Veelgestelde vragen over draadloze gasttoegang

Inhoud

Inleiding

Dit document bevat informatie over de meest gestelde vragen (FAQ's) over de functie Draadloze gasttoegang, die deel uitmaakt van het Unified draadloze Cisco-netwerk.

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

Wat is een Ethernet over IP (EoIP)-tunnel naar het onbeveiligde netwerkgebied?

Cisco raadt het gebruik van een controller aan voor gastenverkeer. Deze controller staat bekend als de gastankercontroller.

De gastankercontroller bevindt zich meestal in een onbeveiligd netwerkgebied, vaak de gedemilitariseerde zone (DMZ) genoemd. Andere interne WLAN-controllers waar het verkeer vandaan komt, bevinden zich in de ondernemings-LAN. Er wordt een EoIP-tunnelverbinding tot stand gebracht tussen de interne WLAN-controllers en de gastankercontroller om ervoor te zorgen dat het gastenverkeer van het bedrijfsgegevensverkeer wordt geïsoleerd. Path isolation is een kritieke beveiligingsbeheerfunctie voor gasttoegang. Het zorgt ervoor dat het beleid van de veiligheid en van de kwaliteit van de dienst (QoS) afzonderlijk kan zijn, en tussen gastverkeer en collectief of intern verkeer onderscheiden.

Een belangrijke eigenschap van de Cisco Unified Wireless Network-architectuur is de mogelijkheid om een EoIP-tunnel te gebruiken om een of meer geleverde WLAN's (dwz, SSID's) statisch in kaart te brengen naar een specifieke gastankercontroller binnen het netwerk. Al het verkeer - zowel van als naar een in kaart gebracht WLAN - passeert een statische EoIP-tunnel die is ingesteld tussen een externe controller en de gastankercontroller.

Met behulp van deze techniek kan al het hieraan gekoppelde gastenverkeer op transparante wijze over het ondernemingsnetwerk worden getransporteerd naar een gastankercontroller die zich in het onbeveiligde netwerkgebied bevindt.

Hoe kies ik de juiste controller die als gast ankercontroller moet worden ingezet?

De selectie van de gastankercontroller is een functie van de hoeveelheid gastverkeer zoals gedefinieerd door het aantal actieve gastclientsessies, of zoals gedefinieerd door de uplink-interfacecapaciteit op de controller, of beide.

De totale doorvoersnelheid en clientbeperkingen per gastankercontroller zijn als volgt:

- Cisco 2504 draadloze LAN-controller - 4 * 1 Gbps interfaces en 1000 gastclients
- Cisco 5508 draadloze LAN-controller (WLC) - 8 Gbps en 7.000 gastclients
- Cisco Catalyst 6500 Series draadloze servicesmodule (WiSM-2) - 20 Gbps en 15.000 clients

- Cisco 8500 draadloze LAN-controller (WLC) - 10 Gbps en 64.000 clients

  Opmerking: Cisco 7500 WLC's kunnen niet worden geconfigureerd als gastankercontroller. Raadpleeg Welke controllers kunnen worden gebruikt om gasttoegang in het onbeveiligde netwerkgebied te ondersteunen? voor de lijst met WLC's die gastankerfuncties ondersteunen.

Er kunnen maximaal 2048 gastgebruikersnamen en wachtwoorden worden opgeslagen in de database van elke controller. Daarom als het totale aantal actieve gastreferenties dit aantal overschrijdt, zal meer dan één controller nodig zijn. U kunt de referenties ook opslaan in een externe RADIUS-server.

Het aantal toegangspunten in het netwerk heeft geen invloed op de selectie van de gastankercontroller.

Hoeveel Ethernet over IP-tunnels (EoIP) kunnen op een gastankercontroller worden afgesloten?

Een gastankercontroller kan tot 71 EoIP-tunnels van interne WLAN-controllers beëindigen. Deze capaciteit is gelijk aan elk model van de Cisco draadloze LAN-controller behalve WLC-2504. De 2504 controller kan tot 15 EoIP-tunnels beëindigen. Meer dan één gastankercontroller kan worden geconfigureerd als er extra tunnels nodig zijn.

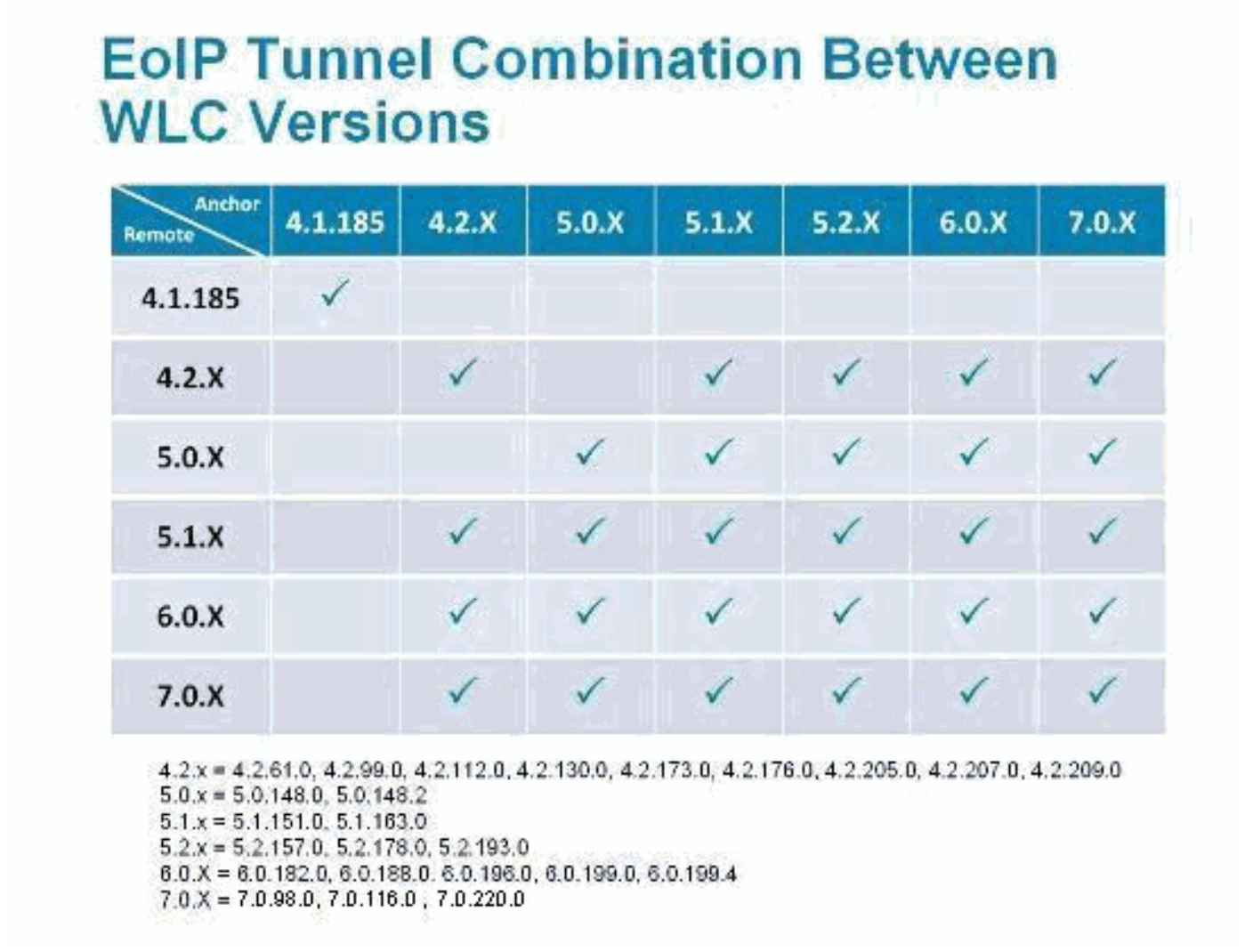
EoIP-tunnels worden geteld per WLAN-controller, onafhankelijk van het aantal getunnelde WLAN's of Secure Set Identifiers (SSID's) in elke EoIP.

Er is één EoIP-tunnel geconfigureerd tussen de gastankercontroller en elke interne controller die toegangspunten ondersteunt met gastclientassociaties.

Kan ik Ethernet over IP (EoIP)-tunnels maken tussen controllers die verschillende softwareversies uitvoeren?

Niet alle softwareversies voor draadloze LAN-controllers ondersteunen dit. In dergelijke gevallen zou de afstandsbediening en ankercontroller dezelfde versie van WLC-software moeten draaien. Echter, de recente softwareversies maken het mogelijk dat de afstandsbediening en ankerbesturing verschillende versies hebben.

Deze matrix maakt een lijst van de softwareversies van de draadloze LAN-controller waarmee u de EoIP-tunnels kunt maken.



Kan de Cisco 2100/2500 Series draadloze LAN-controller worden gebruikt als gastankercontroller in het onbeveiligde netwerkgebied?

Ja, vanaf Cisco Unified Wireless Network Software release 7.4 kan de Cisco 2500 Series draadloze LAN-controller het gastenverkeer (tot 15 EoIP-tunnels) buiten de firewall beëindigen. De Cisco 2000 Series draadloze LAN-controller kan alleen afkomstig zijn van gasttunnels.

Kan de Cisco draadloze LAN-controllermodule voor geïntegreerde services routers (WLCM of WLCM2) worden gebruikt als gastankercontroller in het onbeveiligde netwerkgebied?

Nee, de WLCM of WLCM2 kunnen geen gasttunnels beëindigen. De WLCM kan alleen gastunnels voortbrengen.

Welke controllers kunnen worden gebruikt om gasttoegang in het onbeveiligde netwerkgebied te ondersteunen?

De ankerfunctie van de gasttunnel, die EoIP tunnelbeëindiging, de authentificatie van het Web, en toegangscontrole van gastcliënten omvat, wordt gesteund in deze Draadloze LAN van Cisco controllerplatforms met Versie 4.0 of recentere softwarebeelden:

- Cisco Catalyst 6500 Series draadloze servicesmodule (WiSM2)
- Cisco WiSM-2 Series draadloze LAN-controller
- Cisco Catalyst 3750G geïntegreerde draadloze LAN-controller
- Cisco 5508 Series draadloze LAN-controller
- Cisco 2500 Series draadloze LAN-controller (ondersteuning geïntroduceerd in softwarerelease 7.4)

Als een gastankercontroller buiten de firewall wordt gebruikt, welke firewallpoorten zijn open voor gastentoegang tot het werk?

Op elke firewall tussen de gastankercontroller en de afstandsbediening moeten deze poorten geopend zijn:

- Verouderde mobiliteit: IP-protocol 97 voor gebruikersgegevensverkeer, UDP-16666
- Nieuwe mobiliteit: UDP-16666 en -16667

Voor optioneel beheer moeten deze firewallpoorten open zijn:

- SSH/Telnet - TCP-poort 22/23
- TFTP - UDP-poort 69
- NTP - UDP-poort 123
- SNMP - UDP-poorten 161 (krijgt en zet) en 162 (vallen)
- HTTPS/HTTP - TCP-poort 443/80
- Syslog - TCP-poort 514
- RADIUS-autorisatie/account UDP-poort 1812 en 1813

Kan het gastverkeer door een firewall met geconfigureerde Network Address Translation (NAT) lopen?

Een één-op-één NAT moet worden gebruikt in de EoIP-tunnel die door een firewall gaat.

In een Anchor - Foreign WLC scenario, welke WLC stuurt de RADIUS-accounting?

In dit scenario, wordt de authentificatie altijd gedaan door het anker WLC. Daarom wordt de boekhouding van RADIUS verzonden door het anker WLC.

> **Opmerking**: in een CWA (Central Web Authentication)- en/of CWA-implementatie (Change of Authorisation) moet RADIUS-accounting worden uitgeschakeld op het anker en alleen worden gebruikt op de Foreign WLC.

De gasttunnel tussen de interne controller en de ankercontroller

mislukt. Ik zie deze logbestanden in de WLC: `mm_listen.c:5373 MM-3-INGELDIG_PKT_RECVD: Ontvangen een ongeldig pakket van 10. 40.220.18. Bronlid:0.0.0.0. Bronlid onbekend.`. Waarom?

U controleert de status van de tunnel vanuit de WLC GUI op de **WLAN-**pagina. Klik op de vervolgkeuzelijst in de buurt van een WLAN en kies **Mobiliteitsankers** die de status van besturings- en gegevenspad bevatten. De foutmelding wordt weergegeven vanwege een van de volgende redenen:

1. De anker en de interne controleurs zijn op verschillende versies van code. Zorg ervoor dat dezelfde versies van de code worden uitgevoerd.
2. Misconfiguraties in de configuratie van het mobiliteitshanker. Controleer dat de DMZ zelf is geconfigureerd als het Mobility-anker en de interne WLC's hebben de DMZ WLC geconfigureerd als het Mobility-anker. Raadpleeg het gedeelte Auto-Anchor Mobility configureren van de Configuratiehandleiding voor draadloze LAN-controllers van Cisco, release 7.0, voor meer informatie over het configureren van het Mobility-anker. Dit zou ertoe leiden dat gastgebruikers het verkeer niet kunnen doorgeven.

In een instelling voor draadloze gasttoegang ontvangen clients het IP-adres niet van de DHCP-server. De Thu Jan 22 16:39:09 2009: XX:XX:XX:XX:XX:XX DHCP-dropping RERESPONSE from Export-Foreign STA-foutmelding verschijnt op de interne controller. Waarom?

In een instelling voor draadloze gasttoegang moeten de DHCP-proxyinstelling in de Guest Anker-controllers en de interne controller overeenkomen. Anders, wordt het DHCP- verzoek van cliënten gelaten vallen en u ziet deze foutenmelding op de interne controlemechanisme:

```
Thu Jan 22 16:39:09 2009: XX:XX:XX:XX:XX:XX  DHCP dropping REPLY from Export-Foreign STA
```

Gebruik deze opdracht om de dhcp proxy instelling op de WLC te wijzigen:

```
(Cisco Controller) >config dhcp proxy ?

enable          Enable DHCP processing's proxy style behaviour.
disable         Disable DHCP processing's proxy style behaviour.
```

Gebruik de **show dhcp proxy** opdracht op beide controllers om te verifiëren dat beide controllers dezelfde DHCP proxy instelling hebben.

```
(Cisco Controller) >show dhcp proxy

DHCP Proxy Behaviour: enabled

(Cisco Controller) >
```

Als het gastverkeer wordt getunneld aan het onbeveiligde netwerkgebied, waar krijgen de gastcliënten een IP adres?

Gastverkeer wordt binnen de onderneming via Layer 3 via EoIP vervoerd. Daarom is het eerste punt waarop de Dynamic Host Configuration Protocol (DHCP)-services kunnen worden geïmplementeerd lokaal op de gastankercontroller, of kan de gastankercontroller client-DHCP-verzoeken doorgeven aan een externe server. Dit is ook de methode waarmee de adresresolutie van Domain Name System (DNS) wordt verwerkt.

Ondersteunt de Cisco draadloze LAN-controller webportalen voor gastenverificatie?

Cisco Wireless LAN-controllers, softwareversie 3.2 of hoger, bieden een ingebouwd webportaal dat gastenreferenties voor verificatie vastlegt en eenvoudige brandingmogelijkheden biedt, samen met de mogelijkheid om disclaimer en acceptabele beleidsinformatie weer te geven.

Hoe pas ik het webportaal aan?

Voor meer informatie over het aanpassen van een webportal, raadpleegt u De aanmeldpagina voor webverificatie kiezen.

Hoe worden gastreferenties beheerd?

Gastreferenties kunnen centraal worden gemaakt en beheerd met Cisco Wireless Control System (WCS) versie 7.0 en Network Control System (NCS) over 1.0. Een netwerkbeheerder kan een beperkt-voorrecht administratief rekening binnen WCS oprichten die "lobbyambassadeur"toegang voor het creëren van gastgeloofsbrieven verleent. In WCS of NCS is de persoon met een lobbyambassadeursaccount in staat om gastreferenties te creëren, toe te wijzen, te controleren en te verwijderen voor de controller die dienst doet als een gastankercontroller.

De lobbyambassadeur kan de gastgebruikersnaam (of gebruiker-ID) en het wachtwoord invoeren, of de referenties kunnen automatisch worden gegenereerd. Er is ook een globale configuratieparameter die het gebruik van één gebruikersnaam en wachtwoord voor alle gasten, of een unieke gebruikersnaam en wachtwoord voor elke gast mogelijk maakt.

Raadpleeg het gedeelte Gastgebruikersaccounts maken van de Cisco Wireless Control System Configuration Guide, release 7.0, voor het configureren van de account van de lobbyambassadeur op de WCS.

Is de lobbyfunctie van de ambassadeur beschikbaar in de Cisco draadloze LAN-controller naast het Wireless Control System (WCS) of NCS?

Ja. Als de WCS of NCS niet wordt geïmplementeerd, kan een netwerkbeheerder een account voor lobbyambassadeurs instellen op de gastankercontroller. Een persoon die inlogt in de gast anker controller met behulp van de lobby ambassadeur account zal alleen toegang hebben tot de gast gebruiker management functies.

Als er meerdere gastankercontrollers zijn, moet een WCS of NCS worden gebruikt om tegelijkertijd gebruikersnamen te configureren op meerdere gastankercontrollers.

Raadpleeg het gedeelte Een ambassadeursaccount maken van een sectie van de configuratiehandleiding voor een draadloze LAN-controller in Cisco, release 7.0, voor informatie over het maken van ambassadeursaccounts met draadloze LAN-controllers.

Kunnen de gasten worden geverifieerd met een externe authenticatie, autorisatie en accounting (AAA) server?

Ja. De verificatieverzoeken van de gast kunnen worden doorgegeven aan een externe RADIUS-server.

Wat gebeurt er als een gast inlogt?

Wanneer een draadloze gast inlogt via het webportaal, behandelt de gastankercontroller de verificatie door deze stappen uit te voeren:

1. De gast anker controller controleert zijn lokale database voor gebruikersnaam en wachtwoord, en als ze aanwezig zijn, verleent toegang.
2. Als er geen gebruikersreferenties lokaal aanwezig zijn op de gastankercontroller, controleert de gastankercontroller de WLAN-configuratie-instellingen om te zien of er een externe RADIUS-server(s) is geconfigureerd voor de gast WLAN. Als dit het geval is, maakt de controller een RADIUS-access-request met de gebruikersnaam en het wachtwoord en stuurt deze door naar de geselecteerde RADIUS-server voor verificatie.
3. Als er geen specifieke RADIUS-servers zijn geconfigureerd voor het WLAN, controleert de controller de wereldwijde instellingen van de RADIUS-serverconfiguratie. Alle externe RADIUS-servers die zijn geconfigureerd met de optie om "netwerkgebruiker" te verifiëren worden gevraagd met de referenties van de gastgebruiker. Anders, als geen servers "netwerkgebruiker" hebben geselecteerd en de gebruiker niet is geverifieerd via stap 1 of 2, zal de verificatie mislukken.

Is het mogelijk om de authenticatie van de gastgebruiker over te slaan en alleen de webpagina-disclaimer optie weer te geven?

Ja. Een andere configuratieoptie van draadloze gasttoegang is om gebruikersverificatie volledig te omzeilen en open toegang toe te staan. Het kan echter nodig zijn om een beleid voor acceptabel gebruik en een disclaimer-pagina aan gasten voor te stellen voordat toegang wordt verleend. Om dit te doen, kan een gast WLAN worden geconfigureerd voor webbeleid passthrough. In dit scenario wordt een gastgebruiker omgeleid naar een webpagina die disclaimer-informatie bevat. Om identificatie van de gastgebruiker mogelijk te maken, heeft de passthrough-modus ook een optie voor een gebruiker om een e-mailadres in te voeren voordat hij verbinding maakt.

Moeten we de afstandsbediening en de ankercontroller op de gast in dezelfde mobiliteitsgroep hebben?

Nee. De gastankercontroller en de afstandsbediening kunnen op afzonderlijke mobiliteitsgroepen staan.

Als er meer dan één gast SSID is, kan elk WLAN (SSID) worden geleid naar een uniek webpagina portal?

Ja. Al het gastverkeer, of op één of meerdere WLAN's, wordt omgeleid naar één webpagina. Vanaf WLC versie 4.2 of hoger kan elk WLAN worden doorgestuurd naar een unieke webpagina van een webportal. Raadpleeg de sectie Toewijzen aan aanmelding, inlogfout en inlogpagina's per WLAN van de configuratiehandleiding voor Cisco draadloze LAN-controllers, release 7.0.

Wat is de functionaliteit van de nieuwe instelling in de WLC release 7.0, WebAuth on Mac Filter Failure?

Als een WLAN zowel een Layer 2 (mac-filter) als Layer 3-beveiliging (webauth-on-macfilter-fout) heeft geconfigureerd, `beweegt` de client zich om de status `RUN` te `starten` als een van beide wordt doorgegeven. En als Layer 2 security (mac-filter) mislukt, wordt de client verplaatst naar Layer 3 security (webauth-on-macfilter-fout).

Werkt de client correct als de browser is geconfigureerd voor een proxyserver?

Voorafgaand aan release 7.0 kon client geen TCP-verbinding tot stand brengen wanneer proxyserver in de browser was geconfigureerd. Na release 7.0 wordt deze Webex Proxy-serverondersteuning toegevoegd en kunnen het IP-adres en de poort van de Proxyserver op de controller worden geconfigureerd.

Is er een implementatiegids voor draadloze gasttoegang?

Dit is de link naar de implementatiegids:

Implementatiegids: Cisco Guest Access met de Cisco draadloze LAN-controller

Is er een ontwerpgids voor bekabelde en draadloze gasttoegang?

Dit zijn de links naar de ontwerphandleidingen:

- Cisco Unified draadloze gasttoegangsservices
- Configuratie-voorbeeld van bekabelde gasttoegang met Cisco WLAN-controllers

Gerelateerde informatie

- Configuratie-voorbeeld van bekabelde gasttoegang met Cisco WLAN-controllers
- Implementatiegids: Cisco Guest Access met de Cisco draadloze LAN-controller, release 4.1
- 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.