REAP-implementatiegids bij de Vestigingsvestiging

Inhoud

Inleiding

Dit document bevat informatie waarmee rekening moet worden gehouden bij de implementatie van Remote-Edge access point (REAP). Raadpleeg het Configuratievoorbeeld van Remote-Edge AP (REAP) met lichtgewicht AP's en draadloze LAN-controllers (WLC's) voor basisinformatie over de configuratie van REAP.

Opmerking: De optie REAP wordt ondersteund tot aan WLC release 3.2.215. Van WLC release 4.0.15.5 wordt deze functie Hybrid REAP (H-REAP) genoemd met weinig verbeteringen tot 7.0.x.x. Vanaf de release 7.2.103 heet deze functie FlexConnect.

Op basis van traditioneel Cisco lichtgewicht access point Protocol (LWAPP) gebaseerde access

points (ook wel LAP's genoemd), zoals de 1010, 1020 en de 1100 en 1200 Series AP's die Cisco IOS® softwarerelease 12.3(7)JX of hoger uitvoeren, kunnen centraal beheer en andere toepassingen controle door Cisco's draadloze LAN-controllers (WLC's). Deze LAP's stellen beheerders ook in staat om de controllers te gebruiken als enkele punten van draadloze gegevensaggregatie.

Terwijl deze LAP's controllers in staat stellen geavanceerde functies zoals QoS en toegangscontrolelijst (ACL's) uit te voeren, kan de eis dat de controller één enkel punt van toegang en stress is voor al het draadloze clientverkeer de mogelijkheid belemmeren om op adequate wijze aan de behoeften van de gebruiker te voldoen, in plaats van deze te kunnen realiseren. In sommige omgevingen, zoals afgelegen kantoren, kan de beëindiging van alle gebruikersgegevens bij controllers te intensief blijken, vooral wanneer de beperkte doorvoersnelheid beschikbaar is via een WAN-link. Tevens leidt het gebruik van LAP's die op WLC's vertrouwen voor de beëindiging van gebruikersgegevens tot doorgesneden draadloze connectiviteit tijdens een WAN-uitbraak, waar de koppelingen tussen LAP's en WLC's vaak te sterk zijn met WAN-verbindingen naar afgelegen kantoren.

In plaats daarvan kunt u een AP architectuur gebruiken waar het traditionele LWAPP controlevliegtuig hefboomwerking heeft om taken uit te voeren, zoals dynamisch configuratiebeheer, AP software upgrade, en draadloze inbraakdetectie. Dit maakt het mogelijk dat draadloze gegevens lokaal blijven, en de draadloze infrastructuur centraal wordt beheerd en veerkrachtig voor WAN-uitval.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

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

1030 REAP Architecture Inleiding

Cisco 1030 REAP scheidt het LWAPP besturingsplane van het draadloze gegevensvliegtuig om functionaliteit op afstand te bieden. Cisco WLC's worden nog steeds gebruikt voor gecentraliseerd beheer en beheer, op dezelfde manier als reguliere LAP's. Het verschil is dat alle gebruikersgegevens lokaal bij de AP zijn overbrugd. De toegang tot lokale netwerkbronnen wordt door WAN-uitgangen behouden. Afbeelding 1 illustreert een basis REAP-architectuur.

Afbeelding 1: BASIS REAP-architectuurdiagram

Toelichting: Zie Bijlage A voor een lijst van basisverschillen in de REAP-functionaliteit in vergelijking met traditionele LAP's.

Wanneer moeten REAP's worden gebruikt?

Cisco 1030 REAP moet primair onder deze twee voorwaarden worden gebruikt:

- Als de link tussen de LAP en WLC waarschijnlijk te veel uitvalt, kan de 1030 REAP worden gebruikt om draadloze gebruikers ononderbroken toegang tot gegevens toe te staan tijdens het uitvallen van de link.
- Als alle gebruikersgegevens lokaal moeten worden afgesloten, wat betekent in de bekabelde poort van de AP (in plaats van te worden beëindigd bij de controller, aangezien de gegevens voor alle andere LAP's gelden), kan de 1030 REAP worden gebruikt om centrale controle mogelijk te maken via de controller-interface en/of het draadloze controlesysteem (WCS). Hierdoor kunnen gegevens lokaal blijven.

Wanneer voor dekking of gebruikersdichtheid meer dan twee of drie 1030 REAP's op één locatie nodig zijn, moet u de invoering van een WLC van 2006 of 2106 overwegen. Deze controllers kunnen tot 6 LAP's van elk type ondersteunen. Dit kan financieel levensvatbaarder blijken te zijn, en een vervanging bieden van functies en functionaliteit in vergelijking met een uitsluitend REAP-toepassing.

Net als bij alle AP's van 1000 Series, bestrijkt één enkele AP van 1030 ongeveer 700 vierkante voet. Dit is afhankelijk van de radiofrequentie (RF)-propagatiekenmerken op elke locatie, en het vereiste aantal draadloze gebruikers en hun doorvoerbehoeften. Bij de meeste gebruikelijke implementaties kan één enkele 1000 Series AP 12 gebruikers ondersteunen bij 512 kbps op 802.11b en 12 gebruikers bij 2 mbps op 802.11a tegelijk. Net als bij alle 802.11-gebaseerde technologieën wordt de toegang tot de media gedeeld. Daarom wordt de doorvoersnelheid wanneer meer gebruikers zich bij de draadloze AP aansluiten, dienovereenkomstig gedeeld. Nogmaals, aangezien de gebruikersdichtheid stijgt en/of de doorvoervereisten stijgen, overweeg de toevoeging van een lokale WLC om op kosten-per-gebruiker te besparen en de functionaliteit te vergroten.

Opmerking: U kunt de 1030 REAPs configureren om op dezelfde manier te werken als andere LAPs. Daarom kunnen bestaande REAP-investeringen, wanneer WLC's worden toegevoegd om de grootte van de WLAN-infrastructuur van externe locaties te schalen, ook verder worden aangewend.

REAP implementeren

Omdat de 1030 REAP ontworpen is om op afgelegen plaatsen ver van de WLC infrastructuur te worden geplaatst, worden de traditionele, nul-aanraking methodes die LAPs worden gebruikt om controllers (zoals DHCP optie 43) te ontdekken en zich aan te sluiten meestal niet gebruikt. In plaats daarvan moet de LAP eerst worden geprimeerd zodat de 1030 verbinding kan maken met een WLC-verbinding op een centrale locatie.

Priming is een proces waarbij LAP's een lijst krijgen van WLC's waaraan ze kunnen verbinden. Zodra zij tot één enkele WLC zijn toegetreden, worden LAP's op de hoogte gesteld van alle controllers in de mobiliteitsgroep en zijn zij uitgerust met alle informatie die nodig is om zich aan te sluiten bij een controller in de groep. Raadpleeg het gedeelte Cisco 440X Series draadloze LAN-controllers voor meer informatie over mobiliteitsgroepen, taakverdeling en redundantie van controllers.

Om dit op de centrale plaats, zoals een netwerk operatiecentrum (NOC) of datacenter, te kunnen uitvoeren, moeten REAPs op het bekabelde netwerk worden aangesloten. Hierdoor kunnen ze één enkele WLC ontdekken. Nadat hij is aangesloten op een controller, downloaden de LAP OS-versie die overeenkomt met de WLAN-infrastructuur. Vervolgens worden de IP-adressen van alle WLC's in de mobiliteitsgroep overgedragen naar de AP's. Dit staat APs toe, wanneer aangedreven op hun verre plaatsen, om de minst gebruikte controller uit hun lijsten te ontdekken en aan te sluiten, op voorwaarde dat IP connectiviteit beschikbaar is.

Opmerking: DHCP-optie 43 en Domain Name System (DNS)-raadpleging werken ook met REAP's. Raadpleeg het gedeelte Cisco 440X Series draadloze LAN-controllers voor informatie over de manier waarop u DHCP of DNS op externe locaties kunt configureren om AP's in staat te stellen centrale controllers te vinden.

Op dat moment kan 1030 statische adressen worden gegeven indien gewenst. Dit waarborgt dat het IP-adresseringsschema overeenkomt met de locatie op de bestemming. Bovendien kunnen WLCs-namen worden ingevoerd om te specificeren welke drie controllers elke LAP probeert aan te sluiten. Indien deze drie niet slagen, staat de automatische load-balances van LWAPP de LAP toe om de minst geladen AP uit de resterende lijst van controllers in de cluster te kiezen. U kunt de LAP-configuratie bewerken via de WLC-opdrachtregel-interface (CLI) of GUI, of met meer gemak, via de WCS.

Opmerking: 1030 REAPs vereisen de WLCs waarmee zij verbinden om in Layer 3 LWAPP-modus te werken. Dit betekent dat de controllers IP adressen moeten krijgen. Bovendien moeten de WLC's een DHCP-server beschikbaar stellen op elke externe site, of statische adressen worden toegewezen tijdens het voorbereidingsproces. De DHCP-functionaliteit ingesloten in controllers kan niet worden gebruikt om adressen te geven aan LAP's van 1030s of hun gebruikers.

Zorg er voor dat elke 1030 op de REAP-modus is ingesteld voordat u de 1030 LAP's uitzet om naar afgelegen locaties te verschepen. Dit is heel belangrijk omdat de standaard voor alle LAP's is om regelmatig, lokaal te functioneren, en 1030s moet worden ingesteld om de REAP-functionaliteit uit te voeren. Dit kan op LAP-niveau worden gedaan via de CLI of GUI van de controller, of met meer gemak, door middel van WCS-sjablonen.

Basis REAP Priming-functies

Nadat 1030 REAP's zijn aangesloten op een WLC binnen de mobiliteitsgroep waar REAP's verbonden zijn met wanneer zij op afgelegen locaties worden geplaatst, kan deze informatie worden verstrekt:

Vereiste REAP-instellingen

- Een lijst van IP-adressen voor de WLC in de mobiliteitsgroep (automatisch beschikbaar bij controller/AP-verbinding)
- AP Mode (APs) moet worden geconfigureerd om in REAP-modus te werken om REAP-

functionaliteit uit te voeren)

Optionele REAP-instellingen

- Statisch toegewezen IP-adressen (een optionele instellingsingang op een per-AP-basis)
- Primaire, secundaire en tertiaire WLC-namen (een optionele instellingsinvoer op een per-AP-basis of via WCS-sjablonen)
- AP naam (een optionele informatie setting op a-AP basis)
- AP locatieinformatie (een optionele informationele instelling input op een per-AP-basis of via WCS-sjablonen)

Vereisten van REAP-to-Controller link

Wanneer u REAP's wilt inzetten, moeten een paar basisvereisten in acht worden genomen. Deze vereisten betreffen de snelheid en de snelheid van het WAN links REAP LWAPP controle verkeer zal verplaatsen. De 1030 LAP is bedoeld voor gebruik via WAN-koppelingen, zoals IP-beveiligingstunnels, Frame Relay, DSL (niet PPPoE) en huurlijnen.

Opmerking: De REAP LWAPP-implementatie van 1030 gaat uit van een MTU-pad van 1500 bytes tussen de AP en de WLC. Elke fragmentatie die zich voordoet in doorvoer door een MTU van minder dan 1500 leidt tot onvoorspelbare resultaten. Daarom is de LAP 1030 niet geschikt voor omgevingen, zoals PPPoE, waar routers actief pakketten fragmenteren naar sub-1500 bytes.

WAN-koppelingslatentie is met name belangrijk omdat elke 1030 LAP per 30 seconden een hartslag-bericht terugstuurt naar controllers. Nadat de hartslag berichten verloren zijn, sturen de LAP's 5 opeenvolgende hartslagen, één keer per seconde. Als geen van allen succesvol zijn, bepaalt de LAP dat de connectiviteit van de controller doorgesneden is en de 1030s terugkeren naar de standalone REAP-modus. Hoewel de LAP 1030 grote latenties tussen zichzelf en de WLC kan tolereren, moet ervoor worden gezorgd dat de latentie niet meer dan 100 ms tussen de LAP en de controller bedraagt. Dit is het gevolg van timers aan de cliënt die de hoeveelheid tijd die klanten wachten beperken alvorens de timers vaststellen dat een authenticatie heeft gefaald.

REAP-beperkingen

Hoewel de 1030 AP ontworpen is om centraal te worden beheerd en om de dienst van WLAN tijdens de uitvoer van WAN te verlenen, zijn er een paar verschillen tussen welke diensten REAP met de connectiviteit van WLC biedt en wat het kan verstrekken wanneer de connectiviteit wordt verbroken.

WLAN’s

Terwijl 1030 REAP tot 16 WLAN’s kan ondersteunen (draadloze profielen die een Service Set Identifier [SSID] bevatten, samen met alle beveiliging, QoS en ander beleid), elk met zijn eigen Multiple Basic Service Set-id (MBSSID), kan de 1030 REAP alleen de eerste WLAN ondersteunen wanneer de connectiviteit met een controller wordt onderbroken. Tijdens tijden van WAN-koppelingsbeëindiging worden alle WLAN’s behalve de eerste beëindigd. Daarom dient WLAN 1 bedoeld te zijn als primaire WLAN en dient het beveiligingsbeleid dienovereenkomstig te worden geprogrammeerd. Beveiliging op deze eerste WLAN-router is met name belangrijk omdat als de WAN-link faalt, dit ook geldt voor de backend-RADIUS-verificatie. Dit komt doordat dergelijk verkeer het LWAPP-besturingsplane oversteekt. Daarom krijgen gebruikers geen draadloze

toegang.

Aanbevolen wordt om een lokale verificatie/encryptie-methode, zoals het vooraf gedeelde sleutelgedeelte van Wi-Fi Protected Access (WAP-PSK), te gebruiken op deze eerste WLAN. Wired Equivalent Privacy (EFN) is voldoende, maar wordt niet aanbevolen vanwege bekende security kwetsbaarheden. Wanneer WAP-PSK (of EVN) wordt gebruikt, kunnen correct geconfigureerd gebruikers nog steeds toegang krijgen tot lokale netwerkbronnen, zelfs als de WAN-link plat is.

Opmerking: Alle op RADIUS gebaseerde beveiligingsmethoden vereisen dat de authenticatieberichten worden verzonden over het LWAPP-besturingsplane terug naar de centrale site. Daarom zijn alle op RADIUS gebaseerde services niet beschikbaar tijdens WAN-uitval. Dit omvat, maar is niet beperkt tot, RADIUS-gebaseerde MAC-verificatie, 802.1X, WAP, WAP2 en 802.11i.

De 1030 REAP kan slechts op één enkele vorm van netwerk verblijven omdat het geen 802.1q VLAN-markering kan uitvoeren. Daarom eindigt het verkeer op elke SSID op dezelfde slechts netwerk op het bekabelde netwerk. Dit betekent dat terwijl draadloos verkeer via de lucht tussen SSID's kan worden gesegmenteerd, het gebruikersverkeer niet aan de bekabelde kant van elkaar wordt gescheiden.

Security

1030 REAP kan al Layer 2 veiligheidsbeleid bieden dat door de op controller gebaseerde WAN-architectuur van Cisco wordt ondersteund. Dit omvat alle Layer 2-verificatie en coderingstypen, zoals EVN, 802.1X, WAP, WAP2 en 802.11i. Zoals eerder vermeld, vereist het meeste van dit veiligheidsbeleid connectiviteit van de WLC voor achterste authenticatie. De anti-dumpingcontroles van de anti-dumpingrechten van de Verenigde Staten worden volledig uitgevoerd op het AP-niveau en vereisen geen backend RADIUS-verificatie. Daarom kunnen gebruikers, zelfs als de WAN-link is verbroken, nog steeds verbinding maken. De optie van de lijst van klantuitsluitingen in Cisco WLC wordt ondersteund met de LAP 1030. MAC-filtering werkt op de 1030 als connectiviteit terug naar de controller beschikbaar is.

Opmerking: REAP steunt geen WAP2-PSK wanneer AP in standalone modus is.

Alle Layer 3 beveiligingsbeleid is niet beschikbaar bij de LAP 1030. Dit beveiligingsbeleid omvat web-verificatie, op controllers gebaseerde VPN-beëindiging, ACL's en peer-to-peer blokkering, omdat ze bij de controller worden geïmplementeerd. VPN pass-through werkt voor klanten die verbinding maken met externe VPN-concentrators. De controller die alleen verkeer toestaat dat bestemd is voor een gespecificeerde VPN-concentrator (alleen VPN-doorgifte) doet dit echter niet.

Netwerkadresomzetting (NAT)

WLC's waarmee REAP's verbonden zijn, kunnen niet achter NAT-grenzen blijven. REAP's op afgelegen sites kunnen echter achter een NAT-doos zitten, mits de poorten die gebruikt worden voor LWAPP (UDP-poorten 12222 en 12223) naar de jaren 1030 worden doorgestuurd. Dit betekent dat elke REAP een statisch adres moet hebben zodat het doorsturen van havens betrouwbaar kan werken, en dat slechts één enkele AP achter elke NAT-instantie kan wonen. De reden hiervoor is dat er slechts één poortverzendende instantie per NAT IP-adres kan bestaan, wat betekent dat slechts één LAP achter elke NAT-service op afgelegen locaties kan werken. Een-op-één NAT kan met meerdere REAP's werken omdat de LWAPP poorten voor elk extern IP adres naar elk intern IP adres (statisch REAP IP-adres) kunnen worden doorgestuurd.

QoS-kwaliteit (Quality of Service)

Packet Priority-bits op basis van 802.1p prioriteitsbits is niet beschikbaar omdat REAP geen 802.1q-markering kan uitvoeren. Dit betekent dat Wi-Fi Multimedia (WM) en 802.11e niet worden ondersteund. Packet prioritering op basis van SSID's en netwerken voor Identity Bases worden ondersteund. VLAN-toewijzing via Op identiteit gebaseerde netwerken werkt echter niet met REAP omdat er geen 802.1q-markering kan worden uitgevoerd.

roaming en taakverdeling voor klanten

In omgevingen waar meer dan één enkele REAP aanwezig is en waar de mobiliteit tussen-AP verwacht wordt, moet elke LAP op zelfde subnet zijn. Layer 3 mobiliteit wordt niet ondersteund in de LAP 1030. Meestal is dit geen beperking, omdat verafgelegen kantoren meestal niet genoeg LAP's gebruiken om een dergelijke flexibiliteit nodig te hebben.

Gegressieve taakverdeling voor klanten is beschikbaar op alle REAP's op locaties met meer dan één AP wanneer de upstream controller-connectiviteit beschikbaar is (alleen is load-balanceren op de host controller ingeschakeld).

Radio Resource Management (RRM)

Wanneer connectiviteit met controllers aanwezig is, ontvangen 1030 LAPs dynamische kanaaloutput en stroomoutput van het RRM mechanisme in WLCs. Wanneer de WAN-link is ingedrukt, werkt RRM niet en worden de kanaal- en stroominstellingen niet gewijzigd.

Soortdetectie en IDS-functies

De REAP-architectuur ondersteunt alle schurkendetectie en inbraakdetectiehandtekeningen (IDS) die overeenkomen met die van reguliere LAP's. Wanneer de connectiviteit echter verloren gaat met een centrale controller, wordt alle verzamelde informatie niet gedeeld. Daarom is de zichtbaarheid in de RF-domeinen van afgelegen locaties verloren.

Samenvatting van REAP-beperking

De tabel in Bijlage B vat de mogelijkheden van REAP tijdens normaal gebruik samen en wanneer verbinding met de WLC over de WAN-link niet beschikbaar is.

REAP en Central WLAN-architectuur beheren

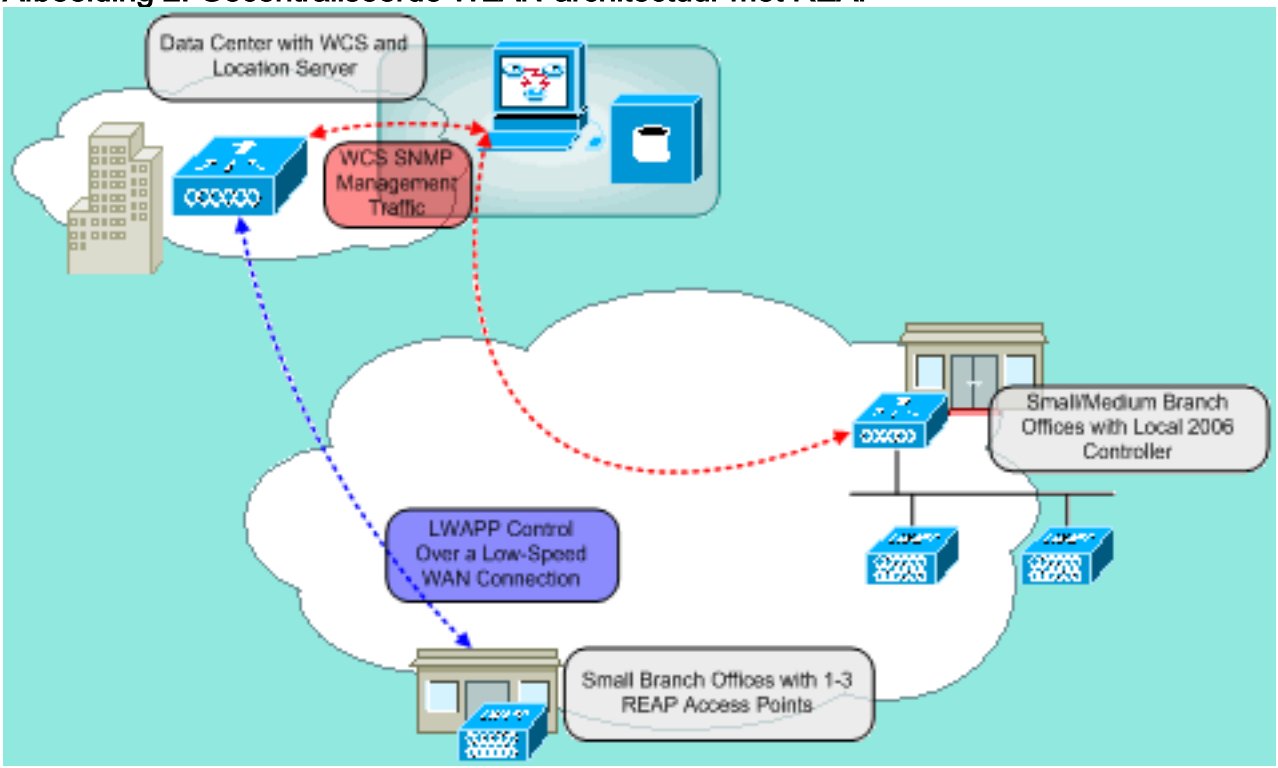
1030 REAP management is niet anders dan dat van gewone LAP's en WLC's. Het beheer en de configuratie worden allemaal uitgevoerd op het niveau van de controller, hetzij via de CLI van elke controller, hetzij via een web GUI. De configuratie- en netwerkzichtbaarheid voor het hele systeem worden verleend via de WCS, waar alle controllers en AP's (REAP of anderszins) als één systeem kunnen worden beheerd. Wanneer de REAP-controller connectiviteit is verstoord, worden de beheermogelijkheden ook verstoord.

Gecentraliseerde WLAN-architectuur met REAP

Afbeelding 2 toont hoe elk deel van de gecentraliseerde LWAPP-architectuur samen werkt om aan

een verscheidenheid aan draadloze netwerkbehoeften te voldoen. Beheer en locatieservices worden centraal verleend via de WCS en de 2700 Locatie applicatie.

Afbeelding 2: Gecentraliseerde WLAN-architectuur met REAP



Bijlage A

Wat zijn de belangrijkste verschillen tussen de REAP-architectuur en de reguliere LAP's?

- Als DHCP-optie 43 of DNS-resolutie niet beschikbaar is op externe locaties, moet 1030 eerst op het centrale kantoor worden voorbereid. Het is naar de bestemming gebracht.
- Op een fout in WAN-link blijft alleen het eerste WLAN actief.Veiligheidsbeleid dat een RADIUS-toets vereist, mislukt.Verificatie/encryptie die WAP-PSK gebruikt wordt aanbevolen voor WLAN 1. WLAN werkt, maar wordt niet aanbevolen.
- Geen Layer 3-encryptie (alleen Layer 2-encryptie)
- WLC's die REAP's verbinden met kunnen niet achter NAT-grenzen wonen. REAPs kan echter, op voorwaarde dat elk intern statisch REAP IP adres zowel LWAPP poorten (12222 en 12223) aan hen heeft doorgestuurd.**Opmerking:** Port Address Translation (PAT) / NAT met overlading wordt niet ondersteund omdat de bronpoort van het LWAPP-verkeer dat afkomstig is van de LAP in de loop der tijd kan worden gewijzigd. Dit breekt de LWAPP-associatie. Het zelfde probleem kan zich voordoen met NAT implementaties voor REAP waar het havenadres verandert, zoals PIX/ASA, wat van de configuratie afhangt.
- Alleen LWAPP controle berichten verplaatsen de WAN-link.
- Het gegevensverkeer wordt overbrugd op de Ethernet-poort van de 1030.
- De LAP 1030 voert geen 802.1Q markering (VLAN's) uit. Daarom eindigt draadloos verkeer van alle SSIDs op het zelfde bedrade net.

Bijlage B

Wat zijn de verschillen in functionaliteit tussen de normale en standalone REAP-modi?

		REAP (normale modus)	REAP (standalone modus)
Protocols	IPv4	Ja	Ja
	IPv6	Ja	Ja
	Alle andere protocollen	Ja (alleen als client ook IP is ingeschakeld)	Ja (alleen als client ook IP is ingeschakeld)
	IP proxy-ARP	Nee	Nee
WLAN	Aantal SSID's	16	1 (de eerste)
	Dynamische kanaaltoewijzing	Ja	Nee
	Dynamische stroomregeling	Ja	Nee
	Dynamische taakverdeling	Ja	Nee
VLAN	Meervoudige interfaces	Nee	Nee
	Ondersteuning van 802.1Q	Nee	Nee
WLAN-beveiliging	Detectie van AP-schurk	Ja	Nee
	Uitsluitingslijst	Ja	Ja (alleen bestaande leden)
	Peer-to-peer blokkering	Nee	Nee
	Inbraakdetectiesysteem	Ja	Nee
Layer 2 security	MAC-verificatie	Ja	Nee
	802,1x	Ja	Nee
	64/128/152-bits	Ja	Ja

	WAP-PSK	Ja	Ja
	WAP2-PSK	Ja	Nee
	GOEDKOPE	Ja	Nee
	WAP2-MAP	Ja	Nee
Layer 3 beveiliging	Web verificatie	Nee	Nee
	IPsec	Nee	Nee
	L2TP	Nee	Nee
	VPN-doorvoer	Nee	Nee
	Toegangscontrolelijsten	Nee	Nee
QoS	QoS-profielen	Ja	Ja
	Downlink QoS (gewogen round-robin wachtrijen)	Ja	Ja
	Ondersteuning van 802.1p	Nee	Nee
	Contracten voor bandbreedte per gebruiker	Nee	Nee
	WMM	Nee	Nee
	802.11e (toekomst)	Nee	Nee
	AAA QoS-profiel omzeilen	Ja	Nee
Mobiliteit	Intra-Subnet	Ja	Ja
	Inter-Subnet	Nee	Nee
DHCP	Interne DHCP-	Nee	Nee

	server		
	Externe DHCP-server	Ja	Ja
Topologie	Direct Connect (2006)	Nee	Nee

Gerelateerde informatie

- Configuratievoorbeeld van Remote-Edge AP (REAP) met lichtgewicht AP's en draadloze LAN-controllers (WLC's)
- AP-taakverdeling en AP-back-up in Unified draadloze netwerken
- Deploying Cisco 440X Series Wireless LAN Controllers (Cisco 440X Series wireless LAN-controllers implementeren)
- Configuratievoorbeeld voor draadloos LAN-controller en lichtgewicht access point
- Technische ondersteuning en documentatie – Cisco Systems