Guida alla distribuzione di REAP presso le filiali

Sommario

Introduzione

In questo documento vengono fornite le informazioni di cui è necessario tenere conto quando si distribuisce il punto di accesso remoto (REAP, Remote-Edge Access Point). Per informazioni di base sulla configurazione del protocollo REAP, fare riferimento agli esempi di configurazione dei Remote-Edge AP (REAP) con Lightweight AP e Wireless LAN Controller (WLC).

Nota: la funzione REAP è supportata fino alla versione WLC 3.2.215. Dalla versione WLC 4.0.155.5, questa funzionalità è denominata Hybrid REAP (H-REAP) con alcuni miglioramenti fino alla versione 7.0.x.x. Dalla versione 7.2.103, questa funzione è denominata FlexConnect.

I Cisco Lightweight Access Point Protocol (LWAPP)-based Access Point (AP) tradizionali, (noti anche come LAP), come i 1010, 1020 e le serie 1100 e 1200 AP con software Cisco IOS® versione 12.3(7)JX o successive, consentono la gestione e il controllo centrali tramite i Wireless

LAN Controller (WLC) di Cisco. Inoltre, questi LAP consentono agli amministratori di utilizzare i controller come singoli punti di aggregazione dei dati wireless.

Mentre questi LAP permettono ai controller di eseguire funzioni avanzate come QoS e applicazione degli Access Control List (ACL), la necessità che il controller sia un singolo punto di ingresso e uscita per tutto il traffico client wireless può ostacolare, più che consentire, la capacità di soddisfare adeguatamente le esigenze degli utenti. In alcuni ambienti, ad esempio negli uffici remoti, la terminazione di tutti i dati utente sui controller può rivelarsi troppo dispendiosa in termini di larghezza di banda, soprattutto quando la velocità di trasmissione è limitata su un collegamento WAN. Inoltre, se i collegamenti tra i LAP e i WLC sono soggetti a interruzioni, come accade spesso con i collegamenti WAN agli uffici remoti, l'uso dei LAP che si basano sui WLC per la terminazione dei dati degli utenti causa l'interruzione della connettività wireless durante le interruzioni della WAN.

Al contrario, è possibile utilizzare un'architettura AP in cui il control plane LWAPP tradizionale viene utilizzato per eseguire attività quali la gestione della configurazione dinamica, l'aggiornamento del software AP e il rilevamento delle intrusioni wireless. Ciò consente ai dati wireless di rimanere locali e all'infrastruttura wireless di essere gestita centralmente e resiliente alle interruzioni della WAN.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Introduzione all'architettura 1030 REAP

Il Cisco 1030 REAP separa il control plane LWAPP dal data plane wireless per fornire funzionalità remote. I WLC Cisco vengono ancora utilizzati per il controllo e la gestione centralizzati allo stesso modo dei LAP standard. La differenza è che tutti i dati utente vengono collegati localmente all'access point. L'accesso alle risorse di rete locali viene mantenuto durante le interruzioni della WAN. La Figura 1 illustra un'architettura REAP di base.

Figura 1: Diagramma dell'architettura REAP di base

Nota: vedere Appendice A per un elenco delle differenze di base nella funzionalità REAP rispetto ai LAP tradizionali.

Quando utilizzare i REAP AP?

Cisco 1030 REAP AP deve essere utilizzato principalmente nelle due condizioni seguenti:

- Se il collegamento tra il LAP e il WLC è soggetto a interruzioni, il REAP 1030 può essere utilizzato per consentire agli utenti wireless un accesso ininterrotto ai dati in caso di errore del collegamento.
- Se tutti i dati dell'utente devono essere terminati localmente, ossia sulla porta cablata dell'access point (invece di essere terminati sul controller, come avviene per tutti gli altri LAP), il punto di accesso 1030 REAP può essere utilizzato per consentire il controllo centrale tramite l'interfaccia del controller e/o il sistema di controllo wireless (WCS). In questo modo i dati rimangono locali.

Se la copertura o la densità degli utenti richiedono più di due o tre 1030 REAP in un singolo sito, si consiglia di implementare un WLC 2006 o 2106. Questi controller possono supportare fino a 6 LAP di qualsiasi tipo. Questa soluzione è più redditizia dal punto di vista finanziario e offre un soprainsieme di funzionalità e caratteristiche rispetto a un'installazione solo REAP.

Come per tutti i access point serie 1000, un singolo access point serie 1030 copre circa 1500 metri quadrati. Ciò dipende dalle caratteristiche di propagazione della radiofrequenza (RF) in ciascun sito e dal numero richiesto di utenti wireless e dalle relative esigenze di velocità di trasmissione. Nella maggior parte delle implementazioni comuni, un singolo access point serie 1000 può supportare contemporaneamente 12 utenti a 512 kbps su 802.11b e 12 utenti a 2 mbps su 802.11a. Come tutte le tecnologie basate su 802.11, l'accesso ai contenuti multimediali è condiviso. Pertanto, quando più utenti si uniscono all'access point wireless, la velocità di trasmissione viene condivisa di conseguenza. Anche in questo caso, con l'aumento della densità degli utenti e/o dei requisiti di throughput, è opportuno considerare l'aggiunta di un WLC locale per risparmiare sul costo per utente e aumentare la funzionalità.

Nota: è possibile configurare i 1030 REAP in modo che funzionino esattamente come gli altri LAP. Pertanto, quando si aggiungono i WLC per scalare le dimensioni dell'infrastruttura WLAN dei siti remoti, è possibile continuare a sfruttare gli investimenti REAP esistenti.

Distribuisci REAP

Poiché il protocollo 1030 REAP è progettato per essere installato in siti remoti lontano dall'infrastruttura WLC, i tradizionali metodi zero-touch LAP utilizzati per rilevare e collegare i controller (come l'opzione DHCP 43) di solito non vengono utilizzati. Al contrario, il LAP deve essere innescato per consentire al 1030 di collegarsi ad un WLC in un sito centrale.

Il priming è un processo in cui ai LAP viene assegnato un elenco di WLC a cui possono connettersi. Una volta uniti a un singolo WLC, i LAP vengono informati di tutti i controller del gruppo di mobilità e vengono dotati di tutte le informazioni necessarie per unirsi a qualsiasi controller del gruppo. Per ulteriori informazioni sui gruppi di mobilità, sul bilanciamento del carico e sulla ridondanza dei controller, fare riferimento a Implementazione dei Cisco Wireless LAN Controller serie 440X.

Per eseguire questa operazione nella sede centrale, ad esempio un centro operativo di rete

(NOC) o un centro dati, i REAP devono essere collegati alla rete cablata. Ciò consente loro di scoprire un singolo WLC. Una volta aggiunti a un controller, i LAP scaricano la versione del sistema operativo LAP corrispondente all'infrastruttura WLAN. Quindi, gli indirizzi IP di tutti i WLC nel gruppo di mobilità vengono trasferiti agli access point. In questo modo, una volta accesi presso i siti remoti, gli access point possono rilevare e collegarsi al controller meno utilizzato dai loro elenchi, a condizione che sia disponibile la connettività IP.

Nota: anche l'opzione DHCP 43 e la ricerca DNS (Domain Name System) funzionano con i REAP. Per informazioni su come configurare DHCP o DNS sui siti remoti in modo da consentire ai punti di accesso di trovare i controller centrali, consultare il documento sulla distribuzione dei Cisco Wireless LAN Controller serie 440X.

A questo punto, è possibile assegnare al modello 1030 indirizzi statici, se lo si desidera. In questo modo si garantisce che lo schema di indirizzamento IP corrisponda al sito remoto di destinazione. Inoltre, è possibile immettere i nomi dei WLC per indicare dettagliatamente i tre controller che ciascun LAP tenterà di connettere. Se questi tre errori si verificano, la funzionalità di bilanciamento automatico del carico di LWAPP consente al LAP di scegliere il punto di accesso meno caricato dall'elenco dei controller rimanenti nel cluster. La modifica della configurazione LAP può essere effettuata tramite l'interfaccia della riga di comando (CLI) o l'interfaccia grafica utente del WLC, o con maggiore facilità, tramite il WCS.

Nota: i 1030 REAP richiedono che i WLC a cui si connettono funzionino in modalità LWAPP di layer 3. È quindi necessario assegnare ai controller indirizzi IP. Inoltre, i WLC richiedono la disponibilità di un server DHCP in ogni sito remoto, oppure l'assegnazione di indirizzi statici durante il processo di priming. La funzionalità DHCP integrata nei controller non può essere utilizzata per fornire indirizzi ai LAP 1030 o ai loro utenti.

Prima di spegnere i 1030 LAP da inviare ai siti remoti, verificare che ogni 1030 sia impostato sulla modalità REAP. Questa operazione è molto importante perché per impostazione predefinita, in tutti i LAP vengono eseguite funzionalità locali regolari. Per eseguire la funzionalità REAP, è necessario impostare il valore 1030. Questa operazione può essere eseguita a livello di LAP dalla CLI o dalla GUI del controller o con maggiore facilità tramite i modelli WCS.

Funzioni base di preparazione REAP

Dopo la connessione di 1030 REAP a un WLC all'interno del gruppo di mobilità a cui si connettono i REAP quando vengono collocati in siti remoti, è possibile fornire le seguenti informazioni:

Impostazioni REAP necessarie

- Un elenco di indirizzi IP per il WLC nel gruppo di mobilità (fornito automaticamente al momento della connessione al controller o all'access point)
- Per eseguire la funzionalità REAP, è necessario configurare i punti di accesso in modalità REAP

Impostazioni REAP opzionali

- Indirizzi IP assegnati in modo statico (un'impostazione opzionale immessa su base per punto di accesso)
- Nomi WLC primari, secondari e terziari (impostazione facoltativa immessa per punto o tramite

modelli WCS)
- Nome punto di accesso (un'impostazione informativa facoltativa per ogni punto di accesso)
- Informazioni sulla posizione dei punti di accesso (impostazione informativa facoltativa immessa per punto di accesso o tramite modelli WCS)

Requisiti di collegamento tra REAP e controller

Quando si prevede di distribuire i REAP, è necessario ricordare alcuni requisiti di base. Questi requisiti riguardano la velocità e la latenza dei collegamenti WAN attraversati dal traffico di controllo REAP LWAPP. Il 1030 LAP è progettato per essere usato su collegamenti WAN, come tunnel di sicurezza IP, Frame Relay, DSL (non PPPoE) e linee affittate.

Nota: l'implementazione di 1030 REAP LWAPP presuppone un percorso MTU di 1500 byte tra l'AP e il WLC. Ogni frammentazione che avviene in transito a causa di una MTU inferiore a 1500 byte porta a risultati imprevedibili. Pertanto, il 1030 LAP non è adatto ad ambienti, come il PPPoE, in cui i router frammentano proattivamente i pacchetti fino a meno di 1500 byte.

La latenza del collegamento WAN è particolarmente importante perché ogni 1030 LAP invia ai controller, per impostazione predefinita, messaggi heartbeat ogni 30 secondi. Dopo la perdita dei messaggi di heartbeat, i LAP inviano 5 heartbeat consecutivi, una volta al secondo. Se nessuna delle operazioni ha esito positivo, il LAP determina che la connettività del controller viene interrotta e il router 1030s torna alla modalità REAP standalone. Mentre il 1030 LAP può tollerare ampie latenze tra se stesso e il WLC, è necessario garantire che la latenza tra il LAP e il controller non superi i 100 ms. Ciò è dovuto ai timer lato client che limitano il tempo di attesa dei client prima che i timer determinino un errore di autenticazione.

Limitazioni REAP

Sebbene il 1030 AP sia progettato per essere gestito centralmente e per fornire il servizio WLAN durante le interruzioni del collegamento WAN, esistono alcune differenze tra i servizi offerti dal REAP con la connettività WLC e quelli che può fornire quando la connettività viene interrotta.

WLAN

Mentre 1030 REAP può supportare fino a 16 WLAN (profili wireless che contengono un SSID [Service Set Identifier] ciascuno, insieme a tutte le policy di sicurezza, QoS e di altro tipo), ognuna con un proprio MBSSID (Multiple Basic Service Set ID), 1030 REAP può supportare la prima WLAN solo quando la connettività con un controller viene interrotta. Durante i periodi di interruzione del collegamento WAN, tutte le WLAN ad eccezione della prima vengono rimosse. Pertanto, la WLAN 1 deve essere considerata come la principale WLAN e le policy di sicurezza devono essere pianificate di conseguenza. La sicurezza di questa prima WLAN è particolarmente importante perché, in caso di errore del collegamento WAN, si verifica anche l'autenticazione RADIUS back-end. Questo perché il traffico attraversa il piano di controllo LWAPP. L'accesso wireless non viene pertanto concesso ad alcun utente.

Su questa prima WLAN si consiglia di utilizzare un metodo di autenticazione/crittografia locale, ad esempio la parte di chiave già condivisa di WPA-PSK (Wi-Fi Protected Access). WEP (Wired Equivalent Privacy) è sufficiente, ma non è consigliato a causa di vulnerabilità note della sicurezza.Quando si utilizza WPA-PSK (o WEP), gli utenti configurati correttamente possono comunque accedere alle risorse di rete locali anche se il collegamento WAN non è attivo.

Nota: tutti i metodi di sicurezza basati su RADIUS richiedono la trasmissione di messaggi di autenticazione attraverso il control plane LWAPP al sito centrale. Pertanto, tutti i servizi basati su RADIUS non sono disponibili durante le interruzioni della WAN. Sono incluse, senza limitazioni, le autenticazioni MAC basate su RADIUS, 802.1X, WPA, WPA2 e 802.11i.

Il protocollo 1030 REAP può risiedere solo su una singola subnet perché non può eseguire il tagging VLAN 802.1q. Pertanto, il traffico su ciascun SSID termina sulla stessa subnet nella rete cablata. Ciò significa che, mentre il traffico wireless potrebbe essere segmentato via etere tra gli SSID, il traffico utente non è separato sul lato cablato.

Sicurezza

1030 REAP può fornire tutti i criteri di sicurezza di layer 2 supportati dall'architettura WAN basata su controller di Cisco. Sono inclusi tutti i tipi di autenticazione e crittografia di livello 2, ad esempio WEP, 802.1X, WPA, WPA2 e 802.11i. Come accennato in precedenza, la maggior parte di questi criteri di sicurezza richiede la connettività WLC per l'autenticazione back-end. WEP e WPA-PSK sono completamente implementati a livello AP e non richiedono l'autenticazione RADIUS back-end. Pertanto, anche se il collegamento WAN non è attivo, gli utenti possono comunque connettersi. La funzione di elenco di esclusione dei client fornita nel Cisco WLC è supportata con il 1030 LAP. Il filtro MAC funziona sul 1030 se è disponibile la connettività al controller.

Nota: il protocollo REAP non supporta WPA2-PSK quando l'access point è in modalità standalone.

Tutti i criteri di sicurezza di layer 3 non sono disponibili con il 1030 LAP. Questi criteri di sicurezza includono l'autenticazione Web, la terminazione VPN basata su controller, gli ACL e il blocco peer-to-peer, in quanto implementati nel controller. Il pass-through VPN non funziona per i client che si connettono a concentratori VPN esterni. Tuttavia, non è possibile usare la funzionalità del controller che consente solo il traffico destinato a un concentratore VPN specificato (solo pass-through VPN).

NAT (Network Address Translation)

I WLC a cui i REAP si connettono non possono risiedere dietro i limiti NAT. Tuttavia, i REAP presso i siti remoti possono rimanere dietro una scatola NAT, a condizione che le porte utilizzate per LWAPP (porte UDP 1222 e 1223) siano inoltrate agli access point serie 1030. Ciò significa che ogni REAP deve avere un indirizzo statico per consentire l'inoltro delle porte in modo affidabile e che solo un singolo AP può risiedere dietro ogni istanza NAT. Ciò si verifica perché può esistere una sola istanza di inoltro porta per ogni indirizzo IP NAT, il che significa che solo un LAP può funzionare dietro ogni servizio NAT nei siti remoti. Il protocollo NAT uno-a-uno può funzionare con più REAP perché le porte LWAPP possono essere inoltrate per ciascun indirizzo IP esterno a ciascun indirizzo IP interno (indirizzo IP statico REAP).

QoS (Quality of Service)

La definizione di priorità dei pacchetti basata sui bit di precedenza 802.1p non è disponibile perché il REAP non è in grado di eseguire il tagging 802.1q. Ciò significa che Wi-Fi Multimedia (WMM) e 802.11e non sono supportati. Sono supportate la definizione di priorità dei pacchetti basata su SSID e Identity Base Networking. Tuttavia, l'assegnazione della VLAN tramite Identity-Based Networking non funziona con il REAP perché non può eseguire il tagging 802.1q.

Roaming e bilanciamento del carico dei client

Negli ambienti in cui sono presenti più punti REAP e in cui è prevista la mobilità tra punti di accesso, ogni punto di accesso deve trovarsi sulla stessa subnet. La mobilità di layer 3 non è supportata nel 1030 LAP. In genere, non si tratta di una limitazione, in quanto gli uffici remoti di solito non impiegano un numero sufficiente di LAP per richiedere tale flessibilità.

Il bilanciamento del carico client aggressivo viene fornito tra tutti i REAP nei siti con più di un singolo AP quando è disponibile la connettività del controller upstream (solo il bilanciamento del carico è abilitato sul controller host).

Gestione risorse radio (RRM)

In presenza di connettività ai controller, i 1030 LAP ricevono un canale dinamico e un'uscita di alimentazione dal meccanismo RRM nei WLC. Quando il collegamento WAN è inattivo, RRM non funziona e le impostazioni dei canali e dell'alimentazione non vengono modificate.

Rilevamento di anomalie e funzionalità IDS

L'architettura REAP supporta tutti i rogue detection e intrusion detection signature (IDS) che corrispondono a quelli dei LAP standard. Tuttavia, quando si perde la connettività con un controller centrale, tutte le informazioni raccolte non vengono condivise. Di conseguenza, la visibilità nei domini RF dei siti remoti viene persa.

Riepilogo limitazioni REAP

La tabella dell'Appendice B riepiloga le funzionalità del REAP durante il normale funzionamento e quando la connessione al WLC sul collegamento WAN non è disponibile.

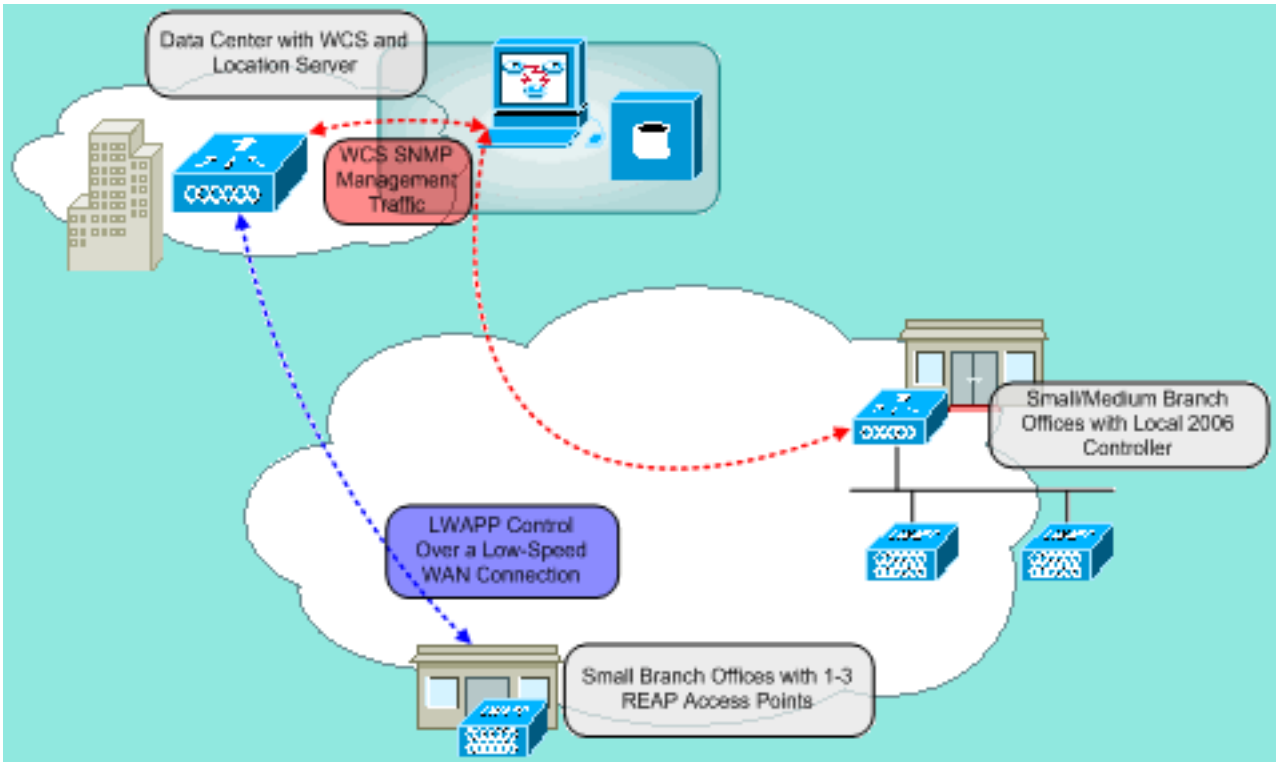
Gestione dell'architettura REAP e WLAN centrale

La gestione del 1030 REAP è uguale a quella dei LAP e WLC standard. La gestione e la configurazione vengono eseguite a livello di controller, tramite la CLI di ciascun controller o l'interfaccia GUI Web. La configurazione e la visibilità della rete a livello di sistema vengono fornite attraverso il sistema WCS, dove tutti i controller e i punti di accesso (REAP o altri) possono essere gestiti come un unico sistema. Quando la connettività del controller REAP viene interrotta, vengono interrotte anche le funzionalità di gestione.

Architettura WLAN centralizzata con REAP

Nella Figura 2 viene mostrato come ogni parte dell'architettura LWAPP centralizzata interagisce per soddisfare una varietà di esigenze di rete wireless. I servizi di gestione e localizzazione vengono forniti a livello centrale tramite WCS e Location Appliance 2700.

Figura 2: Architettura WLAN centralizzata con REAP



Appendice A

Quali sono le principali differenze tra l'architettura REAP e i LAP standard?

- Se l'opzione DHCP 43 o la risoluzione DNS non è disponibile nei siti remoti, è necessario innescare il 1030 nell'ufficio centrale. Quindi, viene spedito al sito di destinazione.
- In caso di errore del collegamento WAN, rimane attiva solo la prima WLAN.I criteri di protezione che richiedono RADIUS avranno esito negativo.L'autenticazione/crittografia che utilizza WPA-PSK è consigliata per la WLAN 1. WEP funziona, ma non è consigliata.
- Nessuna crittografia di livello 3 (solo crittografia di livello 2)
- I WLC a cui i REAP si connettono non possono risiedere dietro i limiti NAT. Tuttavia, i REAP possono, a condizione che ogni indirizzo IP statico interno dei REAP abbia entrambe le porte LWAPP (1222 e 1223) inoltrate.**Nota: il protocollo** PAT (Port Address Translation) / NAT con overload non è supportato perché la porta di origine del traffico LWAPP proveniente dal LAP può cambiare nel tempo. Questo interrompe l'associazione LWAPP. Lo stesso problema può verificarsi con le implementazioni NAT per REAP in cui l'indirizzo della porta cambia, ad esempio PIX/ASA, a seconda della configurazione.
- Solo i messaggi di controllo LWAPP attraversano il collegamento WAN.
- Il traffico di dati è bloccato sulla porta Ethernet del router 1030.
- Il LAP 1030 non esegue il tagging 802.1Q (VLAN). Pertanto, il traffico wireless da tutti gli SSID termina sulla stessa subnet cablata.

Appendice B

Quali sono le differenze di funzionalità tra le modalità REAP normale e standalone?

	REAP (modalità normale)	REAP (modalità standalone)

Protocolli	IPv4	Sì	Sì
	IPv6	Sì	Sì
	Tutti gli altri protocolli	Sì (solo se il client è abilitato anche per IP)	Sì (solo se il client è abilitato anche per IP)
	ARP proxy IP	No	No
WLAN	Number of SSIDs	16	1 (il primo)
	Assegnazione dinamica dei canali	Sì	No
	Controllo dinamico dell'alimentazione	Sì	No
	Bilanciamento dinamico del carico	Sì	No
VLAN	Interfacce multiple	No	No
	Supporto 802.1Q	No	No
Sicurezza WLAN	Rilevamento punti di accesso non autorizzati	Sì	No
	Elenco di esclusione	Sì	Sì (solo membri esistenti)
	Blocco peer-to-peer	No	No
	Sistema di	Sì	No

	rilevamento intrusioni		
Sicurezza di livello 2	Autenticazione MAC	Sì	No
	802.1X	Sì	No
	WEP (64/128/152 bit)	Sì	Sì
	WPA-PSK	Sì	Sì
	WPA2-PSK	Sì	No
	WPA-EAP	Sì	No
	WPA2-EAP	Sì	No
Sicurezza di livello 3	Autenticazione Web	No	No
	IPSec	No	No
	L2TP	No	No
	Pass-through VPN	No	No
	Access Control Lists	No	No
QoS	Profili QoS	Sì	Sì
	QoS downlink (code round robin ponderate)	Sì	Sì
	supporto 802.1p	No	No
	Contratti sulla larghezza di banda per utente	No	No

	WMM	No	No
	802.11e (in futuro)	No	No
	Override del profilo QoS AAA	Sì	No
Mobilità	All'interno della subnet	Sì	Sì
	Inter-subnet	No	No
DHCP	Server DHCP interno	No	No
	Server DHCP esterno	Sì	Sì
Topologia	Connessione diretta (2006)	No	No

Informazioni correlate

- Esempio di configurazione di Remote-Edge AP (REAP) con Lightweight AP e Wireless LAN Controller (WLC)
- Bilanciamento del carico e fallback dell'access point nelle reti wireless unificate
- Implementazione dei Cisco Wireless LAN Controller serie 440X
- Esempio di configurazione base di Wireless LAN Controller e Lightweight Access Point
- Documentazione e supporto tecnico – Cisco Systems