Domande frequenti sull'accesso guest wireless

Sommario

Introduzione

Questo documento descrive le informazioni per le domande più frequenti (FAQ) sulla funzione Wireless Guest Access, che fa parte della rete Cisco Unified Wireless.

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

Che cos'è un tunnel Ethernet over IP (EoIP) per l'area di rete non protetta?

Cisco consiglia di utilizzare un controller dedicato al traffico guest. Questo controller è noto come controller di ancoraggio guest.

Il controller di ancoraggio guest si trova generalmente in un'area di rete non protetta, spesso denominata zona demilitarizzata (DMZ). Altri controller WLAN interni da cui ha origine il traffico si trovano nella LAN aziendale. Viene stabilito un tunnel EoIP tra i controller WLAN interni e il controller di ancoraggio guest per garantire l'isolamento del percorso del traffico guest dal traffico dati aziendale. L'isolamento dei percorsi è una funzione di gestione della sicurezza di importanza critica per l'accesso guest. Garantisce che le policy di sicurezza e qualità del servizio (QoS) possano essere separate e differenziate tra il traffico guest e il traffico interno o aziendale.

Una funzionalità importante dell'architettura di rete wireless unificata Cisco è la capacità di utilizzare un tunnel EoIP per mappare staticamente una o più WLAN con provisioning (ossia SSID) su uno specifico controller di ancoraggio guest nella rete. Tutto il traffico, sia in entrata che in uscita da una WLAN mappata, attraversa un tunnel EoIP statico stabilito tra un controller remoto e il controller di ancoraggio guest.

Utilizzando questa tecnica, tutto il traffico guest associato può essere trasportato in modo trasparente attraverso la rete aziendale a un controller di ancoraggio guest che risiede nell'area di rete non protetta.

Come è possibile selezionare il controller corretto da distribuire come controller di ancoraggio guest?

La selezione del controller di ancoraggio guest è una funzione della quantità di traffico guest definita dal numero di sessioni client guest attive o dalla capacità dell'interfaccia uplink sul controller o da entrambi.

Di seguito sono riportati i limiti totali di throughput e client per controller di ancoraggio guest:

- Cisco Wireless LAN Controller 2504 - 4 * interfacce da 1 Gbps e 1000 client guest

- Cisco 5508 Wireless LAN Controller (WLC) - client guest a 8 Gb/s e 7.000
- Cisco Catalyst serie 6500 Wireless Services Module (WiSM-2) - 20 Gbps e 15.000 client
- Cisco 8500 Wireless LAN Controller (WLC) - 10 Gbps e 64.000 client

---

Nota: non è possibile configurare i WLC di Cisco 7500 come controller di ancoraggio guest. Per un elenco dei WLC che supportano la funzione di ancoraggio guest, fare riferimento a Quali controller possono essere utilizzati per supportare l'accesso guest nell'area di rete non protetta?.

Nel database di ogni controller è possibile memorizzare un massimo di 2048 nomi utente e password guest. Pertanto, se il numero totale di credenziali guest attive è superiore a questo numero, è necessario più di un controller. In alternativa, è possibile archiviare le credenziali guest in un server RADIUS esterno.

Il numero di punti di accesso nella rete non influisce sulla selezione del controller di ancoraggio guest.

Quanti tunnel Ethernet over IP (EoIP) possono essere terminati su un controller di ancoraggio guest?

Un controller di ancoraggio guest può terminare fino a 71 tunnel EoIP dai controller WLAN interni. Questa capacità è la stessa su tutti i modelli di Cisco Wireless LAN Controller ad eccezione di WLC- 2504. Il controller 2504 può terminare fino a 15 tunnel EoIP. Se sono necessari tunnel aggiuntivi, è possibile configurare più controller di ancoraggio guest.

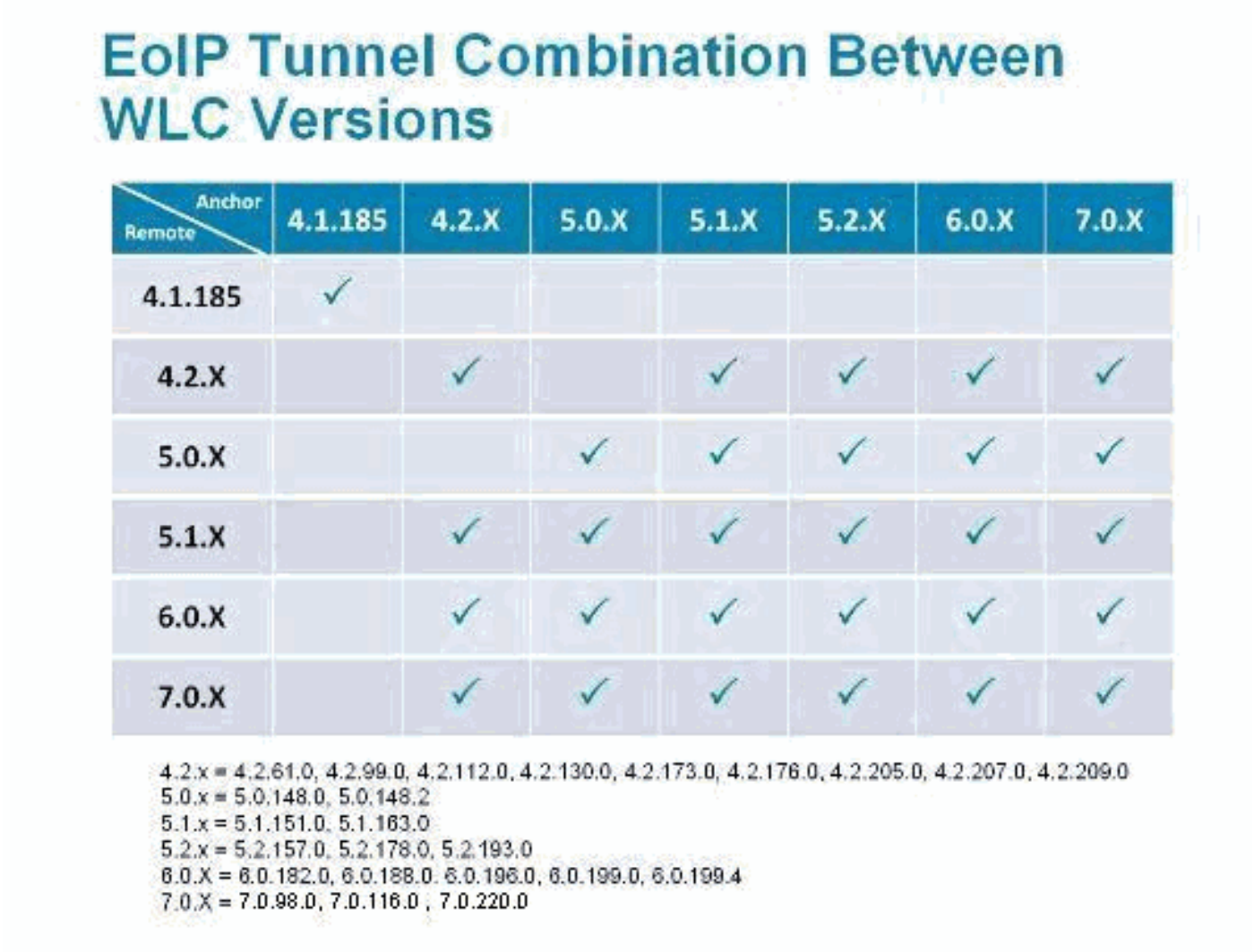
I tunnel EoIP vengono conteggiati per controller WLAN, indipendentemente dal numero di WLAN tunneling o di SSID (Secure Set Identifier) in ciascun EoIP.

Tra il controller di ancoraggio guest e ogni controller interno che supporta punti di accesso con associazioni client guest è configurato un tunnel EoIP.

È possibile creare tunnel Ethernet over IP (EoIP) tra controller che eseguono versioni software diverse?

Non tutte le versioni del software Wireless LAN Controller supportano questa funzionalità. In questi casi, il telecomando e il controller di ancoraggio devono eseguire la stessa versione del software WLC. Tuttavia, le versioni software più recenti consentono ai controller remoti e di ancoraggio di avere versioni diverse.

In questa matrice vengono elencate le versioni del software Wireless LAN Controller con cui è possibile creare i tunnel EoIP.



È possibile utilizzare Cisco serie 2100/2500 Wireless LAN Controller come controller di ancoraggio guest nell'area di rete non protetta?

Sì, a partire dal software Cisco Unified Wireless Network versione 7.4, il controller LAN wireless Cisco serie 2500 può terminare (fino a 15 tunnel EoIP) il traffico guest all'esterno del firewall. Il Cisco serie 2000 Wireless LAN Controller può originare solo tunnel guest.

È possibile utilizzare il Cisco Wireless LAN Controller Module per Integrated Services Router (WLCM o WLCM2) come controller di ancoraggio guest nell'area di rete non protetta?

No, WLCM o WLCM2 non possono terminare i tunnel guest. WLCM può originare solo tunnel guest.

Quali controller possono essere utilizzati per supportare l'accesso

guest nell'area di rete non protetta?

La funzione di ancoraggio del tunnel guest, che include la terminazione del tunnel EoIP, l'autenticazione Web e il controllo dell'accesso dei client guest, è supportata nelle seguenti piattaforme Cisco Wireless LAN Controller con immagini software versione 4.0 o successive:

- Cisco Catalyst serie 6500 Wireless Services Module (WiSM2)
- Cisco serie WiSM-2 Wireless LAN Controller
- Controller LAN wireless integrato Cisco Catalyst 3750G
- Cisco serie 5508 Wireless LAN Controller
- Cisco serie 2500 Wireless LAN Controller (supporto introdotto nel software versione 7.4)

Se un controller di ancoraggio guest viene utilizzato al di fuori del firewall, quali porte del firewall sono aperte per l'accesso guest al lavoro?

Su qualsiasi firewall tra il controller di ancoraggio guest e i controller remoti, queste porte devono essere aperte:

- Mobilità legacy: protocollo IP 97 per il traffico di dati degli utenti, porta UDP 1666
- Nuova mobilità: porte UDP 1666 e 1667

Per la gestione opzionale, è necessario che le porte del firewall siano aperte:

- SSH/Telnet - Porta TCP 22/23
- TFTP - Porta UDP 69
- NTP - Porta UDP 123
- SNMP - Porte UDP 161 (get e set) e 162 (trap)
- HTTPS/HTTP - porta TCP 443/80
- Syslog - Porta TCP 514
- Porta UDP 1812 e 1813 autenticazione/account RADIUS

Il traffico guest può passare attraverso un firewall con la configurazione NAT (Network Address Translation)?

È necessario utilizzare un NAT uno a uno sul tunnel EoIP che attraversa un firewall.

In uno scenario Anchor - Foreign WLC, quale WLC invia l'accounting RADIUS?

In questo scenario, l'autenticazione viene sempre eseguita dal WLC di ancoraggio. Pertanto, l'accounting RADIUS viene inviato dal WLC di ancoraggio.

Nota: in una distribuzione CWA (Central Web Authentication) e/o CoA (Change of Authorization), l'accounting RADIUS deve essere DISABILITATO sull'ancoraggio e utilizzato solo sul WLC esterno.

Il tunnel guest tra il controller interno e il controller di ancoraggio non funziona. Questi log vengono visualizzati nel WLC:

mm_Listen.c:5373 MM-3-INVALID_PKT_RECVD: ricevuto un pacchetto non valido da 10. 40.220.18. Membro di origine:0.0.0. membro di origine sconosciuto.. Perché?

È possibile controllare lo stato del tunnel dalla GUI del WLC nella pagina WLAN. Fare clic sulla casella a discesa accanto a una WLAN e scegliere Mobility Anchors (Ancoraggi mobilità) che contiene lo stato del controllo e il percorso dati. Il messaggio di errore viene visualizzato per uno dei motivi seguenti:

1. I controller di ancoraggio e interni si trovano in versioni diverse del codice. Assicurarsi che eseguano le stesse versioni del codice.
2. Configurazioni errate nella configurazione dell'ancora per la mobilità. Verificare che la DMZ sia configurata come ancoraggio di mobilità e che i WLC interni abbiano la DMZ WLC configurata come ancoraggio di mobilità. Per ulteriori informazioni su come configurare l'ancoraggio di mobilità, consultare la sezione Configurazione dell'ancoraggio automatico della guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0. In questo modo gli utenti guest non sarebbero in grado di passare il traffico.

In una configurazione di accesso guest wireless, i client non ricevono l'indirizzo IP dal server DHCP. Sul controller interno viene visualizzato il messaggio di errore Thu Jan 22 16:39:09 2009: XX:XX:XX:XX:XX DHCP dropping REPLY from Export-Foreign STA. Perché?

In una configurazione di accesso guest wireless, l'impostazione del proxy DHCP nei controller di ancoraggio guest e nel controller interno devono corrispondere. In caso contrario, le richieste DHCP dei client vengono eliminate e sul controller interno viene visualizzato questo messaggio di errore:

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

Utilizzare questo comando per modificare l'impostazione del proxy dhcp sul WLC:

<#root>

```
(Cisco Controller) >
```

config dhcp proxy ?

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

Utilizzare il comando show dhcp proxy su entrambi i controller per verificare che entrambi abbiano la stessa impostazione del proxy DHCP.

<#root>

```
(Cisco Controller) >
```

show dhcp proxy

```
DHCP Proxy Behaviour: enabled

(Cisco Controller) >
```

Se il traffico guest è indirizzato all'area di rete non protetta, dove i client guest ottengono un indirizzo IP?

Il traffico guest viene trasportato all'interno dell'azienda al layer 3 tramite EoIP. Pertanto, il primo punto in cui è possibile implementare i servizi DHCP (Dynamic Host Configuration Protocol) è localmente nel controller di ancoraggio guest oppure il controller di ancoraggio guest può inoltrare le richieste DHCP client a un server esterno. Questo metodo consente inoltre di gestire la risoluzione degli indirizzi DNS (Domain Name System).

Cisco Wireless LAN Controller supporta i portali Web per l'autenticazione guest?

I Cisco Wireless LAN Controller, software versione 3.2 o successive, offrono un portale Web incorporato che acquisisce le credenziali degli utenti per l'autenticazione e offre semplici funzionalità di branding, oltre alla possibilità di visualizzare informazioni su declinazioni di

responsabilità e policy per un utilizzo accettabile.

Personalizzazione del portale Web

Per informazioni sulla personalizzazione di un portale Web, vedere Scelta della pagina di accesso per l'autenticazione Web.

Come vengono gestite le credenziali guest?

Le credenziali dei guest possono essere create e gestite a livello centrale utilizzando Cisco Wireless Control System (WCS) versione 7.0 o Network Control System (NCS) versione 1.0. Un amministratore di rete può stabilire un account amministrativo con privilegi limitati all'interno di WCS che consente l'accesso a "lobby ambassador" allo scopo di creare credenziali guest. In WCS o NCS, la persona con un account lobby ambassador è in grado di creare, assegnare, monitorare ed eliminare le credenziali guest per il controller che funge da controller di ancoraggio guest.

L'ambasciatore della sala di attesa può immettere il nome utente guest (o l'ID utente) e la password oppure è possibile generare automaticamente le credenziali. È inoltre disponibile un parametro di configurazione globale che consente di utilizzare un nome utente e una password per tutti gli utenti guest oppure un nome utente e una password univoci per ogni utente guest.

Per configurare l'account lobby ambassador sul sistema WCS, fare riferimento alla sezione Creating Guest User Accounts della guida alla configurazione di Cisco Wireless Control System, versione 7.0.

La funzione lobby ambassador è disponibile nel controller LAN wireless Cisco in aggiunta al Wireless Control System (WCS) o NCS?

Sì. Se WCS o NCS non è distribuito, un amministratore di rete può stabilire un account lobby ambassador sul controller di ancoraggio guest. Una persona che accede al controller di ancoraggio guest utilizzando l'account di ambasciatore della sala di attesa ha accesso solo alle funzioni di gestione degli utenti guest.

Se sono presenti più controller di ancoraggio guest, è necessario utilizzare un controller WCS o NCS per configurare contemporaneamente i nomi utente su più controller di ancoraggio guest.

Per informazioni su come creare account di ambasciatori della sala di attesa utilizzando i Wireless LAN Controller, fare riferimento alla sezione Creazione di un account di ambasciatori della guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0.

È possibile autenticare i guest con un server di autenticazione, autorizzazione e accounting (AAA) esterno?

Sì. Le richieste di autenticazione guest possono essere inoltrate a un server RADIUS esterno.

Cosa succede quando un guest esegue l'accesso?

Quando un guest wireless accede tramite il portale Web, il controller di ancoraggio guest gestisce l'autenticazione eseguendo la procedura seguente:

1. Il controller di ancoraggio guest verifica il nome utente e la password nel database locale e, se presenti, concede l'accesso.
2. Se sul controller di ancoraggio guest non sono presenti credenziali utente in locale, il controller di ancoraggio guest controlla le impostazioni di configurazione della WLAN per verificare se sono stati configurati server RADIUS esterni per la WLAN guest. In questo caso, il controller crea un pacchetto di richiesta di accesso RADIUS con nome utente e password e lo inoltra al server RADIUS selezionato per l'autenticazione.
3. Se per la WLAN non sono stati configurati server RADIUS specifici, il controller controlla le impostazioni di configurazione globali del server RADIUS. Tutti i server RADIUS esterni configurati con l'opzione per l'autenticazione dell'utente di rete vengono richiesti con le credenziali dell'utente guest. In caso contrario, se per nessun server è stato selezionato "utente di rete" e l'utente non è stato autenticato tramite i passaggi 1 o 2, l'autenticazione non riesce.

È possibile ignorare l'autenticazione dell'utente guest e visualizzare solo l'opzione di esclusione di responsabilità della pagina Web?

Sì. Un'altra opzione di configurazione dell'accesso guest wireless consiste nell'ignorare completamente l'autenticazione utente e consentire l'accesso aperto. Tuttavia, potrebbe essere necessario presentare agli ospiti una politica sull'utilizzo accettabile e una pagina di esclusione di responsabilità prima di concedere l'accesso. A tale scopo, è possibile configurare una WLAN guest per la trasmissione dei criteri Web. In questo scenario, un utente guest viene reindirizzato a una pagina del portale Web contenente informazioni sulla dichiarazione di non responsabilità. Per consentire l'identificazione dell'utente guest, la modalità passthrough dispone anche di un'opzione per l'immissione di un indirizzo e-mail prima della connessione.

È necessario che il controller remoto e il controller di ancoraggio guest si trovino sullo stesso gruppo di mobilità?

No. Il controller di ancoraggio guest e il telecomando possono trovarsi in gruppi di mobilità separati.

Se sono presenti più SSID guest, è possibile indirizzare ciascuna

WLAN (SSID) a un portale di pagine Web univoco?

Sì. Tutto il traffico guest, su una o più WLAN, viene reindirizzato a una pagina Web. A partire dalla versione 4.2 o successive del WLC, ciascuna WLAN può essere indirizzata a una pagina univoca del portale Web. Fare riferimento alla sezione Assegnazione di login, errori di login e disconnessione per WLAN della guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0.

Quali sono le funzionalità della nuova impostazione in WLC release 7.0, WebAuth on Mac Filter Failure?

Se per una WLAN sono configurate sia la sicurezza di layer 2 (mac-filter) sia la sicurezza di layer 3 (webauth-on-macfilter-failure), il client passa allo stato RUN se viene passato uno dei due. E se si verifica un errore di protezione di livello 2 (mac-filter), il client viene spostato nella protezione di livello 3 (webauth-on-macfilter-failure).

Il client funziona correttamente se il browser è configurato per il server proxy?

Nelle versioni precedenti alla 7.0, il client non era in grado di stabilire una connessione TCP quando il server proxy era configurato nel browser. Dopo la versione 7.0, viene aggiunto il supporto del server proxy WebAuth e l'indirizzo IP e la porta del server proxy possono essere configurati sul controller.

È disponibile una guida alla distribuzione di Wireless Guest Access?

Questo è il collegamento alla guida alla distribuzione:

Guida all'installazione: Cisco Guest Access con Cisco Wireless LAN Controller

È disponibile una guida alla progettazione per l'accesso guest wireless e cablato?

Di seguito sono riportati i collegamenti alle guide alla progettazione:

- Servizi Cisco Unified Wireless Guest Access
- Esempio di configurazione di WLAN Controller in Wired

Informazioni correlate

- Esempio di configurazione di WLAN Controller in Wired

- Guida all'installazione: Cisco Guest Access Using the Cisco Wireless LAN Controller, release 4.1
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).