Installatie-handleiding voor binnengebruik

Inhoud

Inleiding

Het lichtgewicht access point 1242/1131 is een twee-radio Wi-Fi infrastructuurapparaat voor geselecteerde indoor implementaties. Het is een Lichtgewicht Access Point Protocol (LWAPP)-gebaseerd product. Het levert een 2,4 GHz radio en een 5,8 GHz radio die compatibel is met 802.11b/g en 802.11a. Eén radio kan worden gebruikt voor lokale (client) toegang voor het access point (AP) en de tweede radio kan worden ingesteld voor draadloze backhaul. LAP1242/LAP131 ondersteunt P2P, P2MP en het maastype van architecturen.

Lees de handleiding door voordat u een van de installaties probeert.

In dit document wordt de implementatie van Enterprise Wireless mesh voor binnenvermaasd beschreven. Dit document maakt het voor draadloze eindgebruikers mogelijk de fundamentele waarden van mesh binnenin te begrijpen, waar u de binnenste netten kunt configureren en de binnenste netten kunt configureren. Indoor mesh is een subset van Cisco Enterprise Wireless mesh die wordt uitgevoerd met draadloze controllers en lichtgewicht AP's.

Indoor mesh is een subset van de Enterprise mesh-architectuur die op Unified draadloze architectuur wordt toegepast. Vandaag de dag is er sprake van een maaswijdte binnen de deur. Met een indoor-mesh wordt een van de radio's (meestal 802.11b/g) en/of de bekabelde Ethernet-link gebruikt om verbinding te maken met klanten, terwijl de tweede radio (meestal 802.11a) wordt gebruikt om clientverkeer te backhaul. De backhaul kan één hop zijn of meerdere hop. Indoor mesh brengt u deze waarden naar binnen:

- Niet hoeft Ethernet bedrading aan elke AP uit te voeren.
- Ethernet switch poort is niet vereist voor elke AP.
- Netwerkconnectiviteit waar draden geen connectiviteit kunnen bieden.
- Flexibiliteit in implementatie - niet beperkt tot 100 m van een Ethernet switch.
- Eenvoudig te implementeren een ad-hoc draadloos netwerk.

De grootwinkelbedrijven worden door de kostenbesparingen op de bedrading en om de eerder genoemde redenen sterk aangetrokken tot binnenmaaswijdten.

Inventaris specialisten gebruiken dit in het maken van inventarislijsten voor detailhandelaren, fabrieken en andere bedrijven. Ze willen snel een tijdelijk WiFi-netwerk op een klantensite inzetten om real-time connectiviteit voor hun handheld-apparaten mogelijk te maken. Educatieve seminars, conferenties, productie en gastvrijheid zijn enkele van de plekken waar binnenmaasarchitectuur nodig is.

Wanneer u deze gids hebt gelezen, zult u begrijpen waar te gebruiken en hoe te om binnenkorrelgrootte te vormen. U zult ook begrijpen dat de binnenmazen in NEMA-behuizingen GEEN vervanging voor outdoorvermaasingen zijn. Verder zult u ook de superioriteit van binnenvermaasd over de flexibiliteit van de verbindingsrol (enkel hopvermaasd) begrijpen die door autonome APs wordt gebruikt.

Aannames:

U hebt kennis van Cisco Unified Wireless Network, architectuur en producten. U hebt kennis van

Cisco mesh-producten voor buitengebruik en een aantal van de terminologie die wordt gebruikt voor netwerken met een netwerk.

Lijst van termen	
LWAPP	Lichtgewicht access point protocol - het protocol voor het controleren en afstemmen van gegevens tussen AP's en de draadloze LAN-controller.
WLAN-controller/controller/WLC	Draadloze LAN-controller - Cisco-apparaten die het netwerkbeheer van een WLAN centraliseren en vereenvoudigen door een groot aantal beheerde end-points in één enkel, uniform systeem in te vouwen, waardoor een uniform intelligent WLAN-netwerksysteem met informatie wordt ingeschakeld.
RAP	Root Access point/router-access point - Cisco draadloze apparaten fungeren als brug tussen de controller en andere draadloze AP's. AP's die verbonden zijn aan de controller.
MAP	korrelgrootte APs - Cisco draadloos apparaat dat op een RAP of een MAP via de lucht op een radio 802.11a en ook servicecontracten op een radio 802.11b/g aansluit.
ouder	Een AP (of een RAP/MAP) dat toegang tot andere APs over de lucht op een radio 802.11a verleent.
buurvrouw	Alle AP's in een netwerk van mesh zijn buren en hebben buren. RAP heeft geen buurman aangezien het is aangesloten op de controller.
Kinderkind	Een AP verder van de controller is altijd een kind. Een kind zal één ouder en

	veel buren in een vermaasd netwerk hebben. Als de ouder sterft, wordt de volgende buurman met de beste gemakwaarde gekozen ouder.
SNR	Verhouding signaal-tot-geluid
BGN	Naam van bridge-groep
MAART	Uitbreidbaar verificatieprotocol
PSK	Voorgedeelde sleutel
AWPP	Adaptief draadloos Path-protocol

Overzicht

Het Cisco Indoor mesh Network Access Point is een twee-radio Wi-Fi infrastructuurapparaat voor geselecteerde indoor-implementaties. Het is een Lichtgewicht Access Point Protocol (LWAPP)-gebaseerd product. Het levert een 2,4 GHz radio en een 5,8 GHz radio die compatibel is met 802.11b/g, 802.11a standaarden. Eén radio (802.11b/g) kan worden gebruikt voor lokale (client)toegang voor de AP en de tweede radio (802.11a) kan worden ingesteld voor draadloze backhaul. Het voorziet in een binnenmaasarchitectuur, waar verschillende knooppunten (radio's) met elkaar praten via backhaul en ook lokale clienttoegang bieden. Deze AP kan ook worden gebruikt voor point-to-point en point-to-multipoint bridging architecturen. De oplossing voor draadloos mesh-netwerk is ideaal voor grote indoor dekking, aangezien u hoge gegevenssnelheden en een goede betrouwbaarheid kunt hebben met een minimale infrastructuur. Dit zijn de belangrijkste functies die bij de eerste release van dit product zijn geïntroduceerd:

- In een binnenomgeving gebruikt voor 3 hoptellingen. Maximaal 4.
- Relay-knooppunt en -host voor eindgebruikers. Een 802.11a-radio wordt gebruikt als een backhaul-interface en een 802.11b/g-radio voor klantenservice.
- Beveiliging van AP's binnen de maaswijdte - EAP en PSK ondersteund.
- De LWAPP MAP's in een vermaasde omgeving communiceren met de controllers op dezelfde manier als met Ethernet-verbonden AP's.
- Draadloze point-to-point overbrugging.
- Draadloze point-to-multipoint overbrugging.
- Optimale selectie van ouders. SNR, EASE en BGN
- BGN-verbeteringen. NULL en standaard modus.
- Lokale toegang.
- zwarte lijst van ouders. Uitsluitingslijst.
- Zelfherstel met AWPP.
- Ethernet-overbrugging.
- Basissteun van Voice uit de 4.0 release.
- Selectie van dynamische frequentie.
- Anti-strand - standaard BGN en DHCP-failover.

Opmerking: deze functies worden niet ondersteund:

- 4,9 GHz openbaar veiligheidskanaal
- Routing rond interferentie
- Background-scannen
- Universele toegang
- Ondersteuning van werkgroepbridge

Software voor binnenmesh

Software binnen is een speciale release aangezien deze is gericht op AP's binnen, met name binnenshuis. In deze release werken zowel de binnenste AP's in de lokale modus als in de brugmodus. Sommige functies die beschikbaar zijn in de release 4.1.17.0 worden niet in deze release geïmplementeerd. Er zijn verbeteringen aangebracht in de opdrachtregel interface (CLI), grafische gebruikersinterface (GUI - webbrowser) en op de staatsmachine zelf. Het doel van deze verbeteringen is om vanuit uw oogpunt waardevolle informatie te verkrijgen over dit nieuwe product en de functionele levensvatbaarheid ervan.

Specifieke verbeteringen van binnenwateren:

- **Indoor Environment** - Indoor mesh wordt geïmplementeerd met behulp van LAP1242s en LAP1131. Deze worden geïmplementeerd in omgevingen binnenshuis waar Ethernet-kabel niet beschikbaar is. De implementatie is eenvoudig en sneller om een draadloze dekking te bieden aan afgelegen gebieden in het gebouw (bijvoorbeeld kleinhandelsdistributiecentra, onderwijs voor seminars/conferenties, productie, ziekenhuizen).
- **Verbeteringen in Bridge Group Name (BGN)** - Om een netwerkbeheerder in staat te stellen een netwerk van mesh AP's binnen een netwerk te organiseren in een door gebruikers opgegeven sector, biedt Cisco een mechanisme dat Bridge Group Name wordt genoemd, of BGN. De BGN, echt de sectornaam, zorgt ervoor dat een AP zich verbindt met andere AP's met dezelfde BGN. Als AP geen geschikte sector vindt die zijn BGN aanpast, werkt AP in standaardmodus, en verkiest AP de beste ouder die op de standaard BGN reageert. Deze optie heeft al veel waardering vanuit het veld gekregen omdat hij zich inzet tegen de gestrande AP-omstandigheden (als iemand de BGN niet heeft geconfigureerd). In de 4.1.171.0 softwarerelease, werken APs, wanneer het gebruik van de standaard BGN, niet als binnenshuis vermaasd knooppunt en heeft geen clienttoegang. Het is in de onderhoudsmodus om toegang te krijgen via de controller en als de beheerder de BGN niet repareert, wordt het AP na 30 minuten opnieuw opgestart.
- **Verbeteringen** in **beveiliging** - security in binnenvermaasde code wordt standaard ingesteld voor EAP (Extensible Authentication Protocol). Dit wordt gedefinieerd in RFC3748. Hoewel het EAP-protocol niet beperkt is tot draadloze LAN's en kan worden gebruikt voor bekabelde LAN-verificatie, wordt het meestal gebruikt in draadloze LAN's. Wanneer EAP wordt ingeroepen door een 802.1X-ingeschakeld NAS-apparaat (Network Access Server), zoals een 802.11a/b/g draadloos access point, kunnen moderne EAP-methoden een veilig verificatiemechanisme bieden en een veilige PMK (Pair-wise Master Key) tussen de client en NAS tot stand brengen. PMK kan vervolgens worden gebruikt voor de draadloze encryptie-sessie die TKIP of CCMP (gebaseerd op AES) gebruikt.Vóór de softwarerelease 4.1.171.0 gebruikten AP's met een buitenmaas PMK/BMK om zich aan te sluiten bij de controller. Dit was een proces met drie cycli. Nu worden de cycli verkort voor een snellere convergentie.Het algemene doel van de beveiliging van binnennetten is:Aanraakconfiguratie op nul zetten voor voorzieningszekerheid.Privacymelding en verificatie voor gegevensframes.Wederzijdse authenticatie tussen het netwerk en de knooppunten.Mogelijkheid om standaardMAP-methoden te gebruiken voor de authenticatie van de AP-knooppunten van

binnenmazen.Ontkoppeling van LWAPP en beveiliging van de binnenmaas.De ontdekking, routing en syncing worden verbeterd van de huidige architectuur om de vereiste elementen aan te passen ter ondersteuning van de nieuwe beveiligingsprotocollen.AP's met binnenkorrelgrootte ontdekken andere access points door te scannen en te luisteren naar onnodige buurupdates van andere mesh AP's. Elke RAP of binnenste MAPs die aangesloten zijn op het netwerk adverteert kernveiligheidsparameters in hun NEIGH_UPD frames (veel zoals 802.11 baken frames).Zodra deze fase voorbij is, wordt een logisch verband tussen een binnenvermaasde AP en wortelAP tot stand gebracht.

- **Verbeteringen in WCS**Binnenverlichting is toegevoegd.binnenste mesh kan worden gegenereerd met hoptelling, ergste SNR, enz.De verbindingstest (ouder-aan-Kind, Kind-aan-Ouder) kan tussen de knopen worden uitgevoerd die zeer intelligente informatie toont.De informatie van AP wordt weergegeven is veel meer dan de eerdere.Je kunt ook de potentiële buren bekijken.Het toezicht op de gezondheid is verbeterd en gemakkelijker toegankelijk.

Ondersteunde hardware en software

Voor binnenmaaswijdten geldt een minimum aan hardware- en softwarevereisten:

- Cisco LWAPP APs AIR-LAP1242AG-A-K9 en AIR-LAP1131AG-A-K9 steun voor de configuratie van het binnenste netwerk.
- Cisco mesh release 2 ondersteunt Enterprise mesh (binnen- en buitenproducten). Dit kan alleen worden geïnstalleerd op Cisco-controller, Cisco 440x/210x en WISM's.
- U kunt Cisco Enterprise mesh release 2-software downloaden van Cisco.com.

Indoor vs. Outdoorkleding

Dit zijn een aantal van de belangrijkste verschillen tussen de binnen- en buitengaasjes:

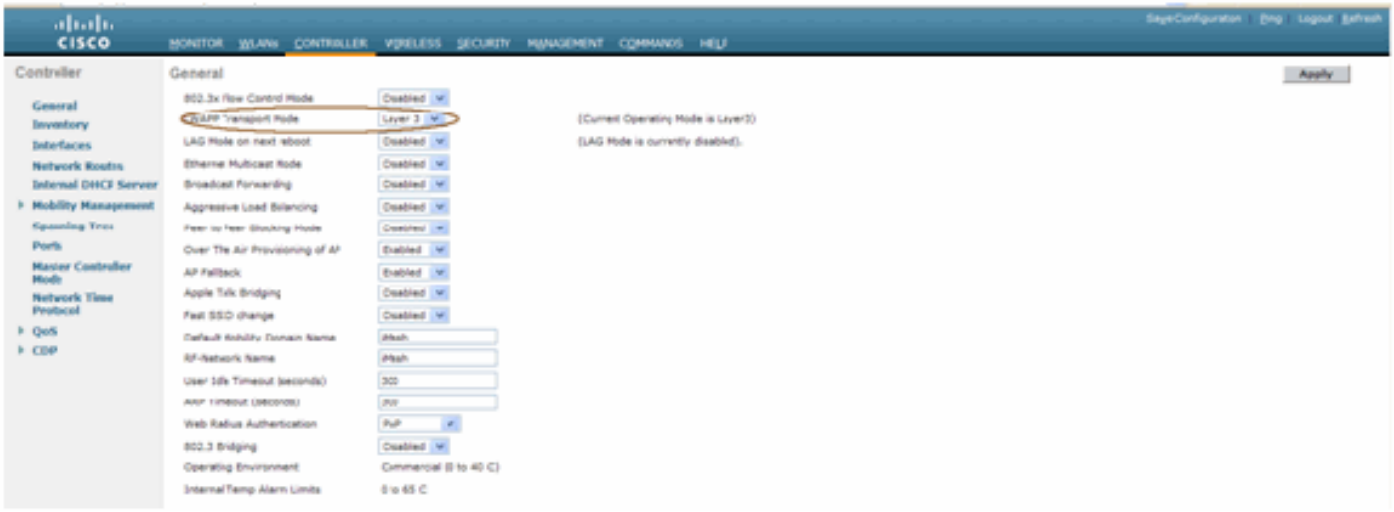
	Indoor mesh	mesh
Omgeving	ALLEEN voor binnen, hardware-indoor	Uitsluitend voor buitengebruik, robuuste hardware
Hardware	AP voor binnen met behulp van LAP1242 en LAP131AG	AP voor buitengebruik met LAP15xx en LAP152x
Voedingsniveau	2,4 GHz:20 dbm 5,8 GHz:17 dbm	2,4 GHz:28 dbm 5,8 GHz:28 dbm
Celgrootte	Ongeveer 150 voet	Ongeveer 1000 voet
Hoogte implementatie	12 voet vanaf de grond	30 meter van de grond

Configuratie

Zorg ervoor dat u de handleiding grondig controleert voordat u een implementatie start, vooral als u nieuwe hardware hebt ontvangen.

Controller L3-modus

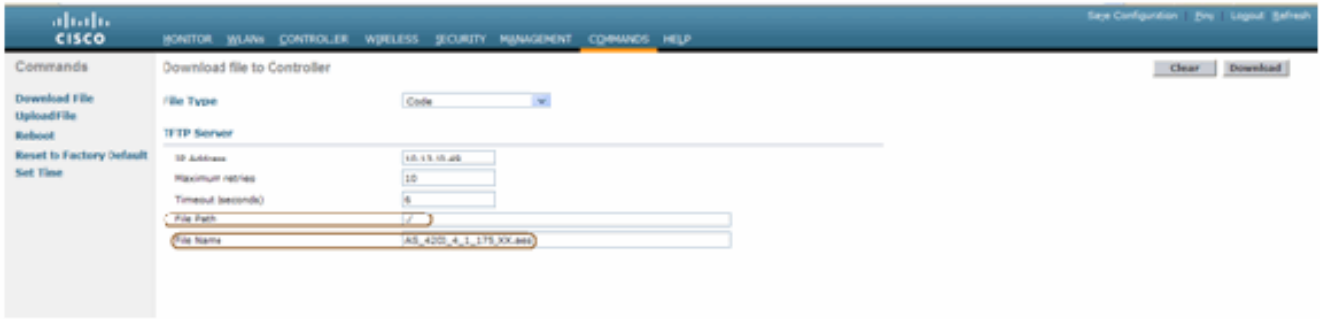
AP's met binnenkorrelgrootte kunnen worden ingezet als een L3-netwerk.



Upgradeer de controller naar de laatste code

Voer de volgende stappen uit:

1. Voor het verbeteren van mesh release 2 op een netwerk met indoor mesh, moet uw netwerk uitgevoerd worden op 4.1.185.0 of mesh release 1, beschikbaar op Cisco.com.
2. Download de laatste code voor de controller op uw TFTP-server. Klik vanuit de interface van Controller GUI op **Opdrachten** > **Downloadbestand**.
3. Selecteer het bestandstype als **code** en geef het IP-adres van uw TFTP-server op. Defineert het pad en de naam van het bestand.



Opmerking: Gebruik de TFTP Server die meer dan 32 MB bestandsgrootteoverdrachten ondersteunt. Bijvoorbeeld, **tftpd32**. Onder File path **"./"** zoals getoond.

4. Nadat u de nieuwe firmware hebt geïnstalleerd, gebruikt u de opdracht sysinfo in de CLI om te controleren of de nieuwe firmware is geïnstalleerd.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 4.1.175.19
RTOS Version..................................... 4.1.175.19
Bootloader Version............................... 4.0.206.0
Build Type....................................... DATA + WPS

System Name...................................... CiscoImesh
System Location.................................
System Contact..................................
System ObjectID.................................. 1.3.6.1.4.1.14179.1.1.4.3
IP Address....................................... 10.13.10.20
System Up Time................................... 1 days 22 hrs 3 mins 35 secs

Configured Country............................... US  - United States
Operating Environment............................ Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to 65 C
Internal Temperature............................. +38 C

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
--More-- or (q)uit
Number of WLANs.................................. 2
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 3

Burned-in MAC Address............................ 00:18:73:34:48:60
Crypto Accelerator 1............................. Absent
Crypto Accelerator 2............................. Absent
Power Supply 1................................... Absent
Power Supply 2................................... Present, OK
```

Opmerking: Officieel biedt Cisco geen ondersteuning voor downloads voor controllers.

MAC-adres

Het is verplicht om MAC-filtering te gebruiken. Deze optie heeft de Cisco Indoor mesh-oplossing gemaakt als een echte "Zero Touch". In tegenstelling tot de vorige releases zal het mesh-scherm niet langer de MAC-filtering optie hebben.

Opmerking: MAC-filtering is standaard ingeschakeld.

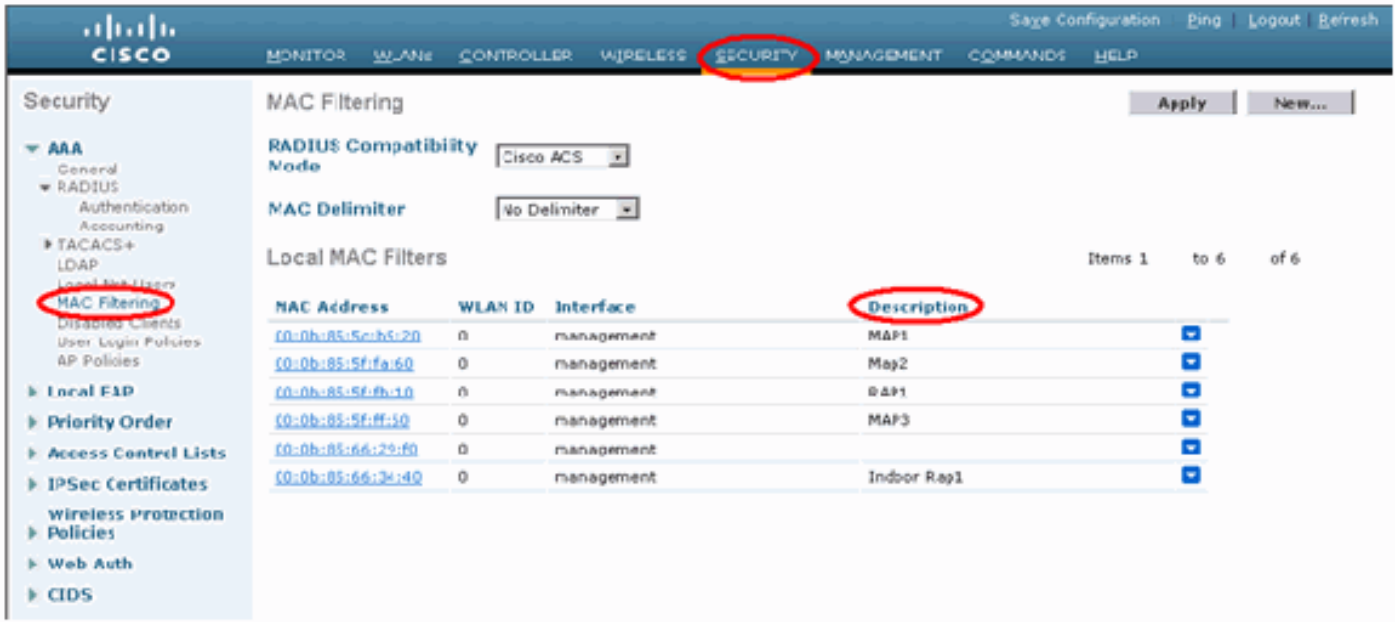
MAC-adres van de radio opnemen

In een tekstbestand kunt u de MAC-adressen opnemen van alle inkomende AP-radio's die u in uw netwerk hebt ingezet. Het MAC-adres is te vinden op de achterzijde van de AP's. Dit helpt u voor toekomstige testen, aangezien de meeste opdrachten van CLI vereisen dat het APs MAC-adres of de namen met de opdracht worden ingevoerd. U kunt de naam van APs ook veranderen in iets makkelijker onthouden, zoals, "bouw aantal-po aantal-AP type: laatste vier tekens van het MAC-adres hex."

Voer het MAC-adres en de Namen van de radio in de controller

De Cisco-controller houdt een MAC-adreslijst van binnenshuis toestemming bij. De controller reageert alleen op ontdekkingsverzoeken van de binnenradio's die op de vergunningslijst staan. Voer de MAC-adressen in van alle radio's die u in uw netwerk op de controller neigt te gebruiken.

Ga in de interface Controller GUI naar **Security** en klik op **MAC-filtering** aan de linkerkant van het scherm. Klik op **Nieuw** om de MAC-adressen in te voeren zoals hier wordt getoond:



Voer ook de namen van de radio's in voor het gemak onder **Beschrijving** (zoals locatie, AP #, enz.) Omschrijving kan ook worden gebruikt voor de plaats waar de radios zijn geïnstalleerd, zodat ze te allen tijde gemakkelijk kan worden geraadpleegd.

MAC-filtering inschakelen

MAC-filtering is standaard ingeschakeld.

Je kunt ook een keuze maken uit de beveiligingsmodus zoals EAP of PSK op dezelfde pagina.

Gebruik dit pad vanuit de GUI-interface van de switch:

GUI-interfacepad: **Draadloos > mesh binnenshuis**

De beveiligingsmodus kan ALLEEN in de CLI worden ingeschakeld door deze opdracht:

```
(Cisco Controller) > show network
```

```
(Cisco Controller) >show network

RF-Network Name.............................. iMesh
Web Mode..................................... Disable
Secure Web Mode.............................. Enable
Secure Shell (ssh)........................... Enable
Telnet....................................... Enable
Ethernet Multicast Mode...................... Disable   Mode: Ucast
Ethernet Broadcast Mode...................... Disable
User Idle Timeout............................ 300 seconds
ARP Idle Timeout............................. 300 seconds
ARP Unicast Mode............................. Disabled
Cisco AP Default Master...................... Disable
Mgmt Via Wireless Interface.................. Disable
Mgmt Via Dynamic Interface................... Disable
Bridge MAC filter Config..................... Enable
Bridge Security Mode......................... EAP
Mesh Multicast Mode.......................... 802.11b/g/n
Mesh Full Sector DFS......................... Enable
Over The Air Provisioning of AP's............ Enable
Mobile Peer to Peer Blocking................. Disable
Apple Talk .................................. Disable
AP Fallback ................................. Enable
--More-- or (q)uit
Web Auth Redirect Ports ..................... 80
Fast SSID Change ............................ Disabled
802.3 Bridging .............................. Disable
```

L3 mesh-implementatie voor binnenshuis

Voor een L3 mesh-netwerk moet u de IP-adressen voor de radio's configureren als u niet van plan bent de DHCP-server (intern of extern) te gebruiken.

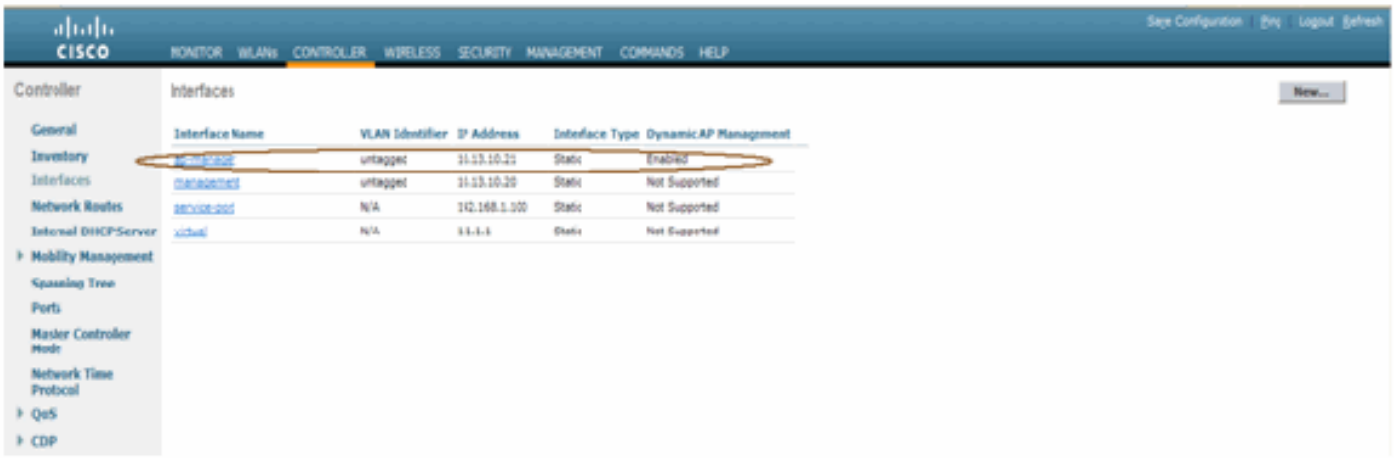
Voor een L3 mesh-netwerk moet u, als u DHCP-server wilt gebruiken, de controller in L3-modus configureren. Bewaar de configuratie en start de controller opnieuw op. Stel optie 43 in op de DHCP-server. Nadat de controller opnieuw is gestart, ontvangen nieuw aangesloten APs hun IP-adres van de DHCP-server.

Interfaces op controller definiëren

AP Manager

Voor een L3 plaatsing, moet u de **AP-manager** definiëren. De AP Manager treedt op als bron IP adres voor communicatie van de controller naar de APs.

Pad: **Controller > Interfaces > ap-Manager > bewerken**.



De **AP-Manager** interface zou een IP adres in zelfde netwerk en VLAN moeten worden toegewezen zoals uw beheersinterface.

Radio Roles

Er zijn twee primaire radioverbindingen mogelijk met deze oplossing:

- Root Access Point (RAP) - De radio waarmee u verbinding wilt maken met de controller (via de switch) neemt de rol van een RAP. De RAP's hebben een bekabelde, met LWAPP verbonden verbinding met de controller. Een RAP is een parent-knooppunt voor een

overbruggingsnetwerk of een netwerk met binnennetten. Een controller kan een of meer RAP hebben, elk een ouderschap van dezelfde of verschillende draadloze netwerken. Er kan meer dan één RAP zijn voor hetzelfde binnennetwerk van een netwerk voor redundantie.

- Indoor mesh access point (MAP) - De radio die geen bekabelde verbinding met de controller heeft, neemt de rol van een access point met binnennetwerk in. Dit AP werd voorheen Pole top AP genoemd. MAP's hebben een draadloze verbinding (via de backhaul-interface) naar mogelijk andere MAP's en ten slotte naar een RAP en dus naar de controller. MAP's kunnen ook een bekabelde Ethernet-verbinding naar een LAN hebben en dienen als een bridge-eindpunt voor dat LAN (met behulp van een P2P- of P2MP-verbinding). Dit kan tegelijkertijd plaatsvinden, indien correct geconfigureerd als een Ethernet-brug. MAP's serviceklanten op de band die niet voor de backhaul-interface wordt gebruikt.

De standaardmodus voor een AP is MAP.

Opmerking: de radiorollen kunnen via GUI of CLI worden ingesteld. De AP's zullen opnieuw beginnen na de rolverandering.

Opmerking: U kunt de controller-CLI gebruiken om de radiolrollen vooraf in te stellen op een AP mits de AP fysiek is verbonden met de switch of u de AP op de switch kunt zien als een RAP of een MAP.

```
(Cisco Controller) >config ap role ?

rootAP          RootAP role for the Cisco Bridge.
meshAP          MeshAP role for the Cisco Bridge.

(Cisco Controller) >config ap role meshAP ?

<Cisco AP>      Enter the name of the Cisco AP.

(Cisco Controller) >config ap role meshAP LAP1242-2

Changing the AP's role will cause the AP to reboot.
Are you sure you want to continue? (y/n)
```

Naam van bridge-groep

Bridge Group Names (BGN) controleert de associatie van de AP's. BGN's kunnen de radio's logischerwijze groeperen om te voorkomen dat twee netwerken op hetzelfde kanaal met elkaar communiceren. Deze instelling is ook handig als u in dezelfde sector (gebied) meer dan één RAP in uw netwerk hebt. Het BGN is een string van maximaal tien tekens.

Een in de fabriek ingestelde groepsnaam wordt toegewezen in het fabricagestadium (NULL VALUE). Het is niet zichtbaar voor u. Als resultaat hiervan, zelfs zonder een bepaald BGN, kunnen de radio's zich nog steeds bij het netwerk aansluiten. Als u twee RAP's in uw netwerk in dezelfde sector hebt (voor meer capaciteit), wordt aanbevolen om de twee RAP's met hetzelfde BGN te configureren, maar op verschillende kanalen.

Opmerking: de naam van de Bridge Group kan al vanaf de CLI en GUI van de controller worden ingesteld.

```
(Cisco Controller) >config ap bridgegroupname set ?

<bridgegroupname> Set bridgegroupname on Cisco AP.
```

Nadat u de BGN hebt ingesteld, stelt u de AP opnieuw in.

Opmerking: het BGN moet heel voorzichtig zijn ingesteld op een actief netwerk. U dient altijd te beginnen met het verste knooppunt (laatste knooppunt) en naar de RAP te gaan. De reden is dat als u de BGN ergens in het midden van de multihop begint te configureren, dan zullen de knooppunten voorbij dit punt vallen aangezien deze knooppunten een ander BGN (oud BGN) zullen hebben.

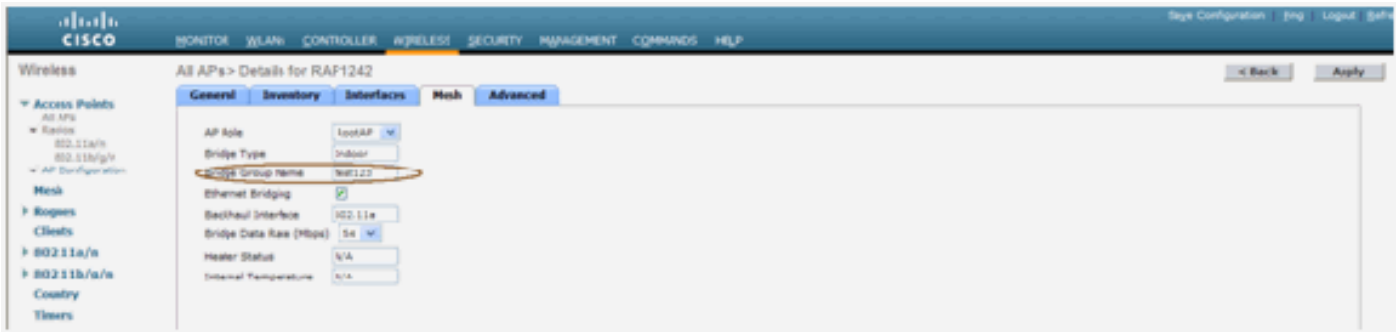
U kunt het BGN verifiëren door deze CLI-opdracht uit te geven:

(Cisco Controller) **> show ap config general**

```
(Cisco Controller) >show ap config general RAP1242

Cisco AP Identifier.............................. 9
Cisco AP Name.................................... RAP1242
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 00:18:74:fa:7d:1f
IP Address Configuration......................... DHCP
IP Address....................................... 10.13.13.11
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 10.13.13.10
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch............................. J2106-1
Secondary Cisco Switch........................... 
Tertiary Cisco Switch............................ 
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Bridge
--More-- or (q)uit
AP Role ......................................... RootAP
Ethernet Bridging ............................... Enabled
Bridge GroupName ................................ test123
Public Safety ..................................  Disabled
Remote AP Debug ................................. Disabled
S/W  Version .................................... 4.1.175.19
Boot  Version ................................... 12.3.7.1
Mini IOS Version ................................ 3.0.51.0
Stats Reporting Period .......................... 180
LED State........................................ Enabled
PoE Pre-Standard Switch.......................... Disabled
PoE Power Injector MAC Addr...................... Disabled
Number Of Slots.................................. 2
AP Model......................................... AIR-LAP1242AG-A-K9
IOS Version...................................... 12.4(20070808:082741)
Reset Button..................................... Enabled
AP Serial Number................................. FTX1035B3RH
AP Certificate Type.............................. Manufacture Installed
Management Frame Protection Validation.......... Disabled
Console Login Name............................... 
Console Login State.............................. Unknown
AP Up Time....................................... 0 days, 02 h 43 m 38 s
AP LWAPP Up Time................................. 0 days, 02 h 42 m 43 s
--More-- or (q)uit
Join Date and Time............................... Sun Aug 19 11:59:07 2007

Join Taken Time.................................. 0 days, 00 h 00 m 24 s
Ethernet Port Duplex............................. Unknown
Ethernet Port Speed.............................. Unknown
```

U kunt ook het BGN configureren of controleren met behulp van de Controller GUI:

Pad: **Draadloos > Alle AP's > Details**.



U kunt zien dat de milieu-informatie van AP ook met deze nieuwe publicatie wordt weergegeven.

Beveiligingsconfiguratie

De standaard beveiligingsmodus voor binnenshuis is is EAP. Dit betekent dat tenzij u deze parameters op uw controller configureren, uw MAP's zich niet aansluiten bij:

CLI-configuratie voor binnenmesh

```
(Cisco Controller) >config mesh local-auth enable

 enable Local Auth

(Cisco Controller) >config advanced eap ?

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 E
AP identity response
request-timeout Configures EAP-Request Timeout in seconds.
request-retries Configures EAP-Request Max Retries.
```

Als u in de PSK-modus wilt blijven, gebruikt u deze opdracht om terug te gaan naar de PSK-modus:

```
(Cisco Controller) >config mesh security psk ?

(Cisco Controller) >config mesh security psk

 All Mesh AP will be rebooted
 Are you sure you want to start? (y/N)n
```

Toon opdrachten voor binnenmesh

Binnen de EAP modus kunt u deze **show** opdrachten controleren om de MAP authenticatie te controleren:

```
(Cisco Controller) >show network

RF Network Name.............................. jaggi123
Web Mode..................................... Disable
Secure Web Mode.............................. Enable
Secure Shell (ssh)........................... Enable
Telnet....................................... Enable
Ethernet Multicast Mode...................... Disable   Mode: Mcast  224.1.1.1
Ethernet Broadcast Mode...................... Disable
User Idle Timeout............................ 300 seconds
ARP Idle Timeout............................. 300 seconds
ARP Unicast Mode............................. Disabled
Cisco AP Default Master...................... Disable
Mgmt Via Wireless Interface.................. Enable
Mgmt Via Dynamic Interface................... Disable
Bridge MAC filter Config..................... Disable
Bridge Security Mode......................... EAP  otherwise PSK
Mesh Multicast Mode.......................... 802.11b/g/n
Mesh Full Sector DFS......................... Enable
Over The Air Provisioning of AP's............ Enable
Mobile Peer to Peer Blocking................. Disable
AP Fallback ................................. Enable
Web Auth Redirect Ports ..................... 80
--More-- or (q)uit
Fast SSID Change ............................ Disabled
802.3 Bridging .............................. Disable
```

(Cisco Controller) >**show wlan 0**

```
(Cisco Controller) >show wlan 0

WLAN Identifier.................................. 0
Profile Name..................................... Mesh_profile
Network Name (SSID).............................. Mesh_ssid
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 2
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Allowed
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... None
--More-- or (q)uit
IPv6 Support..................................... Disabled
Radio Policy..................................... All
Local EAP Authentication......................... Enabled (Profile 'prfMaP1500L1EAuth93')
Security

   802.11 Authentication:........................ Open System
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Disabled
      WPA2 (RSN IE).............................. Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
                                                  Auth Key Management
         802.1x.................................. Enabled
         PSK..................................... Disabled
         CCKM.................................... Disabled
   CKIP ......................................... Disabled
   IP Security Passthru.......................... Disabled
   Web Based Authentication...................... Disabled
   Web-Passthrough............................... Disabled
   Conditional Web Redirect...................... Disabled
   Auto Anchor................................... Disabled
--More-- or (q)uit
   H-REAP Local Switching........................ Disabled
   Infrastructure MFP protection................. Enabled (Global Infrastructure MFP Disabled)
   Client MFP.................................... Optional
   Tkip MIC Countermeasure Hold-down Timer....... 60

 Mobility Anchor List
 WLAN ID       IP Address       Status
```

(Cisco Controller) >**show local-auth config**

```
(Cisco Controller) >show local-auth config

User credentials database search order:
    Primary ..................................... Local DB

Timer:
    Active timeout ............................. 300

Configured EAP profiles:

EAP Method configuration:
    EAP-FAST:
      Server key ................................ <hidden>
      TTL for the PAC ........................... 10
      Anonymous provision allowed ............... Yes
      Authority ID .............................. 436973636f0000000000000000000000
      Authority Information ..................... Cisco A-ID

(Cisco Controller) >show advanced eap


EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries........... 20
EAP Key-Index for Dynamic WEP.............. 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds).............. 1
EAP-Request Max Retries.................... 2
```

```
(Cisco Controller) >show advanced eap
```

EAP-debug van opdrachten binnen

Gebruik deze opdrachten in de controller om problemen met de EAP-modus op te lossen:

```
(Cisco Controller) >debug dot1x all enable

(Cisco Controller) >debug aaa all enable
```

Installatie

Voorvereisten

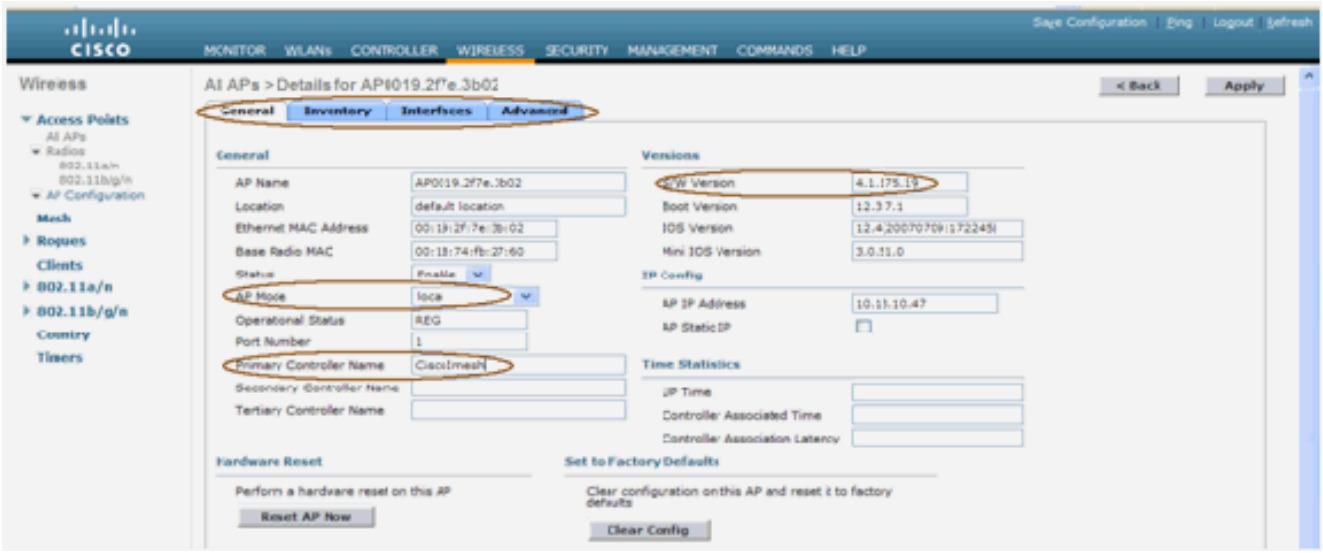
De controller moet de aanbevolen versie van de code uitvoeren. Klik op **Monitor** om de softwareversie te controleren. Hetzelfde kan via CLI worden geverifieerd.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 4.1.175.19
RTOS Version..................................... 4.1.175.19
Bootloader Version............................... 4.0.206.0
Build Type....................................... DATA + WPS

System Name...................................... CiscoImesh
System Location.....................................
System Contact......................................
System ObjectID.................................. 1.3.6.1.4.1.14179.1.1.4.3
IP Address....................................... 10.13.10.20
System Up Time................................... 1 days 22 hrs 3 mins 35 secs

Configured Country............................... US  - United States
Operating Environment............................ Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to 65 C
Internal Temperature............................. +38 C

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
--More-- or (q)uit
Number of WLANs.................................. 2
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 3

Burned-in MAC Address............................ 00:18:73:34:48:60
Crypto Accelerator 1............................. Absent
Crypto Accelerator 2............................. Absent
Power Supply 1................................... Absent
Power Supply 2................................... Present, OK
```

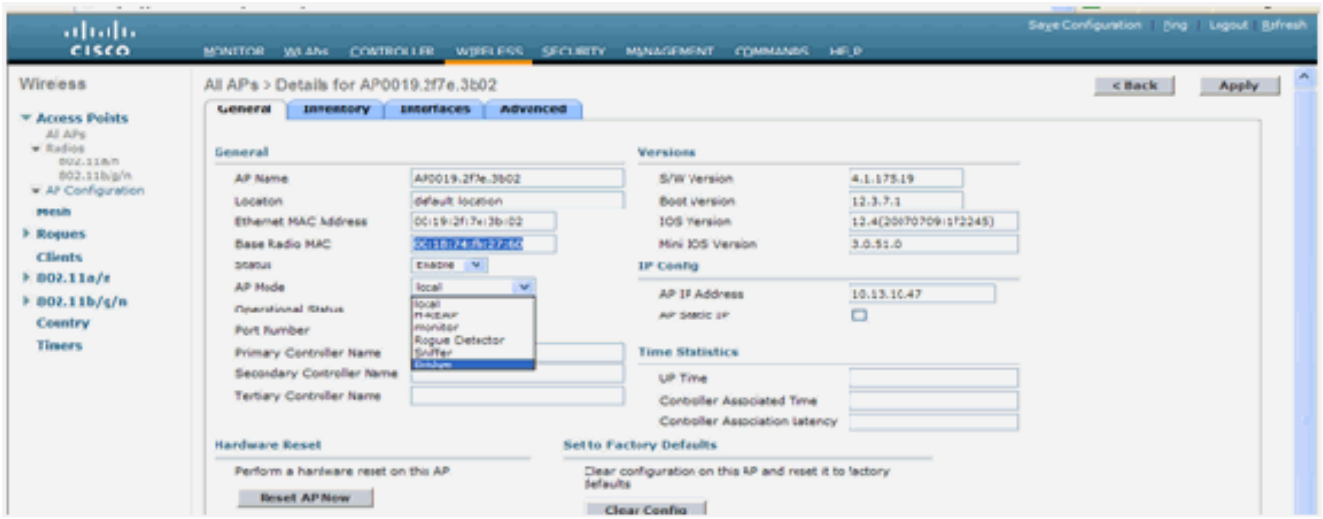
Systemen als de DHCP-server, ACS server en WCS server zouden bereikbaar moeten zijn.

Installatie

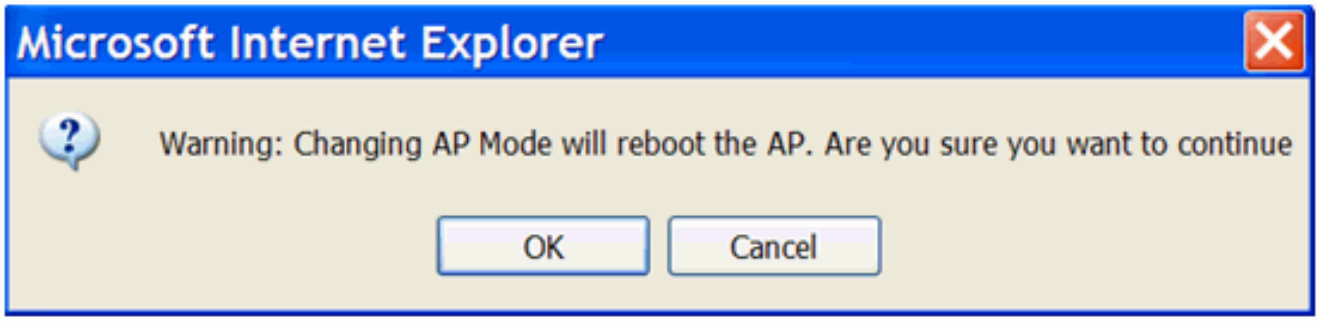
1. Sluit alle LAP's (1131AG/1242AG) aan op een Layer 3-netwerk op hetzelfde subnet als het IP-adres van het beheer. Alle AP's zullen zich bij de controller als AP's in lokale modus aansluiten. In deze modus: druk de AP's af met de naam van de primaire controller, de naam van de secundaire controller en een naam van de tijdelijke controller.



2. Leg het MAC-adres van de basisradio van de AP vast (bijvoorbeeld 00:18:74: fb: 27:60)
3. Voeg het adres van MAC van AP toe voor AP om in overbruggingsmodus toe te treden.
4. Klik op **Security** > **MAC-filtering** > **New**.
5. Voeg het gekopieerde adres van MAC toe, en noem APs in de MAC-filter lijst en de AP lijst.
6. Kies **Bridge** in de lijst **AP Mode**.



7. U wordt gevraagd dit te bevestigen, aangezien het AP opnieuw wordt opgestart.



8. AP herstart en sluit zich aan bij de controller in Bridge-modus. Het nieuwe AP-venster zal een extra tabblad hebben: MESH. Klik op het tabblad **MESH** om de rol, het type brug, de naam van de bridge groep, het overbruggen van Ethernet, de backhaul-interface, de snelheid van de brug, enz. te controleren.

9. In dit venster kunt u de rollijst AP openen en de rol in kwestie kiezen. In dit geval is de standaard rol een MAP.De naam van de Bridge Group is standaard leeg.Achterkant is 802.11a.Bridge Data Rate (d.w.z. Back haul gegevenssnelheid) is 24 Mbps.
10. Sluit de AP die u als RAP wilt aan op de controller. Stel de radio's (MAP's) op de gewenste locaties in. Switch op de radio. U dient alle radio's op de controller te kunnen zien.

```
(Cisco Controller) >show ap summ

Number of APs.................................... 3

AP Name             Slots  AP Model             Ethernet MAC       Location          Port  Country
-----------------   -----  -------------------  -----------------  ----------------  ----  -------
RAP1242             2      AIR-LAP1242AG-A-K9   00:18:74:fa:7d:1f  default location  1     US
LAP1242-1           2      AIR-LAP1242AG-A-K9   00:1b:2b:a7:ad:bf  default location  1     US
LAP1242-2           2      AIR-LAP1242AG-A-K9   00:14:1b:59:07:af  default location  1     US
```

11. Probeer de belichtingsomstandigheden tussen de knooppunten te bepalen. Als de condities voor het zicht niet bestaan, moet u de ruimte van de Fresnel zone ruimte creëren om bijna-lijn-van-plaats omstandigheden te verkrijgen.
12. Als u meer dan één controller hebt aangesloten op hetzelfde netwerk van binnennetwerken, moet u de naam van de primaire controller op elk knooppunt specificeren. Anders wordt de controller die eerst wordt gezien als de primaire controller gebruikt.

Configuratie van voeding en kanaal

Het backhaul-kanaal kan op een RAP worden ingesteld. MAP's worden afgestemd op het RAP-kanaal. De lokale toegang kan onafhankelijk worden ingesteld voor MAP's.

Vanuit de Switch GUI, volg het pad: **Draadloos > 802.11a radio > configuratie**.

Opmerking: het standaard Tx-vermogensniveau op de backhaul is het hoogste vermogensniveau (niveau 1) en het Radio Resource Management (RRM) is standaard uitgeschakeld.

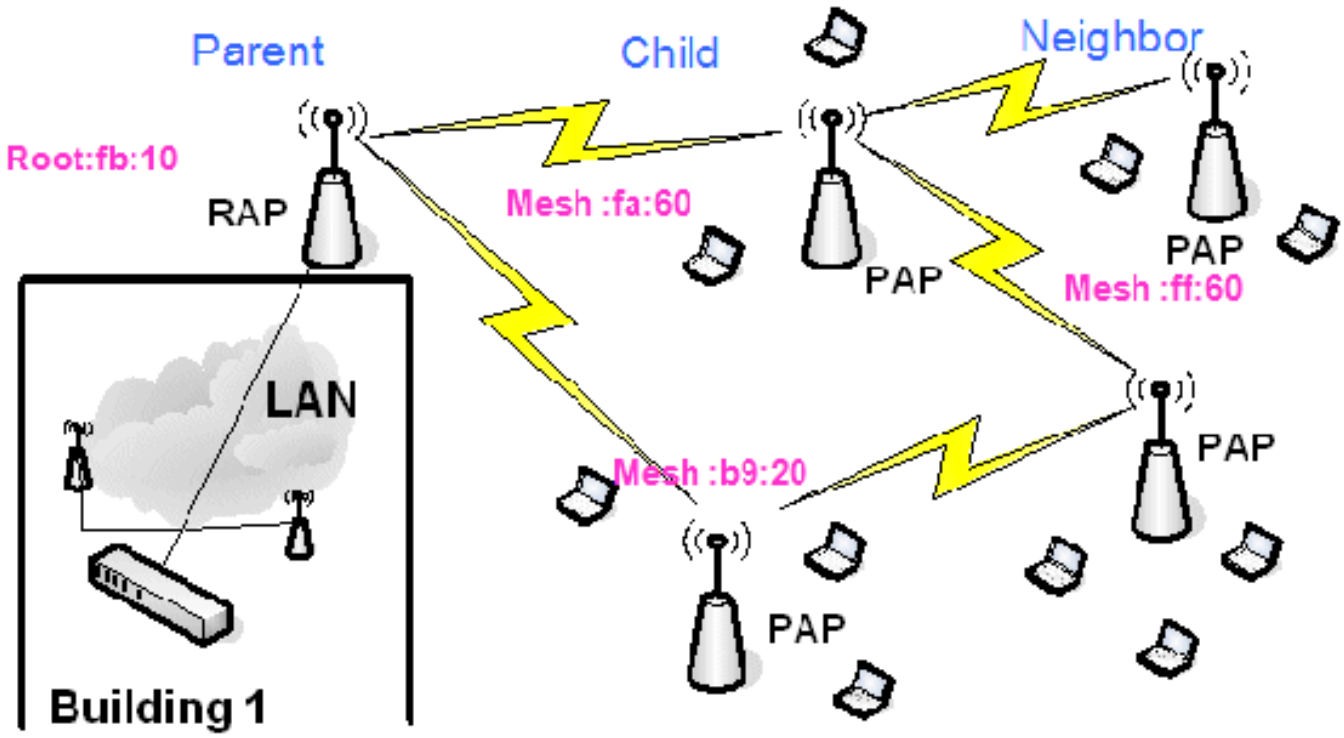
Als u RAP's koppelt, raden we u aan alternatieve zenders op elke RAP te gebruiken. Dit zal kanaalinterferentie verminderen.

RF-controle

In een netwerk met binnennetten moeten we de relatie tussen ouder en kind tussen de knooppunten verifiëren. **Hop** is een draadloos verband tussen de twee radio's. De ouder-kind relatie verandert wanneer u door het netwerk reist. Het hangt af van waar u zich in het binnennetwerk bevindt.

De radio dichter bij de controller in een draadloze verbinding (hop) is een **ouder** van de radio aan de andere kant van de hop. In een meervoudig hopsysteem is er een structuur van het boomtype waar het knooppunt dat is aangesloten op de controller een RAP (**Parent**) is. De onmiddellijke knoop aan de andere kant van de eerste hop is een **Kind**, en de volgende knooppunten in de tweede hop zijn de **buren** voor die specifieke ouder.

Afbeelding 1: Twee hop-netwerken



In afbeelding 1 worden AP-namen genoemd voor het gemak. In de volgende screenshot wordt de **RAP (fb:10)** onderzocht. Dit knooppunt kan de APs (in de feitelijke installatie) van binnenmesh **(fa:60 en b9:20)** als kinderen en **MAP ff:60 als buurman** zien.

Vanuit de switch GUI-interface volgt u het pad: **Draadloos > Alle AP > Rap1 > buurtinformatie**.

Zorg ervoor dat de relatie tussen ouders en kinderen correct wordt ingesteld en onderhouden voor uw mesh-netwerk.

Controleer de interconnecties

Laat zien dat mesh een informatieve opdracht is om de interconnectiviteit in uw netwerk te verifiëren.

U moet deze opdrachten in elk knooppunt (AP) geven met behulp van de controller-CLI en de resultaten in een Word- of tekstbestand uploaden naar de uploadsite.

```
(Cisco Controller) >show mesh ?

env             Show mesh environment.
neigh           Show AP neigh list.
path            Show AP path.
stats           Show AP stats.
secbh-stats     Show Mesh AP secondary backhaul stats.
per-stats       Show AP Neighbor Packet Error Rate stats.
queue-stats     Show AP local queue stats.
security-stats  Show AP security stats.
config          Show mesh configurations.
secondary-backhaul Show mesh secondary-backhaul
client-access   Show mesh backhaul with client access.
public-safety   Show mesh public safety.
background-scanning Show mesh background-scanning state.
cac             Show mesh cac.
```

In uw netwerk van het binnennetwerk, kies een meervoudige verbinding van de hop en geef deze opdrachten uit die van de RAP beginnen. Upload het resultaat van de opdrachten naar de uploadsite.

In de volgende sectie, zijn al deze opdrachten uitgegeven voor het twee Netwerk van binnenste mesh in Afbeelding 1.

Indoor mesh pad weergeven

Deze opdracht geeft u de MAC-adressen, de radioverslagpunten van de knooppunten, de Signal to Noise-ratio's in dBs voor Uplink/Downlink (SNRUp, SNRDown) en de Link SNR in dB voor een bepaald pad weer.

```
(Cisco Controller) >show mesh path RAP1242

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
RAP1242           is a Root AP.
(Cisco Controller) >show mesh path LAP1242-2

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-1           56      29     29       27       0x86b    UPDATED NEIGH PARENT BEACON
RAP1242             56      41     32       34       0x86b    UPDATED NEIGH PARENT BEACON
RAP1242           is a Root AP.
```

Samenvatting binnen mesh

Deze opdracht zal u de MAC-adressen, ouder-kind-relaties en Uplink/Downlink SNRs in dB tonen.

```
(Cisco Controller) >show mesh neigh ?

detail          Show Link rate neigh detail.
summary         Show Link rate neigh summary.
(Cisco Controller) >show mesh neigh  summary RAP1242

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-2           56      0      0        0        0x860    BEACON
LAP1242-1           56      0      33       0        0x960    CHILD BEACON


(Cisco Controller) >show mesh neigh  summary LAP1242-1

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-2           56      30     29       28       0x961    UPDATED CHILD BEACON
RAP1242             56      43     46       31       0x86b    UPDATED NEIGH PARENT BEACON
```

Tegen deze tijd zou u de relaties tussen de knooppunten van uw netwerk moeten kunnen zien en de RF connectiviteit moeten kunnen verifiëren door de SNR waarden voor elke verbinding te zien.

AP-console toegangsbeveiliging

Deze functie geeft verbeterde beveiliging van de toegang tot de console van AP. Er is een console-kabel voor AP vereist om deze functie te gebruiken.

Deze worden ondersteund:

- Een CLI om de gebruiker-id/wachtwoord combinatie naar de gespecificeerde AP te duwen:

```
(Cisco Controller) >config ap username Cisco password Cisco ?

all             Configures the Username/Password for all connected APs.
<Cisco AP>      Enter the name of the Cisco AP.
```

- Een CLI-opdracht om de gebruikersnaam/wachtwoordcombinatie te gebruiken naar alle AP's die bij de controller zijn geregistreerd:

```
(Cisco Controller) >config ap username Cisco password Cisco all
```

Met deze opdrachten is de user-id/password combinatie die van de controller wordt geduwd, persisterend in de herlading op de AP's. Als een AP van de controller wordt gewist, is er geen beveiligingstoegangsmodus. AP genereert een SNMP-val met een succesvolle inlognaam. AP zal ook een SNMP val op een console inlogfout voor drie opeenvolgende malen genereren.

Ethernet-overbrugging

Om veiligheidsredenen wordt de Ethernet poort op de MAPs standaard uitgeschakeld. Hij kan alleen worden ingeschakeld door Ethernet Bridging te configureren op de RAP en de respectievelijke MAP's.

Als resultaat hiervan moet Ethernet Bridging worden ingeschakeld voor twee scenario's:

- Wanneer u de knooppunten van de binnenmaas als bruggen wilt gebruiken.
- Wanneer u een Ethernet-apparaat (zoals PC/laptop, videocamera etc.) op de MAP wilt aansluiten via de Ethernet-poort.

Pad: **Draadloos** > Klik op om het even welke AP > **mesh**.

Er is een CLI-opdracht die kan worden gebruikt om de afstand tussen de knooppunten die de overbrugging doen te configureren. Probeer bij elke hop een Ethernet-apparaat aan te sluiten zoals een Video Camera en zie de prestaties.

Verbetering in naam van bridge

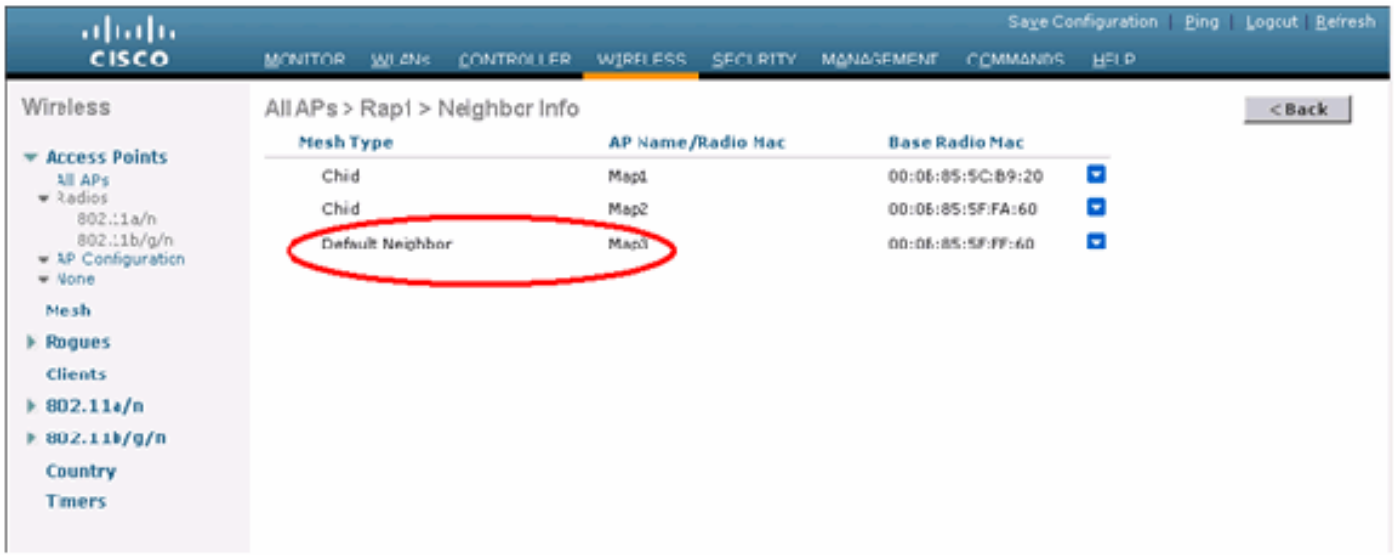
Het is mogelijk dat een AP ten onrechte voorzien is van een "naam van een bridgegroup" waarvoor het niet bedoeld was. Afhankelijk van het netwerkontwerp kan dit AP al dan niet in staat zijn om zijn juiste sector/boom te vinden. Als een sector niet compatibel is, kan deze gestrand worden.

Om zo'n gestrande AP te herstellen werd het concept van "standaard" bridgegroup name geïntroduceerd met de 3.2.xx.x code. Het basisidee is dat een AP die geen verbinding kan maken met een andere AP met zijn geconfigureerde bridgegroup name, probeert verbinding te maken met "default" (het woord) als bridgegroupname. Alle knooppunten met 3.2.xx.x en latere software accepteren andere knooppunten met deze naam van de brug.

Deze functie kan ook helpen om een nieuw knooppunt of een verkeerd ingesteld knooppunt aan een actief netwerk toe te voegen.

Als u een actief netwerk hebt, neem een vooraf ingesteld AP met een ander BGN en maak het zich bij het netwerk aan. U ziet deze AP in de controller met behulp van "standaard" BGN nadat u het MAC-adres in de controller hebt toegevoegd.

```
(CiscoController) >show mesh path Map3:5f:ff:60

00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT DEFAULT (106B), snrUp 48, snrDown 4
8, linkSnr 49
00:0B:85:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B), snrUp 72, snrDown 63,
 linkSnr 57
00:0B:85:5F:FB:10 is RAP
```



AP die de standaard BGN gebruikt kan als normale Indoor mesh AP handelen die cliënten associeert en indoor mesh ouderrelaties vormt.

Zodra deze AP met de standaard BGN een andere ouder met de juiste BGN vindt, zal het aan het switches.

Logs - Berichten, SYS, AP en Trap

Vastlegging berichten

Het rapportageniveau voor berichtdocumenten inschakelen. Geef deze opdracht op vanaf de CLI-controller:

```
(Cisco Controller) >config msglog level ?

critical        Critical hardware or software Failure.
error           Non-Critical software error.
security        Authentication or security related error.
warning         Unexpected software events.
verbose         Significant system events.

(Cisco Controller) >config msglog level verbose
```

Om Berichtenlogs te zien geeft u deze opdracht uit van de CLI van de controller:

```
(Cisco Controller) >show msglog

Message Log Severity Level ..................... VERBOSE
Mon Jul 11 01:42:08 2005  [SECURITY] apf_foreignap.c 765: Received a packet for
which no AP was configured from 00:0F:B5:93:71:E7 on port 0.
Fri Jul  8 06:12:02 2005  [ERROR] spam_radius.c 93: spamRadiusProcessResponse: A
P Authorization failure for 00:0b:85:0e:04:80
Fri Jul  8 05:40:15 2005  [ERROR] spam_tmr.c 501: Did not receive hearbeat reply
 from AP 00:0b:85:0e:05:80
Fri Jul  8 05:38:45 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:05:80
Fri Jul  8 05:38:40 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:14:00
Fri Jul  8 05:38:40 2005  Previous message occurred 5 times
Fri Jul  8 05:33:54 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:05:80
Fri Jul  8 05:32:23 2005  [ERROR] poe.c 449: poeInitPowerSupply : poePortResync
returned FAILURE.
Fri Jul  8 05:32:17 2005  [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0
Fri Jul  8 05:32:17 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11a swi
tch group reset
Fri Jul  8 05:32:16 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11bg sw
itch group reset
Fri Jul  8 05:32:16 2005  Previous message occurred 2 times
Fri Jul  8 05:31:19 2005  [CRITICAL] osapi_sem.c 794: Error!  osapiMutexTake cal
```

Om de Berichtvastlegging te uploaden, gebruikt u de Controller GUI-interface:

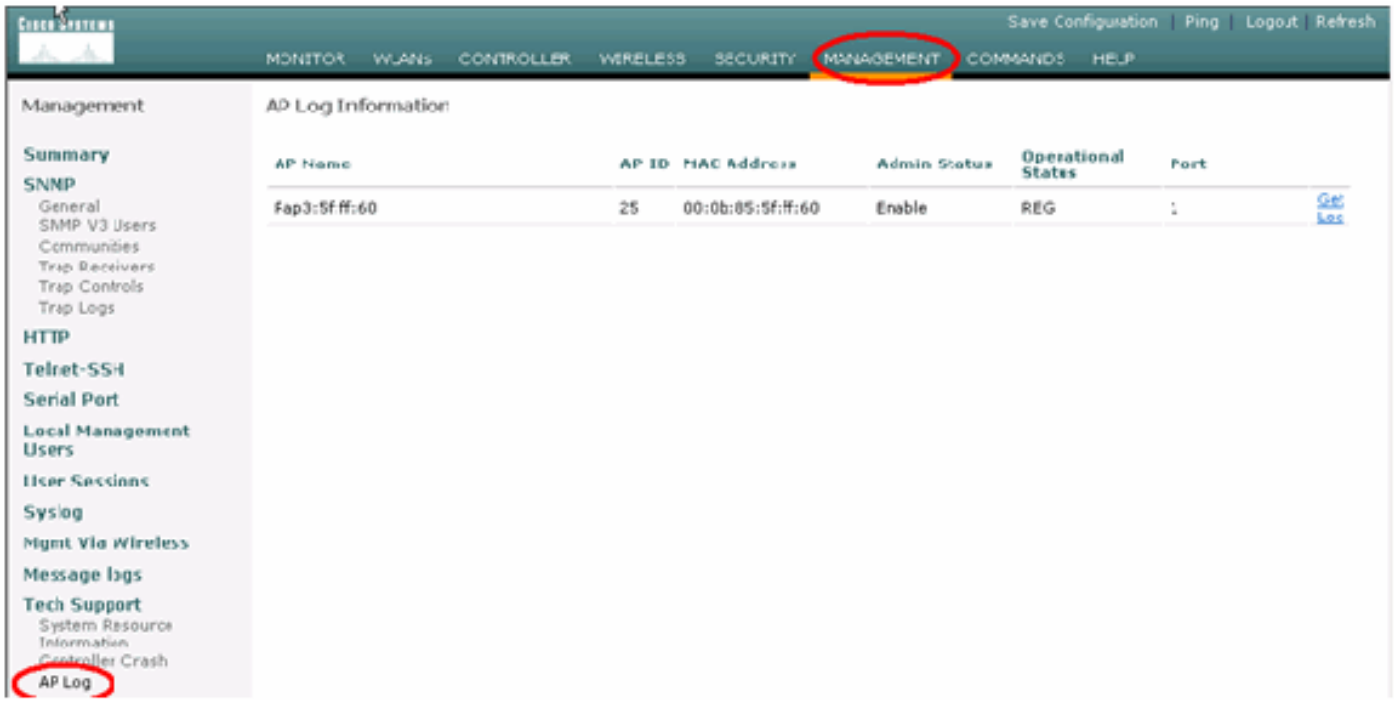
1. Klik op **Opdrachten** > **Upload**.

2. Voer informatie over de TFTP-server in. Op deze pagina kunt u verschillende uploadopties instellen en u wilt dat deze bestanden worden verzonden:BerichtenlogboekEvent LogTrap-logboekCrash File (indien aanwezig)Klik op **Management** > **Controller** crash om te

controleren op
crashbestanden.

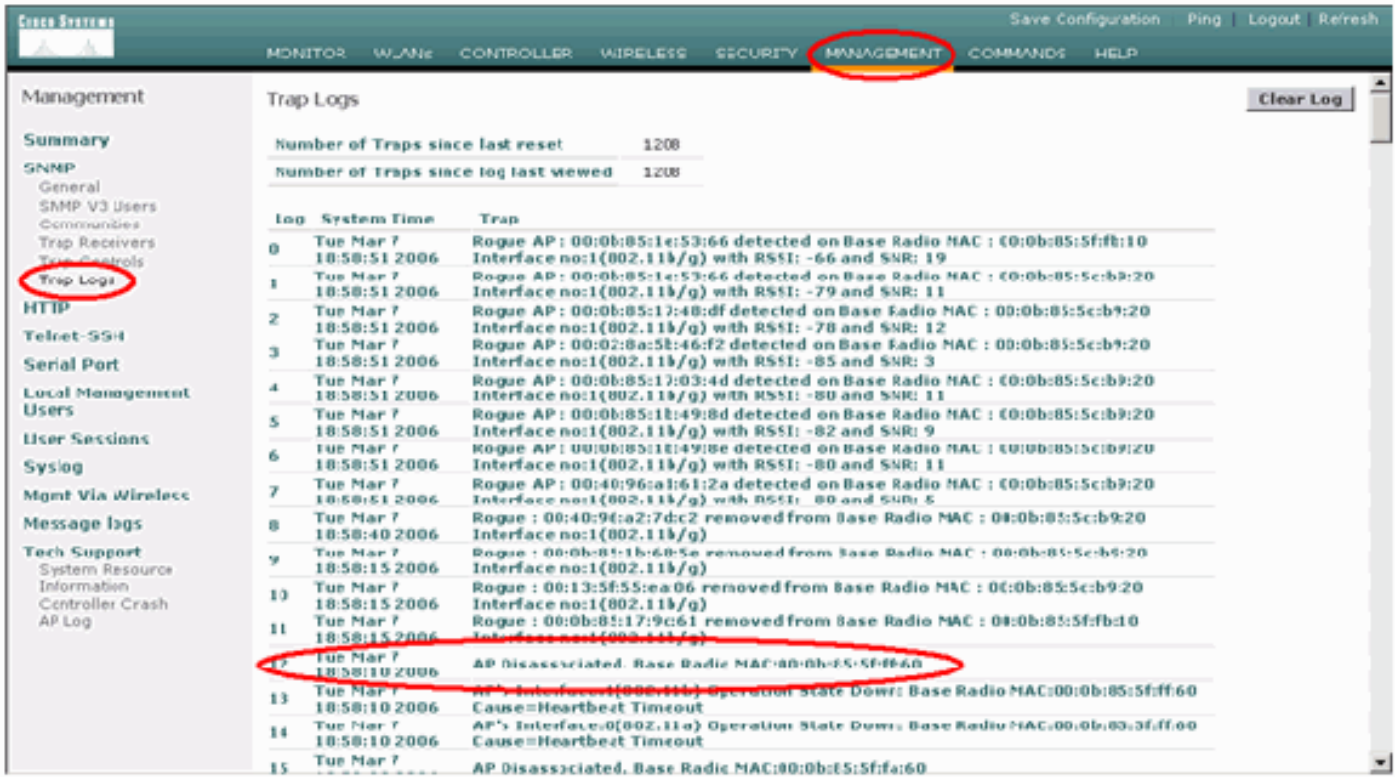
AP-logboek

Ga naar deze GUI-pagina op het controller om de AP-logbestanden voor uw lokale AP te controleren, indien aanwezig:



Vastlegging vallen

Ga naar deze GUI-pagina van de controller en controleer de Trap-vastlegging:



Prestaties

Startup Convergence Test

Convergentie is de tijd die een RAP/MAP heeft genomen om een stabiele LWAPP-verbinding met een WLAN-controller tot stand te brengen vanaf het moment dat deze voor het eerst werd opgestart zoals hieronder vermeld:

Convergentietest	Convergentietijd (min:sec)			
	RAP	MAP1	MAP2	MAP3
upgrade op afbeelding	2:34	3:50	5:11	6:38
Controller herstart	0:38	0:57	1:12	1:32
Infraroodmesh-netwerk	2:44	3:57	5:04	6:09
RAP-herstart	2:43	3:57	5:04	6:09
MAP opnieuw samenvoegen		3:58	5:14	6:25
MAP wijziging van parent (hetzelfde kanaal)		0:38		

WCS

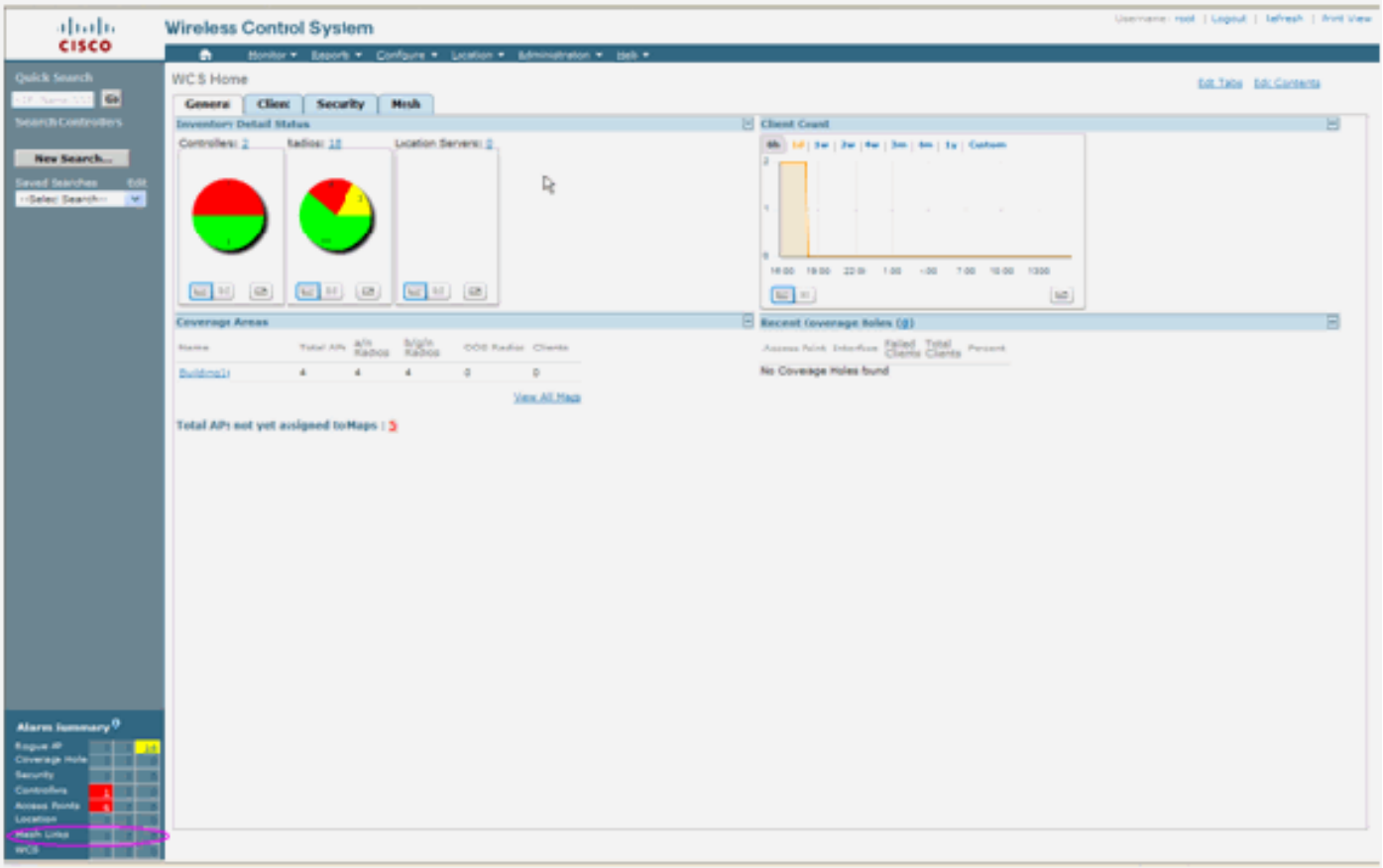
Reindeur mesh-alarmen

WCS zal deze alarmen en gebeurtenissen met betrekking tot het binnengaasnetwerk genereren op basis van de vallen van de controller:

- slechte link SNR

- ouder gewijzigd
- Kinderlicht verplaatst
- MAP Verandert parent regelmatig
- Console-poortgebeurtenis
- MAC-autorisatiefout
- Verificatiefouten
- Uitgesloten kind

Klik op **mesh-links**. Het zal alle alarmen met betrekking tot de maaswijdten binnen tonen.



Deze waarschuwingen zijn van toepassing op maaswijdten binnen:

- Slechte link SNR - Dit alarm wordt gegenereerd als de link SNR onder 12db daalt. De gebruiker kan deze drempel niet wijzigen. Als slechte SNR op de backhaul-link voor kind/ouder wordt gedetecteerd, wordt de val gegenereerd. De val zal SNR waarde en de MAC adressen bevatten. De ernst van de alarmen is groot. SNR (signaal-ruis) ratio is belangrijk omdat hoge signaalsterkte niet genoeg is om goede ontvangerprestaties te garanderen. Het inkomende signaal moet sterker zijn dan om het even welke lawaai of verstoring die aanwezig is. Het is bijvoorbeeld mogelijk om een hoge signaalsterkte te hebben en nog steeds slechte draadloze prestaties te hebben als er een sterke storing of een hoog geluidsniveau is.
- Ouder gewijzigd - Dit alarm wordt gegenereerd wanneer het kind naar een andere ouder wordt verplaatst. Wanneer het ouder wordt verloren, zal het kind zich bij een andere ouder voegen, en het kind zal een val verzenden die zowel de oude ouder- als de nieuwe MAC-adressen van de ouder aan WCS bevat. Alarmernst: Informatie.
- Kinderslot verplaatst - Dit alarm wordt gegenereerd wanneer WCS een kinderval krijgt. Wanneer het ouder AP zijn verlies van een kind ontdekte en niet met dat kind kon communiceren, zal het een Kind in verloor val naar WCS sturen. De val zal het kind MAC adres bevatten. Alarmernst: Informatie.

- MAP ouder is frequent veranderd - Dit alarm wordt gegenereerd als AP binnen in mesh vaak zijn ouder verandert. Wanneer de MAP ouder-change-teller de drempel binnen een bepaalde duur overschrijdt, zal zij een val naar WCS sturen. De val bevat het aantal tijden van MAP-wijzigingen en de duur van de tijd. Als er bijvoorbeeld 5 veranderingen binnen 2 minuten plaatsvinden, wordt de val verstuurd. Alarmernst: Informatie.
- Uitgesloten ouder - Dit alarm wordt gegenereerd wanneer een kind een ouder zwarte lijst heeft. Een kind kan een ouder blokkeren wanneer het kind er niet in slaagde om na een vast aantal pogingen op te sporen bij de controller. Het kind herinnert zich de ouder op de zwarte lijst en wanneer het kind zich bij het netwerk aansluit, stuurt het de val die het MAC-adres van de Zwarte Parent bevat en de duur van de zwarte lijst.

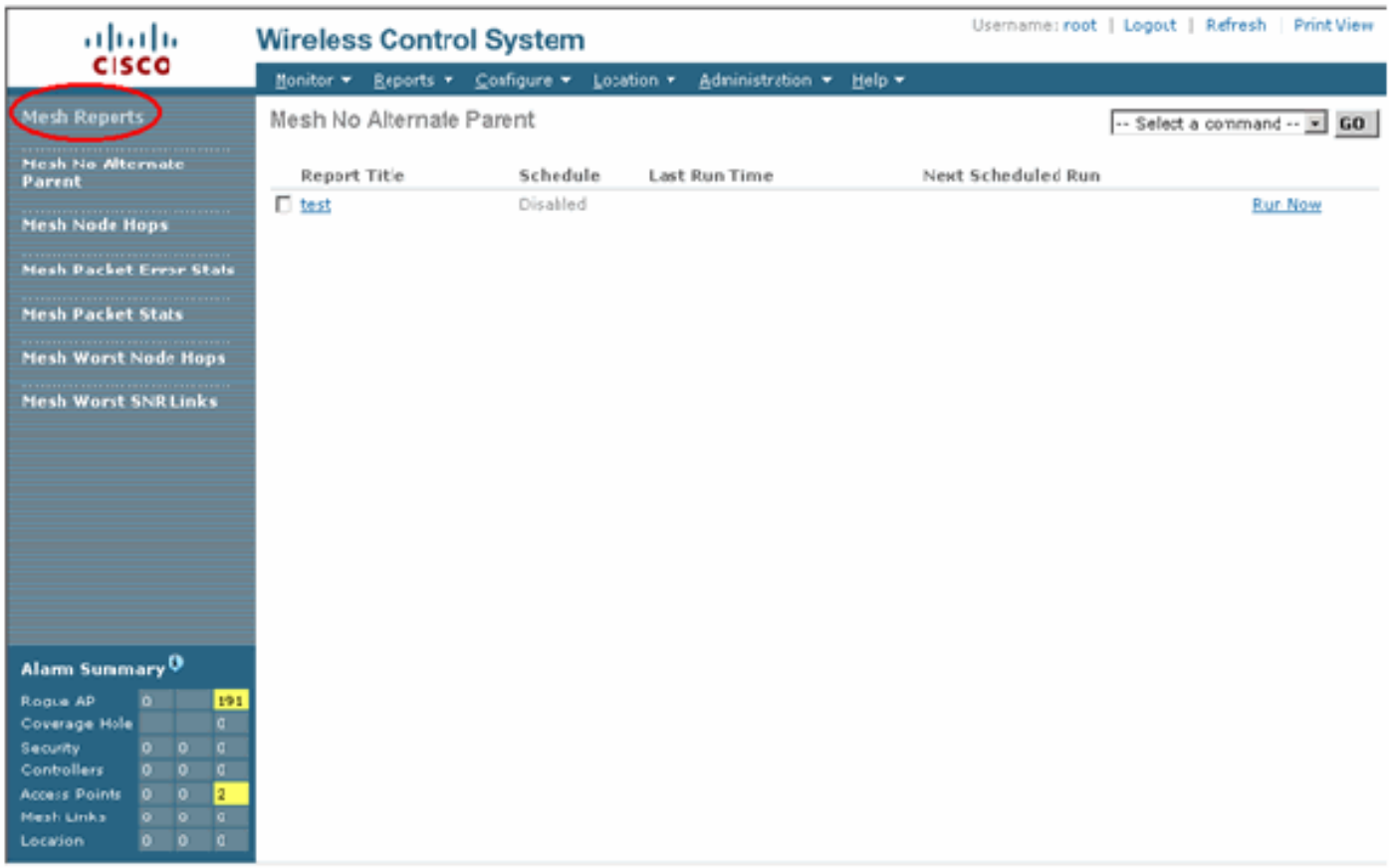
Andere alarmen dan binnenmaasverbindingen:

- Console Port Access - de console poort biedt de klant de mogelijkheid om de gebruikersnaam en het wachtwoord te wijzigen om de gestrande AP voor buitengebruik te herstellen. Echter, om elke geautoriseerde gebruiker toegang tot AP te verhinderen, moet WCS een alarm sturen wanneer iemand probeert in te loggen. Dit alarm is vereist om bescherming te bieden aangezien AP fysiek kwetsbaar is terwijl het zich buiten bevindt. Dit alarm zal worden gegenereerd als de gebruiker met succes aan de AP troostpoort heeft ingelogd, of als hij drie opeenvolgende malen heeft gefaald.
- MAC-autorisatie-fout - Dit alarm wordt gegenereerd wanneer AP probeert zich aan te sluiten bij het binnenmesh maar niet echt bevestig omdat het niet in de MAC-filterlijst staat. WCS krijgt een val van de controller. De val zal het MAC-adres van het AP bevatten dat de vergunning niet heeft verleend.

Verslag en statistieken mesh

Het uitgebreide verslag- en statistiekkader wordt van 4.1.185.0 overgeheveld:

- Geen alternatief pad
- mesh-knooppunt
- Packet error Stats
- Packet Stats
- slechtste knooppunt
- Ergste SNR-links



Geen alternatief pad

Binnenmesh AP heeft doorgaans meer dan één buur. Als een binnenvermaasd AP zijn ouderverbinding verliest zou AP de alternatieve ouder moeten kunnen vinden. In sommige gevallen, als er geen buren worden getoond, zal de AP niet naar andere ouders kunnen gaan als zij haar ouders verliest. Het is cruciaal voor de gebruiker om te weten welke AP's geen alternatieve ouders hebben. In dit verslag worden alle AP's opgesomd die geen andere buren hebben dan de huidige ouder.

Indoor mesh-knooppunt

Dit rapport laat het aantal hop zien weg van de Root AP (RAP). U kunt het rapport op basis van deze criteria opstellen:

- AP per controller
- AP op vloer

Packet-foutenpercentages

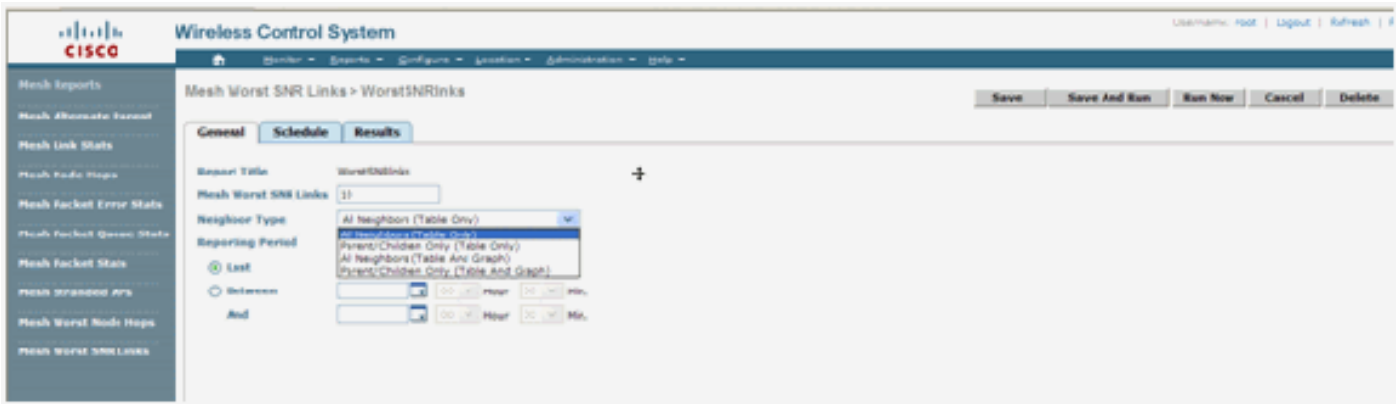
De pakketfouten kunnen worden veroorzaakt door interferentie en pakketdruppels. De berekening van de pakketfout is gebaseerd op verzonden pakketten en pakketten die met succes zijn verzonden. Het pakketfoutenpercentage wordt op de backhaul-link gemeten en wordt voor zowel de buren als de ouder verzameld. AP stuurt periodiek pakketinformatie naar de controller. Zodra het ouder verandert, stuurt AP de verzamelde pakketfoutinformatie naar de controller uit. WCS opinieert pakketfoutinformatie van de controller elke 10 minuten standaard en slaat deze op in de database voor maximaal 7 dagen. In WCS wordt het pakketfoutenpercentage als grafiek weergegeven. Het pakketfoutendiagram is gebaseerd op de historische gegevens die in de database zijn opgeslagen.

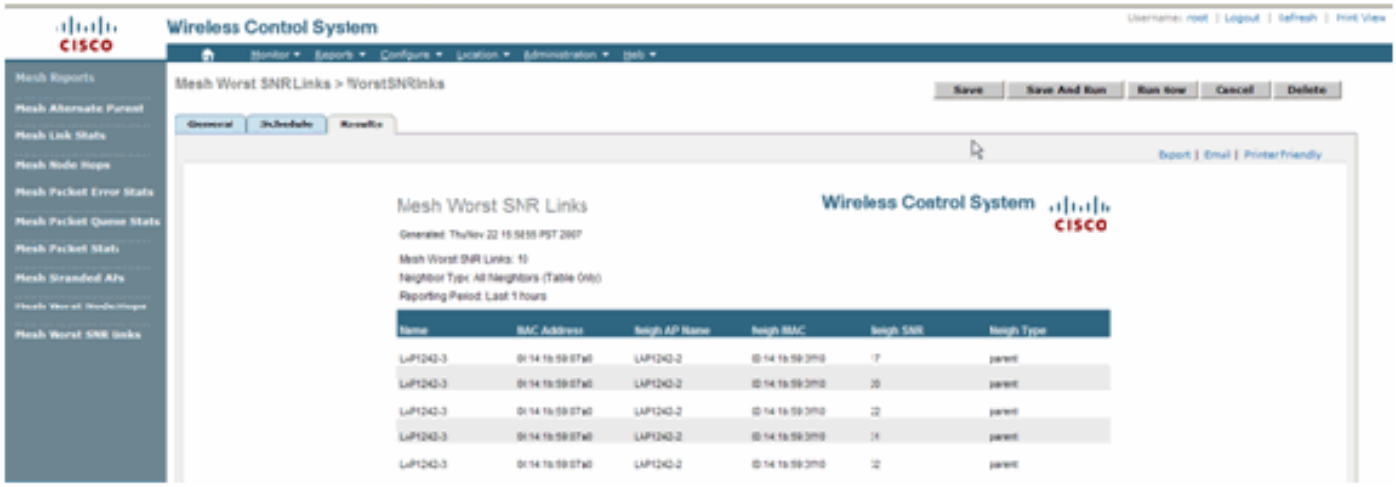
Packet Stats

Dit rapport toont de tegenwaarden van buurtotaal verzenden pakketten en de pakketten van de Buren Totale die met succes worden verzonden. U kunt het verslag op basis van bepaalde criteria opstellen.

De slechtste SNR-koppelingen

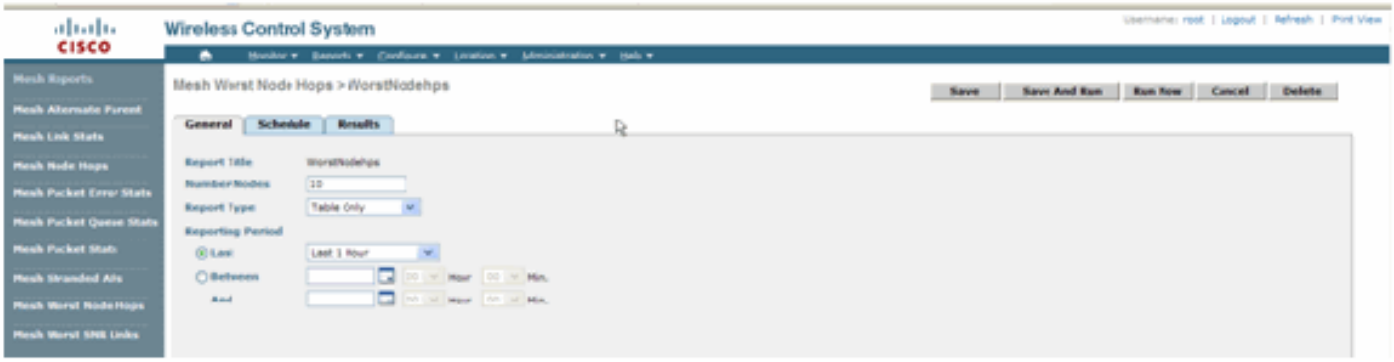
Ruisproblemen kunnen zich op verschillende tijdstippen voordoen en ruis kan in verschillende snelheden of gedurende verschillende tijdsduur toenemen. Het volgende cijfer biedt de mogelijkheid om rapport te maken voor zowel radio a en b/g als selectieve interfaces. Het rapport somt de 10 ergste SNR links standaard op. U kunt kiezen uit 5 tot 50 ergste koppelingen. Het rapport kan worden gegenereerd voor de laatste 1 uur, afgelopen 6 uur, afgelopen dag, afgelopen 2 dagen en tot 7 dagen. De gegevens worden standaard elke 10 minuten gevraagd. De gegevens worden maximaal zeven dagen in de gegevensbank bewaard. De selectiecriteria voor buurttype kunnen alleen alle buren, ouders/kinderen zijn.



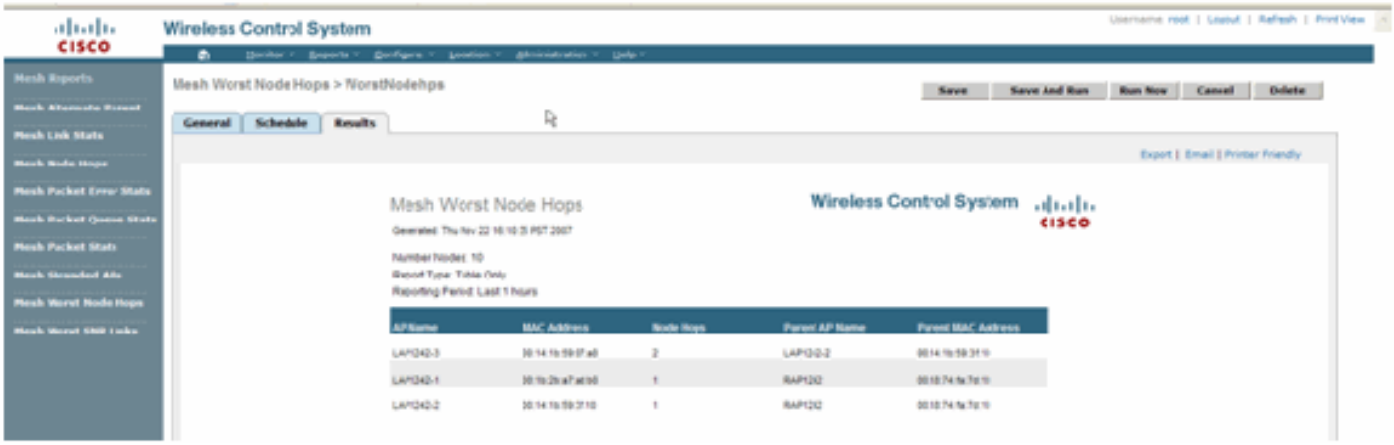


slechtste knooppunt

Dit rapport bevat standaard de 110 slechtste hop-AP's. Als de AP's te veel hoop weg zijn, zouden de verbindingen zeer zwak kunnen zijn. De gebruiker kan AP's isoleren die veel hops van Root AP hebben en de juiste actie ondernemen. U kunt ervoor kiezen dit **aantal knooppunten** tussen 5 en 50 te wijzigen. De criteria voor **het** type **rapport** in deze afbeelding kunnen alleen Tabel of Tabel en Grafiek zijn:



Dit getal laat het resultaat van het laatste verslag zien:



Security statistieken

De statistieken met betrekking tot mesh-beveiliging worden weergegeven op de pagina met AP-details onder het kopje Bridging. Een ingang in de Statistische tabel Indoor meshNodeSecurity wordt gecreëerd wanneer een kind binnenvermaasd knooppunt associeert of authenticeert met een parent Indoor mesh-knooppunt. Vermeldingen worden verwijderd wanneer het mesh-knooppunt van de controller verdwijnt.

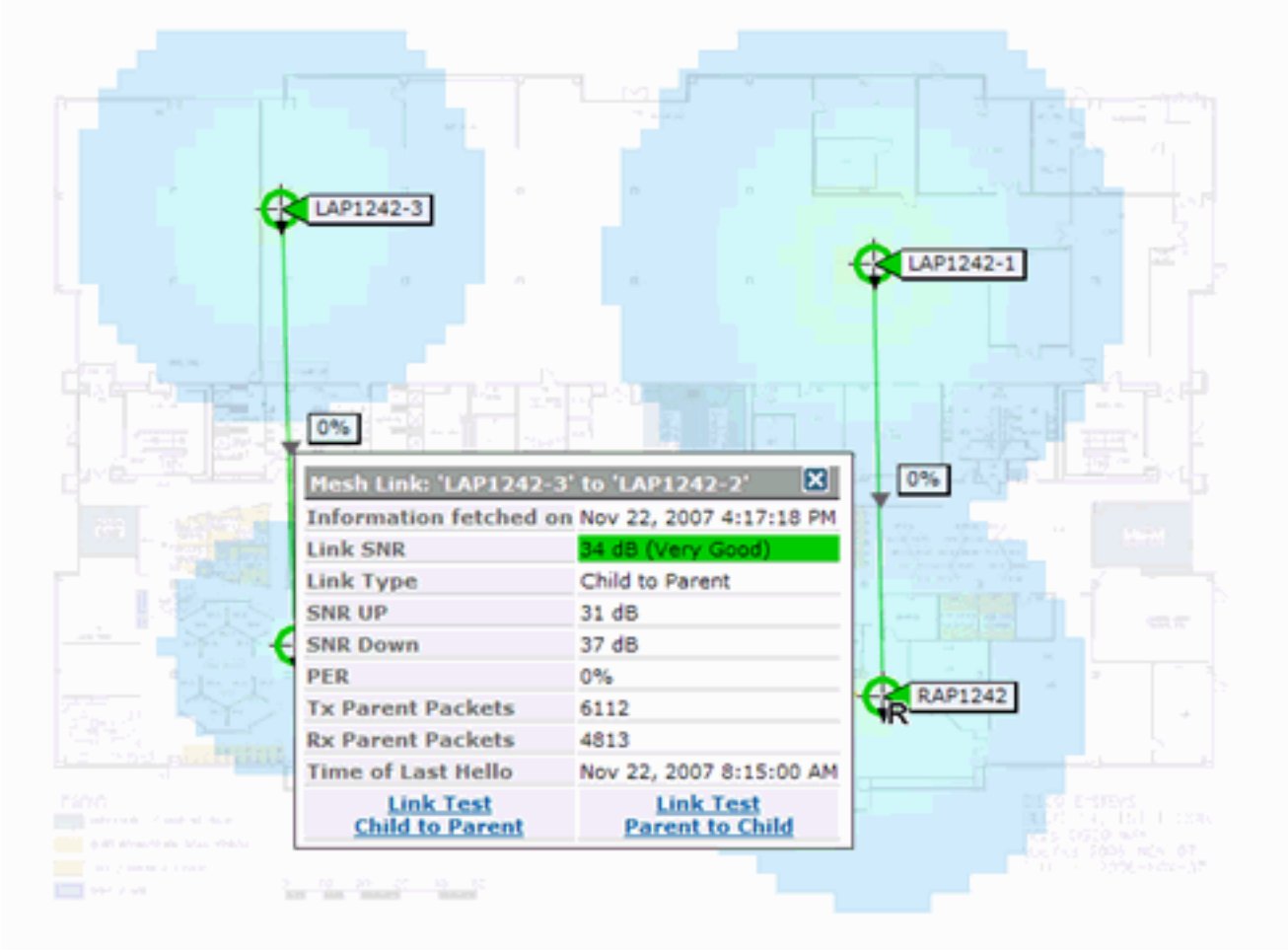
Koppeltest

De AP-to-AP verbindingstest wordt ondersteund op WCS. Men kan om het even welke twee APs selecteren en een verbindingstest tussen de twee gebruiken.

Als deze APs RF buren zijn, dan kan de verbindingstest een resultaat hebben. Het resultaat wordt in een dialoogvenster op de kaart zelf weergegeven zonder dat er een volledige pagina is opgefrist. Het dialoogvenster kan eenvoudig worden afgewerkt.

Als deze 2 AP's echter geen RF-buren zijn, dan probeert WCS geen pad tussen de 2 AP's te vinden om een combinatie van meerdere link-test te doen.

Wanneer de muis over het pijltje wordt verplaatst op de koppeling tussen de twee knooppunten, verschijnt dit venster:



Test knooppunt-to-knooppunt

Het Link Test-gereedschap is een on-demand tool om de verbindingskwaliteit tussen twee AP's te controleren. In WCS wordt deze optie toegevoegd op de pagina met AP-details.

Op de pagina met AP-details, onder het tabblad **Indoor mesh Link** waar de links naast de pagina staan, is er een link om de link-test uit te voeren.

Het controllergereedschap CLI Link heeft de optionele invoerparameters: Packet size, Total Link testpakketten, duur van test, en Data Link rate. De link test heeft standaardwaarden voor deze optionele parameters. De MAC-adressen voor de knooppunten zijn de enige verplichte invoerparameters.

Het gereedschap van de Koppel test sterkte, het verzonden pakket en het tussen knooppunten ontvangen pakket. De link voor de Test van de Koppel wordt in het AP detailrapport weergegeven. Wanneer u op de link klikt, is er een pop-upscherm dat de resultaten van de Link Test toont. De Link Test is alleen van toepassing op ouder-kind en tussen buren.

De uitvoer van de Test van de Koppel genereert verzonden, ontvangen Packets, foutenpakketten (emmers om diff redenen), SNR, Ruis Vloer, en RSSI.

De Lijntest geeft ten minste deze gegevens op de GUI:

- Verstuurde Link Test Packet
- Link Test Packets Ontvangen
- Signaalsterkte in dBm

- Verhouding signaal tot ruis

Links tussen buurlanden op aanvraag

Dit is een nieuwe optie in de WCS Map. U kunt op een mesh-eenheid klikken en er verschijnt een pop-upvenster met detailinformatie. U kunt dan op **Beeld mesh-buren** klikken, die de buurinformatie voor de geselecteerde AP ophalen en een tabel met alle buren voor de geselecteerde binnenvermaasde AP weergeven.

De View mesh buurband toont alle buren voor de gemarkeerde AP. Deze momentopname toont alle buren, het Type van de buren, en de SNR waarde.

Ping Test

De Ping Test is een On-demand gereedschap gebruikt om tussen de controller en AP te pingelen. Het Ping Test-gereedschap is beschikbaar in zowel de AP-detailpagina als in MAP. Klik op de koppeling **Ping Test uitvoeren** in de pagina met AP-details of in de informatie van de MAP AP om de ping van de controller naar de huidige AP te starten.

Conclusie

Enterprise Mesh (d.w.z. indoor mesh) is een uitbreiding van Cisco draadloze dekking naar plaatsen waar draadloos Ethernet geen connectiviteit kan bieden. Flexibiliteit en beheerbaarheid van een draadloos netwerk worden gerealiseerd met een netwerk van ondernemingen.

De meeste eigenschappen verbonden APs worden verstrekt door de topologie van het binnennetwerk. De voorzien van een netwerk van de onderneming kan ook naast de verbonden APs op de zelfde controller bestaan.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems