat nuttig is in scenario's waarin u een beperkt aantal clients hebt die verbinding kunnen maken met een controller. Het aantal clients dat u per WLAN kunt configureren, is afhankelijk van het platform dat u gebruikt.

Lees het gedeelte Het maximale aantal clients per WLAN configureren van de configuratiehandleiding van de Cisco draadloze LAN-controller, release 7.0.16.0 voor informatie over de clientlimieten per WLAN voor de verschillende platforms van draadloze LAN-controllers.

V. Wat is PKC en hoe werkt het met de draadloze LAN-controller (WLC)?

A. PKC staat voor Proactive Key Caching. Het is ontworpen als een uitbreiding van de 802.11i IEEE standaard.

PKC is een functie die is ingeschakeld in Cisco 2006/410x/440x Series controllers die ervoor zorgen dat goed uitgeruste draadloze clients kunnen zwerven zonder volledige herverificatie met een AAA-server. Om PKC te begrijpen, moet je eerst Key Caching begrijpen.

Key Caching is een functie die werd toegevoegd aan WPA2. Hierdoor kan een mobiel station de master keys (Pairwise Master Key [PMK]) cachen, het krijgt door een succesvolle verificatie met een access point (AP), en **hergebruiken in een toekomstige associatie met dezelfde AP**. Dit betekent dat een gegeven mobiel apparaat één keer met een specifieke AP moet verifiëren, en de sleutel voor toekomstig gebruik in het voorgeheugen onderbrengen. Key Caching wordt verwerkt via een mechanisme dat bekend staat als de PMK Identifier (PMKID), die een hash is van de PMK, een string, het station en de MAC-adressen van de AP. De PMKID identificeert de PMK op unieke wijze.

Zelfs met Key Caching, moet een draadloos station authenticeren met elke AP het wil service van. Dit leidt tot aanzienlijke latentie en overheadkosten, die het afgifteproces vertragen en de mogelijkheid om real-time toepassingen te ondersteunen kunnen belemmeren. Om dit probleem op te lossen werd PKC geïntroduceerd met WPA2.

PKC staat een station toe om een PMK die het eerder had verkregen via een succesvol verificatieproces, te hergebruiken. Dit elimineert de noodzaak voor het station om te authenticeren tegen nieuwe AP's tijdens het zwerven.

Daarom, in een intra-controller roaming, wanneer een mobiel apparaat beweegt van de ene AP naar de andere op dezelfde controller, herberekent de client een PMKID met behulp van de eerder gebruikte PMK en presenteert deze tijdens het associatieproces. De WLC zoekt zijn PMK cache om te bepalen of het zo'n ingang heeft. Als dit wel het geval is, wordt het 802.1x-verificatieproces omzeild en wordt onmiddellijk de WPA2-toetsuitwisseling gestart. Als dit niet het geval is, gaat het door het standaard 802.1X-verificatieproces.

PKC is standaard ingeschakeld met WPA2. Daarom wanneer u WPA2 als Layer 2-beveiliging inschakelt onder de WLAN-configuratie van de WLC, wordt PKC ingeschakeld op de WLC. Configureer ook de AAA-server en de draadloze client voor de juiste EAP-verificatie.

De supplicant aan de clientzijde zou ook WPA2 moeten ondersteunen om PKC te laten werken. PKC kan ook worden geïmplementeerd in een roamingomgeving tussen controllers.

Opmerking: PKC werkt niet met Aironet Desktop Utility (ADU) als client supplicant.

V. Wat zijn de toelichtingen bij deze tijdelijke instellingen op de controller: Adresresolutie Protocol (ARP), Time-out gebruiker inactiviteitstimer en Time-out sessie?

A. De **ARP Time-out** wordt gebruikt om ARP-vermeldingen op de WLC te verwijderen voor de apparaten die van het netwerk worden geleerd.

De **User Idle Time-out:** Wanneer een gebruiker niets doet zonder te communiceren met de LAP voor de hoeveelheid tijd die is ingesteld als User Idle Time-out, wordt de client gedeauthenticeerd

door de WLC. De client moet opnieuw authenticeren en opnieuw koppelen aan de WLC. Het wordt gebruikt in situaties waar een client kan uitvallen van de bijbehorende LAP zonder de LAP te verwittigen. Dit kan gebeuren als de batterij op de client leeg raakt of als de client-partners weggaan.

Opmerking: Ga naar het menu **Controller** om toegang te krijgen tot ARP en User Idle Time-out op de WLC GUI. Kies **Algemeen** aan de linkerkant om de velden ARP en User Idle Time-out te vinden.

De Session Time-out is de maximale tijd voor een clientsessie met de WLC. Na deze tijd, WLC de-authenticeert de client, en de client gaat opnieuw door het gehele authenticatie (re-authenticatie) proces. Dit maakt deel uit van een veiligheidsvoorschrift voor het draaien van de coderingssleutels. Als u een EAP-methode (Extensible Verification Protocol) met sleutelbeheer gebruikt, gebeurt het opnieuw instellen op elk regelmatig interval om een nieuwe coderingssleutel af te leiden. Zonder key management is deze time-outwaarde de tijd die draadloze clients nodig hebben om een volledige herverificatie uit te voeren. De sessietime-out is specifiek voor het WLAN. Deze parameter kan worden benaderd via het menu **WLAN's > Bewerken**.

V. Wat is een RFID-systeem? Welke RFID-tags worden momenteel ondersteund door Cisco?

A. Radio Frequency Identification (RFID) is een technologie die gebruik maakt van radiofrequentiecommunicatie voor een vrij korte-afstandscommunicatie. Een RFID-basissysteem bestaat uit RFID-tags, RFID-lezers en de verwerkingssoftware.

Momenteel ondersteunt Cisco RFID-tags van AeroScout en Pango. Raadpleeg voor meer informatie over het configureren van AeroScout-tags WLC Configuration voor AeroScout RFID-tags.

V. Kan ik EAP-verificatie lokaal uitvoeren op de WLC? Is er een document dat deze functie van Local EAP uitlegt?

A. Ja, EAP-verificatie kan lokaal op de WLC worden uitgevoerd. Local EAP is een verificatiemethode waarmee gebruikers en draadloze clients lokaal op de WLC kunnen worden geverifieerd. Het is ontworpen voor gebruik in externe kantoren die de verbinding met draadloze clients willen behouden wanneer het backend-systeem verstoord raakt of de externe verificatieserver uitvalt. Wanneer u lokale EAP inschakelt, fungeert de WLC als verificatieserver. Raadpleeg voor meer informatie over het configureren van een WLC voor lokale EAP-Fast-verificatie de lokale EAP-verificatie op de draadloze LAN-controller met het configuratievoorbeeld EAP-FAST en LDAP-server.

Q. Wat is de WLAN-overschrijvingsfunctie? Hoe kan ik deze functie configureren? Zullen de LAP's de WLAN-overschrijvingswaarden behouden wanneer ze overschakelen naar de back-up-WLC?

A. De WLAN-overschrijvingsfunctie stelt ons in staat om WLAN's te kiezen uit de WLAN's die op een WLC zijn geconfigureerd die actief op een afzonderlijke LAP-basis kunnen worden gebruikt. Voltooi de volgende stappen om een WLAN-overschrijving te configureren:

1. In de WLC GUI, klik op het menu **Draadloos**.
2. Klik op de optie **Radios** aan de linkerkant en kies **802.11 a/n** of **802.11 b/g/n**.

3. Klik op de koppeling **Configureren** in het vervolgkeuzemenu aan de rechterkant van het toegangspunt dat overeenkomt met de naam van het toegangspunt waarop u de WLAN-override wilt configureren.
4. Kies **Inschakelen** in het vervolgkeuzemenu WLAN-overschrijving. Het menu WLAN-overschrijving is het laatste item aan de linkerkant van het venster.
5. De lijst van alle WLAN's die op de WLC zijn geconfigureerd, wordt weergegeven.
6. Controleer vanuit deze lijst de **WLAN's** die u op de LAP wilt weergeven en klik op **Toepassen** om de wijzigingen door te voeren.
7. Sla uw configuratie op nadat u deze wijzigingen hebt aangebracht.

APs behouden de WLAN-overschrijvingswaarden wanneer ze worden geregistreerd bij andere WLCs, op voorwaarde dat WLAN-profielen en SSID's die u wilt overschrijven worden geconfigureerd over alle WLC's.

Opmerking: in controller-softwarerelease 5.2.157.0 is de WLAN-overschrijvingsfunctie verwijderd uit zowel de controller-GUI als de CLI. Als uw controller is geconfigureerd voor WLAN-overschrijding en u upgrade naar controller-softwarerelease 5.2.157.0, verwijdert de controller de WLAN-configuratie en zendt alle WLAN's uit. U kunt specificeren dat alleen bepaalde WLAN's worden verzonden als u access point groepen configureren. Elk toegangspunt adverteert alleen de ingeschakelde WLAN's die tot de groep van het toegangspunt behoren.

Opmerking: met access point groepen kunnen WLAN's niet worden verzonden op per radio-interface van AP.

V. Wordt IPv6 ondersteund op de Cisco draadloze LAN-controllers (WLC's) en Lichtgewicht access points (LAP's)?

A. Op dit moment ondersteunen de 4400 en 4100 Series controllers alleen IPv6 client passthrough. Native IPv6-ondersteuning wordt niet ondersteund.

Als u IPv6 op de WLC wilt inschakelen, schakelt u het selectievakje **IPv6 Enable** in op de WLAN SSID-configuratie onder de pagina WLAN > Bewerken.

Bovendien is de Ethernet Multicast Mode (EMM) vereist om IPv6 te kunnen ondersteunen. Als u EMM uitschakelt, verliezen clientapparaten die IPv6 gebruiken connectiviteit. Kies **Unicast** of **Multicast** om EMM in te schakelen op de pagina Controller > Algemeen en in het vervolgkeuzemenu Ethernet Multicast Mode. Dit schakelt multicast in Unicast- of Multicastmodus in. Als multicast is ingeschakeld als multicast-unicast, worden pakketten gerepliceerd voor elke AP. Dit kan processor-intensief zijn, dus gebruik het voorzichtig. Multicast die als multicast multicast is ingeschakeld, gebruikt de gebruiker die een multicast adres heeft toegewezen om een traditionelere multicast uit te voeren naar de access points (AP's).

Opmerking: IPv6 wordt niet ondersteund op de controllers van 2006.

Ook is er Cisco bug-id CSCsg78176, die verhindert dat IPv6-passthrough wordt gebruikt wanneer de AAA Override-functie wordt gebruikt.

V. Ondersteuning van Cisco 2000 Series draadloze LAN-controller (WLC) voor webverificatie voor gastgebruikers?

A. Webverificatie wordt ondersteund op alle Cisco WLC's. Web authenticatie is een Layer 3-

verificatiemethode die wordt gebruikt om gebruikers met eenvoudige verificatiereferenties te verifiëren. Er is geen encryptie bij betrokken. Voltooi de volgende stappen om deze functie in te schakelen:

1. Klik vanuit de GUI op het **WLAN-**menu.
2. Klik op een **WLAN**.
3. Ga naar het tabblad **Beveiliging** en kies **Layer 3**.
4. Controleer het vakje **Web Policy** en kies **Verificatie**.
5. Klik op **Toepassen** om de wijzigingen op te slaan.
6. Om een database op de WLC te maken waartegen gebruikers kunnen worden geauthenticeerd, gaat u naar het menu **Security** op de GUI, kiest u **Local Net User** en voltooit u deze acties: Definieer de gebruikersnaam en het wachtwoord voor de gast die gebruikt moet worden om in te loggen. Deze waarden zijn hoofdlettergevoelig.Kies de WLAN-id die u gebruikt.**N.B.:** Raadpleeg voor een gedetailleerdere configuratie het configuratievoorbeeld van de draadloze LAN-controller voor de webverificatie.

V. Kan de WLC worden beheerd in draadloze modus?

A. WLC kan worden beheerd via de draadloze modus zodra deze is ingeschakeld. Raadpleeg voor meer informatie over het inschakelen van de draadloze modus het gedeelte *Draadloze verbindingen inschakelen op de GUI en CLI* van de Configuratiehandleiding voor draadloze LAN-controllers van Cisco, release 7.0.16.0.

Q. Wat is Link Aggregation (LAG)? Hoe schakel ik LAG in op draadloze LAN-controllers (WLC's)?

A. LAG bundelt alle poorten op de WLC in één EtherChannel-interface. Het systeem beheert dynamisch de taakverdeling en poortredundantie met LAG.

Over het algemeen heeft de interface op de WLC meerdere parameters die er aan gekoppeld zijn, waaronder het IP-adres, de standaard-gateway (voor het IP-subnet), de primaire fysieke poort, de secundaire fysieke poort, VLAN-tag en DHCP-server. Wanneer LAG niet wordt gebruikt, wordt elke interface meestal toegewezen aan een fysieke poort, maar er kunnen ook meerdere interfaces worden toegewezen aan één WLC-poort. Wanneer LAG wordt gebruikt, brengt het systeem de interfaces dynamisch in kaart aan het geaggregeerde poortkanaal. Dit helpt bij poortredundantie en taakverdeling. Wanneer een poort uitvalt, wordt de interface dynamisch toegewezen aan de volgende fysieke poort die beschikbaar is, en worden LAP's over poorten gebalanceerd.

Wanneer LAG op een WLC wordt toegelaten, door:sturen WLC gegevenskaders op de zelfde haven waarop zij werden ontvangen. WLC vertrouwt op de buurtverbinding switch om het verkeer over EtherChannel in balans te brengen. De WLC voert op zichzelf geen EtherChannel-taakverdeling uit.

V. Welke modellen van Wireless LAN Controllers (WLC's) ondersteunen Link Aggregation (LAG)?

A. Cisco 5500 Series controllers ondersteunen LAG in softwarerelease 6.0 of hoger, Cisco 4400 Series controllers ondersteunen LAG in softwarerelease 3.2 of hoger, en LAG wordt automatisch ingeschakeld op de controllers binnen Cisco WiSM en Catalyst 3750G geïntegreerde draadloze

LAN-controller Switch. Zonder LAG ondersteunt elke distributiesysteem-poort op een Cisco 4400 Series controller maximaal 48 access points. Als LAG is ingeschakeld, ondersteunt de logische poort van een Cisco 4402 Controller maximaal 50 access points, de logische poort van een Cisco 4404 Controller maximaal 100 access points, en de logische poort op de Catalyst 3750G geïntegreerde draadloze LAN controller Switch en op elke Cisco WiSM controller ondersteunt maximaal 150 access points.

Cisco 2106 en 2006 WLC's ondersteunen LAG niet. Eerdere modellen, zoals Cisco 4000 Series WLC, ondersteunen LAG niet.

V. Wat is de auto-anker mobiliteitsfunctie in Unified Wireless Networks?

A. De auto-ankermobiliteit (of de gast WLAN-mobiliteit) wordt gebruikt om de taakverdeling en beveiliging voor zwervende clients op uw draadloze LAN's (WLAN's) te verbeteren. Onder normale zwervende omstandigheden sluiten clientapparaten zich aan bij een WLAN en worden ze verankerd aan de eerste controller waarmee ze contact opnemen. Als een client naar een andere subnetverbinding zwerft, stelt de controller waaraan de client zwerft een buitenlandse sessie in voor de client met de ankercontroller. Met het gebruik van de auto-anker mobiliteitsfunctie, kunt u een controller of een set controllers als ankerpunten voor clients op een WLAN specificeren.

Opmerking: het mobiliteitshanker mag niet worden geconfigureerd voor Layer 3-mobiliteit. Het mobiliteitshanker wordt alleen gebruikt voor het tunnelen van gasten.

V. Kan een Cisco 2006 draadloze LAN-controller (WLC) worden geconfigureerd als anker voor een WLAN?

A. Een Cisco 2000 Series WLC kan niet worden aangewezen als anker voor een WLAN. WLAN's die op een Cisco 2000 Series WLC zijn gemaakt, kunnen echter een Cisco 4100 Series WLC en Cisco 4400 Series WLC als anker hebben.

V. Welk type mobiliteitstunneling gebruikt de draadloze LAN-controller?

A. Controller-softwarereleases 4.1 tot en met 5.1 ondersteunen zowel asymmetrische als symmetrische mobiliteitstunneling. Controller softwarerelease 5.2 of hoger ondersteunen alleen symmetrische mobiliteitstunneling, die nu altijd standaard is ingeschakeld.

Bij asymmetrische tunneling wordt het clientverkeer naar het bekabelde netwerk rechtstreeks via de buitenlandse controller gerouteerd. Asymmetrische tunneling breekt wanneer een upstream router reverse path filtering (RPF) ingeschakeld heeft. In dit geval wordt het clientverkeer op de router verbroken omdat de PDF-controle ervoor zorgt dat het pad naar het bronadres overeenkomt met het pad waar het pakket vandaan komt.

Wanneer symmetrische mobiliteitstunneling is ingeschakeld, wordt al het clientverkeer naar de ankercontroller verzonden en kan de RPF-controle met succes worden doorstaan. Symmetrische mobiliteitstunneling is ook nuttig in deze situaties:

- Als een firewallinstallatie in het clientpakketpad pakketten laat vallen omdat het IP-bronadres niet overeenkomt met het subnetbestand waarop de pakketten worden ontvangen, is dit nuttig.
- Als de toegangsgroep VLAN op de ankercontroller anders is dan de WLAN-interface VLAN op de buitenlandse controller: in dit geval kan clientverkeer op een onjuist VLAN worden

verzonden tijdens mobiliteitsgebeurtenissen.

V. Hoe hebben we toegang tot de WLC wanneer het netwerk is uitgeschakeld?

A. Wanneer het netwerk neer is, kan WLC door de de diensthaven worden betreden. Deze poort krijgt een IP-adres toegewezen in een heel ander subnetnummer dan andere poorten van de WLC en wordt dus out-of-band beheer genoemd. Raadpleeg het gedeelte *Poorten en interfaces configureren* in de configuratiehandleiding voor draadloze LAN-controllers van Cisco, release 7.0.16.0, voor meer informatie.

V. Ondersteuning van Cisco Wireless LAN-controllers (WLC's) voor de failover (of redundantie)-functie?

A. Ja, als u twee of meer WLCs in uw WLAN-netwerk hebt, kunt u deze voor redundantie configureren. Over het algemeen, sluit een LAP zich aan bij de gevormde primaire WLC. Zodra de primaire WLC faalt, start de LAP opnieuw op en sluit hij zich aan bij een andere WLC in de mobiliteitsgroep. Failover is een functie waarbij de LAP-opiniepeilingen voor de primaire WLC en de primaire WLC aansluiten zodra deze functioneel is. Raadpleeg de WLAN-controller-failover voor het configuratievoorbeeld van lichtgewicht access points voor meer informatie.

V. Wat is het gebruik van toegangscontrolelijsten (ACL's) met voorafgaande verificatie in draadloze LAN-controllers (WLC's)?

A. Met pre-authenticatie ACL, zoals de naam impliceert, kunt u clientverkeer van en naar een specifiek IP-adres toestaan, zelfs voordat de client verificatie uitvoert. Wanneer u een externe webserver voor webverificatie gebruikt, hebben sommige WLC-platforms een pre-authenticatie ACL nodig voor de externe webserver (de Cisco 5500 Series controller, een Cisco 2100 Series controller, Cisco 2000 Series en de controller-netwerkmodule). Voor de andere WLC-platforms is de pre-authenticatie ACL niet verplicht. Het is echter een goede praktijk om een pre-authenticatie ACL voor de externe webserver te configureren wanneer externe webverificatie wordt gebruikt.

Q. Ik heb een MAC-gefilterd WLAN en een volledig open WLAN in mijn netwerk. Selecteert de client standaard het geopende WLAN? Of associeert de client automatisch met de WLAN-id die op het MAC-filter is ingesteld? Ook, waarom is er een "interface"optie op een filter van MAC?

A. De client kan worden gekoppeld aan elk WLAN waarmee de client wordt geconfigureerd om verbinding te maken. De interfaceoptie in het filter van MAC geeft de capaciteit om de filter op of WLAN of een interface toe te passen. Als meerdere WLAN's aan dezelfde interface zijn gekoppeld, kunt u de MAC-filter op de interface toepassen zonder dat u voor elk WLAN een filter hoeft te maken.

V. Hoe kan ik TACACS-verificatie configureren voor beheergebruikers op de draadloze LAN-controller (WLC)?

A. Vanaf WLC versie 4.1 wordt TACACS ondersteund op de WLC's. Raadpleeg TACACS+ configureren om te begrijpen hoe u TACACS+ configureert om beheergebruikers van de WLC te verifiëren.

V. Wat is het gebruik van de instelling voor buitensporige verificatiefouten in een draadloze LAN-controller (WLC)?

A. Deze instelling is een van de regels voor de uitsluiting van clients. De uitsluiting van de client is een beveiligingsfunctie op de controller. Het beleid wordt gebruikt om klanten op een zwarte lijst te zetten om illegale toegang tot het netwerk of aanvallen op het draadloze netwerk te voorkomen.

Als dit excessieve web authenticatie failpolicy is ingeschakeld, wanneer het aantal mislukte web authenticatie pogingen van een client groter is dan 5, is de controller van mening dat de client de maximale pogingen voor web authenticatie heeft overschreden en de client heeft geblokkeerd.

Voltooi de volgende stappen om deze instelling in of uit te schakelen:

1. Ga vanuit de WLC GUI naar **Security > Wireless Protection Policies > Clientuitsluitingsbeleid**.
2. **Excessieve webverificatiefouten** controleren of uitschakelen.

Q. Ik heb mijn autonome access point (AP) geconverteerd naar de lichtgewicht modus. In de Lichtgewicht AP Protocol (LWAPP) modus met de AAA RADIUS server voor client accounting wordt de client normaal gesproken gevolgd met RADIUS accounting op basis van het IP-adres van de WLC. Is het mogelijk om de RADIUS-accounting in te stellen op basis van het MAC-adres van de AP die gekoppeld is aan die WLC en niet op basis van het IP-adres van de WLC?

A. Ja, dit kan met de WLC zijconfiguratie worden gedaan. Voer de volgende stappen uit:

1. Van de controller GUI, onder **Security > Radius Accounting**, is er een uitrolvak voor Call Station ID Type. Kies **MAC-adres AP**.
2. Controleer dit via het LWAP AP-logbestand. Daar kunt u het veld met de naam-station-ID zien dat het MAC-adres weergeeft van het toegangspunt waaraan de betreffende client is gekoppeld.

V. Hoe wijzigt u de WPA-waarde (Wi-Fi Protected Access) voor uitschakelvertraging op een draadloze LAN-controller (WLC) via CLI? Ik weet dat ik dit op Cisco IOS® Access points (AP's) kan doen met de opdracht voor de tijdelijke *waarde van* dot11 wpa-handshake, maar hoe voert u dit uit op een WLC?

A. Het vermogen om de WPA-Handshake timeout te configureren door middel van de WLC's was geïntegreerd in softwarerelease 4.2 en hoger. U hebt deze optie niet nodig in eerdere WLC-softwareversies.

Deze opdrachten kunnen worden gebruikt om de WPA-handshake-time-out te wijzigen:

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

De standaardwaarden blijven op het huidige gedrag van WLCs wijzen.

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

Opmerking: op IOS AP's is deze instelling configureerbaar met de opdracht **dot11 wpa handshake**.

U kunt ook de andere EAP-parameters configureren met de opties onder de opdracht **Geavanceerd tap configureren**.

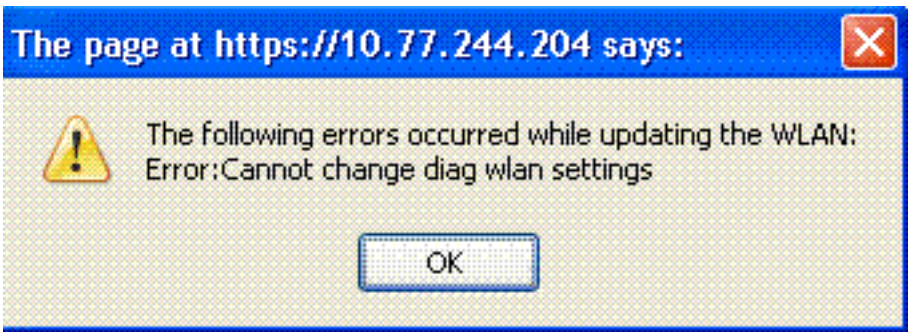
```
(Cisco Controller) >config advanced eap ?

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.
```

Q. Wat is het doel van de kenmerkende kanaaleigenschap in WLAN > Bewerken > Geavanceerde pagina?

A. De diagnostische kanaalfunctie stelt u in staat problemen met betrekking tot clientcommunicatie met een WLAN op te lossen. De client en access points kunnen door middel van een gedefinieerde set tests worden geplaatst om de oorzaak van communicatieproblemen die de klant ervaart te identificeren en vervolgens corrigerende maatregelen toe te staan om de client operationeel te maken op het netwerk. U kunt de controller GUI of CLI gebruiken om het diagnosekanaal in te schakelen, en u kunt de controller CLI of WCS gebruiken om de diagnostische tests uit te voeren.

Het diagnosekanaal kan alleen worden gebruikt om te testen. Als u probeert verificatie of codering voor het WLAN te configureren met het diagnostische kanaal ingeschakeld, ziet u deze fout:



Q. Wat is het maximumaantal AP Groepen dat op een WLC kan worden gevormd?

A. Deze lijst toont het maximumaantal AP groepen dat u op een WLC kunt vormen:

- Een maximum van 50 access point groepen voor de Cisco 2100 Series controller- en

controller-netwerkmodules
- Maximum aantal 300 access point groepen voor de Cisco 4400 Series controllers, Cisco WiSM en Cisco 3750G draadloze LAN-controller Switch
- Maximum aantal 500 access point groepen voor Cisco 5500 Series controllers

Gerelateerde informatie

- Veelgestelde vragen over wireless LAN-controller (WLC)
- Fout en systeemmeldingen van draadloze LAN-controller (WLC) FAQ
- Lichtgewicht access point Veelgestelde vragen
- Configuratiehandleiding voor Cisco draadloze LAN-controllers, release 7.0.16.0
- IPv6-ondersteuning op de draadloze LAN-controller
- Ondersteuning voor wireless producten
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.