

Esempio di configurazione delle funzioni di sicurezza di layer 2 sugli switch Cisco Catalyst a configurazione fissa di layer 3

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Prodotti correlati](#)

[Convenzioni](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Sicurezza porta](#)

[Snooping DHCP](#)

[Ispezione ARP dinamica](#)

[Protezione origine IP](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene fornito un esempio di configurazione di alcune funzioni di sicurezza del layer 2, quali la sicurezza delle porte, lo snooping DHCP, l'ispezione ARP (Dynamic Address Resolution Protocol) e la protezione dell'origine IP, che possono essere implementate sugli switch Cisco Catalyst Layer 3 a configurazione fissa.

[Prerequisiti](#)

[Requisiti](#)

Nessun requisito specifico previsto per questo documento.

[Componenti usati](#)

Per la stesura del documento, sono stati usati switch Cisco Catalyst serie 3750 con versione 12.2(25)SEC2.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con i seguenti hardware:

- Switch Cisco Catalyst serie 3550
- Switch Cisco Catalyst serie 3560
- Cisco Catalyst serie 3560-E Switch
- Cisco Catalyst serie 3750-E Switch

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Premesse

Analogamente ai router, gli switch di layer 2 e layer 3 hanno entrambi i propri set di requisiti di sicurezza di rete. Gli switch sono soggetti a molti degli stessi attacchi dei router di layer 3. Tuttavia, gli switch e il livello 2 del modello di riferimento OSI in generale sono soggetti agli attacchi alla rete in modi diversi. Tra queste:

- **Overflow della tabella CAM (Content Addressable Memory)**Le tabelle CAM (Content Addressable Memory) hanno dimensioni limitate. Se nella tabella CAM vengono inserite un numero sufficiente di voci prima che le altre voci siano scadute, la tabella CAM riempie fino al punto che non è possibile accettare nuove voci. In genere, un intruso alla rete inonda lo switch con un numero elevato di indirizzi MAC (Media Access Control) di origine non validi fino a quando la tabella CAM non si completa. In questo caso, lo switch scarica tutte le porte con il traffico in entrata perché non riesce a trovare il numero di porta per un particolare indirizzo MAC nella tabella CAM. In sostanza, lo switch funziona come un hub. Se l'intruso non mantiene il flusso di indirizzi MAC di origine non valida, lo switch alla fine esclude le voci degli indirizzi MAC precedenti dalla tabella CAM e ricomincia a funzionare come uno switch. L'overflow della tabella CAM provoca solo un flooding del traffico all'interno della VLAN locale, quindi l'intruso vede il traffico solo all'interno della VLAN locale a cui è connesso. L'attacco di overflow della tabella CAM può essere mitigato configurando la sicurezza delle porte sullo switch. Questa opzione consente di specificare gli indirizzi MAC su una particolare porta dello switch o il numero di indirizzi MAC che possono essere appresi da una porta dello switch. Quando viene rilevato un indirizzo MAC non valido sulla porta, lo switch può bloccare l'indirizzo MAC in conflitto o arrestare la porta. La specifica degli indirizzi MAC sulle porte dello switch è una soluzione troppo ingestibile per un ambiente di produzione. È possibile gestire un limite al numero di indirizzi MAC su una porta dello switch. Una soluzione più scalabile a livello amministrativo è l'implementazione della sicurezza dinamica delle porte sullo switch. Per implementare la sicurezza dinamica delle porte, specificare un numero massimo di indirizzi MAC da apprendere.

- **Spoofing degli indirizzi MAC (Media Access Control)** Gli attacchi di spoofing MAC (Media Access Control) implicano l'uso di un indirizzo MAC noto di un altro host per tentare di far avanzare i frame del commutatore di destinazione destinati all'host remoto all'autore dell'attacco di rete. Quando un singolo frame viene inviato con l'indirizzo Ethernet di origine dell'altro host, l'utente malintenzionato sovrascrive la voce della tabella CAM in modo che lo switch inoltri i pacchetti destinati all'host all'utente malintenzionato. Finché l'host non invia traffico, non riceve alcun traffico. Quando l'host invia il traffico, la voce della tabella CAM viene riscritta nuovamente in modo da tornare alla porta originale. Utilizzare la funzione di sicurezza delle porte per mitigare gli attacchi di spoofing degli indirizzi MAC. La funzione di sicurezza delle porte consente di specificare l'indirizzo MAC del sistema connesso a una determinata porta. Consente inoltre di specificare l'azione da eseguire in caso di violazione della sicurezza della porta.
- **Spoofing Address Resolution Protocol (ARP)** Il protocollo ARP viene utilizzato per mappare gli indirizzi IP agli indirizzi MAC in un segmento della rete locale in cui risiedono gli host della stessa subnet. Normalmente, un host invia una richiesta ARP di trasmissione per trovare l'indirizzo MAC di un altro host con un particolare indirizzo IP e una risposta ARP viene dall'host il cui indirizzo corrisponde alla richiesta. L'host richiedente memorizza quindi nella cache la risposta ARP. All'interno del protocollo ARP, un'altra disposizione prevede che gli host eseguano risposte ARP non richieste. Le risposte ARP non richieste sono chiamate Gratuitous ARP (GARP). La tecnologia GARP può essere sfruttata in modo dannoso da un utente malintenzionato per falsificare l'identità di un indirizzo IP su un segmento LAN. Questa funzione viene in genere utilizzata per falsificare l'identità tra due host o tutto il traffico da e verso un gateway predefinito in un attacco "man-in-the-middle". Quando si crea una risposta ARP, un utente malintenzionato può far apparire il proprio sistema come l'host di destinazione richiesto dal mittente. La risposta ARP fa in modo che il mittente memorizzi l'indirizzo MAC del sistema dell'utente non autorizzato nella cache ARP. Questo indirizzo MAC viene memorizzato anche dallo switch nella relativa tabella CAM. In questo modo, l'utente non autorizzato alla rete ha inserito l'indirizzo MAC del proprio sistema sia nella tabella CAM dello switch che nella cache ARP del mittente. In questo modo, l'utente non autorizzato può intercettare i frame destinati all'host che sta effettuando lo spoofing. I timer di hold-down nel menu di configurazione interfaccia possono essere utilizzati per mitigare gli attacchi di spoofing ARP impostando la durata di permanenza di una voce nella cache ARP. Tuttavia, i timer di attesa da soli sono insufficienti. È necessario modificare il tempo di scadenza della cache ARP su tutti i sistemi terminali e sulle voci ARP statiche. Un'altra soluzione che può essere utilizzata per mitigare vari attacchi alla rete basati su ARP, è l'uso dello snooping DHCP insieme all'ispezione ARP dinamica. Queste funzionalità Catalyst convalidano i pacchetti ARP in una rete e consentono l'intercettazione, la registrazione e l'eliminazione di pacchetti ARP con indirizzi MAC non validi per i binding di indirizzi IP. Lo snooping DHCP filtra i messaggi DHCP attendibili per garantire la sicurezza. Questi messaggi vengono quindi utilizzati per compilare e gestire una tabella di binding dello snooping DHCP. Lo snooping DHCP considera non attendibili i messaggi DHCP provenienti da qualsiasi porta rivolta all'utente che non sia una porta del server DHCP. Dal punto di vista dello snooping DHCP, queste porte utente non attendibili non devono inviare risposte del tipo di server DHCP, ad esempio DHCPOFFER, DHCPACK o DHCPNAK. La tabella binding dello snooping DHCP contiene l'indirizzo MAC, l'indirizzo IP, la durata del lease, il tipo di binding, il numero VLAN e le informazioni di interfaccia che corrispondono alle interfacce locali non attendibili di uno switch. La tabella di binding dello snooping DHCP non contiene informazioni sugli host interconnessi con un'interfaccia attendibile. Un'interfaccia non attendibile è un'interfaccia

configurata per ricevere messaggi dall'esterno della rete o del firewall. Un'interfaccia attendibile è un'interfaccia configurata per ricevere solo messaggi dalla rete. La tabella di binding dello snooping DHCP può contenere binding di indirizzi MAC dinamici e statici a indirizzi IP. L'ispezione ARP dinamica determina la validità di un pacchetto ARP in base all'indirizzo MAC valido per le associazioni di indirizzi IP archiviate in un database di snooping DHCP. Inoltre, l'ispezione ARP dinamica può convalidare i pacchetti ARP in base agli Access Control List (ACL) configurabili dall'utente. Ciò consente l'ispezione dei pacchetti ARP per gli host che utilizzano indirizzi IP configurati staticamente. L'ispezione ARP dinamica consente l'uso di Access Control Lists (PACL) per porta e VLAN per limitare i pacchetti ARP di indirizzi IP specifici a indirizzi MAC specifici.

- **Avvio di Dynamic Host Configuration Protocol (DHCP)** Un attacco di fame DHCP funziona trasmettendo richieste DHCP con indirizzi MAC falsificati. Se viene inviato un numero sufficiente di richieste, l'autore di un attacco alla rete può esaurire lo spazio di indirizzi disponibile per i server DHCP per un determinato periodo di tempo. L'utente non autorizzato della rete può quindi configurare un server DHCP non autorizzato sul proprio sistema e rispondere alle nuove richieste DHCP dei client della rete. L'inserimento di un server DHCP non autorizzato nella rete consente a un utente non autorizzato di fornire ai client indirizzi e altre informazioni sulla rete. Poiché le risposte DHCP includono in genere informazioni sul gateway predefinito e sul server DNS, l'autore di un attacco alla rete può specificare il proprio sistema come gateway predefinito e server DNS. Questo si traduce in un attacco man-in-the-middle. Tuttavia, lo scarico di tutti gli indirizzi DHCP non è richiesto per introdurre un server DHCP non autorizzato. Altre funzionalità della famiglia di switch Catalyst, come lo snooping DHCP, possono essere usate per proteggere il sistema da attacchi DHCP in caso di fame. Lo snooping DHCP è una funzione di sicurezza che filtra i messaggi DHCP non attendibili e crea e gestisce una tabella di binding dello snooping DHCP. La tabella di binding contiene informazioni quali l'indirizzo MAC, l'indirizzo IP, la durata del lease, il tipo di binding, il numero di VLAN e le informazioni di interfaccia che corrispondono alle interfacce locali non attendibili di uno switch. I messaggi non attendibili sono quelli ricevuti dall'esterno della rete o del firewall. Le interfacce switch non attendibili sono quelle configurate per ricevere tali messaggi dall'esterno della rete o del firewall. Altre funzionalità degli switch Catalyst, come la protezione dell'origine IP, possono fornire una difesa aggiuntiva contro attacchi come la fame DHCP e lo spoofing IP. Analogamente allo snooping DHCP, IP source Guard è abilitato sulle porte di livello 2 non attendibili. Tutto il traffico IP viene inizialmente bloccato, ad eccezione dei pacchetti DHCP acquisiti dal processo di snooping DHCP. Quando un client riceve un indirizzo IP valido dal server DHCP, alla porta viene applicato un PACL. In questo modo il traffico IP del client viene limitato agli indirizzi IP di origine configurati nel binding. Qualsiasi altro tipo di traffico IP con un indirizzo di origine diverso dagli indirizzi nel binding viene filtrato.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità di sicurezza Port Security, DHCP Snooping, Dynamic ARP Inspection e IP Source Guard.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

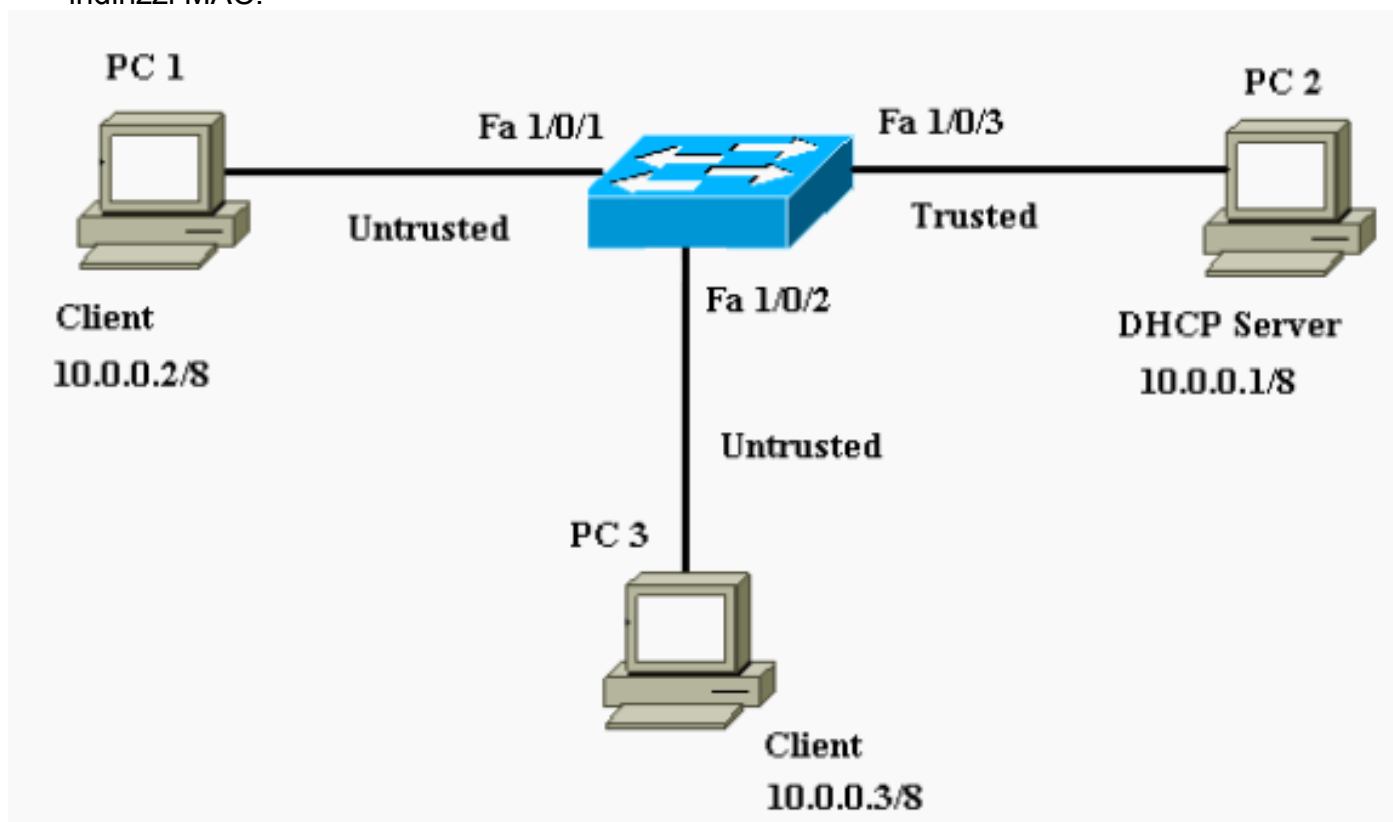
Le configurazioni dello switch Catalyst 3750 contengono quanto segue:

- [Sicurezza porta](#)
- [Snooping DHCP](#)
- [Ispezione ARP dinamica](#)
- [Protezione origine IP](#)

Esempio di rete

Nel documento viene usata questa impostazione di rete:

- PC 1 e PC 3 sono client collegati allo switch.
- Il PC 2 è un server DHCP collegato allo switch.
- Tutte le porte dello switch si trovano nella stessa VLAN (VLAN 1).
- Il server DHCP è configurato in modo da assegnare gli indirizzi IP ai client in base ai relativi indirizzi MAC.



Sicurezza porta

È possibile utilizzare la funzione di sicurezza delle porte per limitare e identificare gli indirizzi MAC delle stazioni a cui è consentito accedere alla porta. In questo modo l'input viene limitato a un'interfaccia. Quando si assegnano indirizzi MAC sicuri a una porta protetta, questa non inoltra i pacchetti con indirizzi di origine esterni al gruppo di indirizzi definiti. Se si limita a uno il numero di indirizzi MAC sicuri e si assegna un unico indirizzo MAC sicuro, alla workstation collegata a quella porta viene garantita l'intera larghezza di banda della porta. Se una porta è configurata come sicura e viene raggiunto il numero massimo di indirizzi MAC sicuri, quando l'indirizzo MAC di una stazione che tenta di accedere alla porta è diverso da tutti gli altri indirizzi MAC sicuri identificati, si verifica una violazione della sicurezza. Inoltre, se una stazione con un indirizzo MAC sicuro configurato o appreso dinamicamente su una porta protetta cerca di accedere a un'altra porta protetta, viene segnalata una violazione. Per impostazione predefinita, la porta viene chiusa quando viene superato il numero massimo di indirizzi MAC sicuri.

Nota: quando uno switch Catalyst 3750 si unisce a uno stack, il nuovo switch riceve gli indirizzi sicuri configurati. Tutti gli indirizzi sicuri dinamici vengono scaricati dal nuovo membro dello stack dagli altri membri.

Per le guide su come configurare la sicurezza delle porte, consultare le [linee guida sulla configurazione](#).

Qui, la funzione di sicurezza delle porte è mostrata configurata sull'interfaccia Fast Ethernet 1/0/2. Per impostazione predefinita, il numero massimo di indirizzi MAC sicuri per l'interfaccia è uno. È possibile usare il comando **show port-security interface** per verificare lo stato di sicurezza delle porte di un'interfaccia.

Sicurezza porta

```
Cat3750#show port-security interface fastEthernet 1/0/2
Port Security           : Disabled
Port Status             : Secure-down
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type               : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 0
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
!--- Default port security configuration on the switch.
Cat3750#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
Cat3750(config)#interface fastEthernet 1/0/2
Cat3750(config-if)#switchport port-security
Command rejected: FastEthernet1/0/2 is a dynamic port.
!--- Port security can only be configured on static
access ports or trunk ports. Cat3750(config-
if)#switchport mode access
!--- Sets the interface switchport mode as access.
Cat3750(config-if)#switchport port-security
!--- Enables port security on the interface.
Cat3750(config-if)#switchport port-security mac-address
0011.858D.9AF9
!--- Sets the secure MAC address for the interface.
Cat3750(config-if)#switchport port-security violation
shutdown
!--- Sets the violation mode to shutdown. This is the
default mode. Cat3750# !--- Connected a different PC (PC
4) to the FastEthernet 1/0/2 port !--- to verify the
port security feature. 00:22:51: %PM-4-ERR_DISABLE:
psecure-violation error detected on Fa1/0/2, putting
Fa1/0/2 in err-disable state 00:22:51: %PORT_SECURITY-2-
PSECURE_VIOLATION: Security violation occurred, caused
by MAC address 0011.8565.4B75 on port FastEthernet1/0/2.
00:22:52: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet1/0/2, changed state to down
00:22:53: %LINK-3-UPDOWN: Interface FastEthernet1/0/2,
changed state to down !--- Interface shuts down when a
security violation is detected. Cat3750#show interfaces
fastEthernet 1/0/2
FastEthernet1/0/2 is down, line protocol is down (err-
```

```

disabled)
!--- Output Suppressed. !--- The port is shown error-
disabled. This verifies the configuration. !--- Note:
When a secure port is in the error-disabled state, !---
you can bring it out of this state by entering !--- the
errdisable recovery cause psecure-violation global
configuration command, !--- or you can manually re-
enable it by entering the !--- shutdown and no shutdown
interface configuration commands.

Cat3750#show port-security interface fastEthernet 1/0/2
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0011.8565.4B75:1
Security Violation Count : 1

```

Nota: gli stessi indirizzi MAC non devono essere configurati come indirizzi MAC sicuri e statici su porte diverse di uno switch.

Quando un telefono IP è collegato a uno switch tramite la porta switchport configurata per la VLAN vocale, il telefono invia pacchetti CDP senza tag e pacchetti CDP voce con tag. L'indirizzo MAC del telefono IP viene quindi appreso sia sul PVID che sul VVID. Se non è stato configurato il numero appropriato di indirizzi sicuri, è possibile visualizzare un messaggio di errore simile al seguente:

```

%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 001b.77ee.eeee on port GigabitEthernet1/0/18.
PSECURE: Assert failure: psecure_sb->info.num_addr <= psecure_sb->max_addr:

```

Per risolvere il problema, è necessario impostare il numero massimo di indirizzi sicuri consentiti sulla porta su due (per i telefoni IP) più il numero massimo di indirizzi sicuri consentiti sulla VLAN di accesso.

Per ulteriori informazioni, fare riferimento a [Configurazione della sicurezza delle porte](#).

[Snooping DHCP](#)

Lo snooping DHCP funziona come un firewall tra host non attendibili e server DHCP. Lo snooping DHCP consente di distinguere tra le interfacce non attendibili connesse all'utente finale e le interfacce attendibili connesse al server DHCP o a un altro switch. Quando uno switch riceve un pacchetto su un'interfaccia non attendibile e l'interfaccia appartiene a una VLAN in cui lo snooping DHCP è abilitato, lo switch confronta l'indirizzo MAC di origine e l'indirizzo hardware del client DHCP. Se gli indirizzi corrispondono (impostazione predefinita), lo switch inoltra il pacchetto. Se gli indirizzi non corrispondono, lo switch scarta il pacchetto. Lo switch scarta un pacchetto DHCP quando si verifica una di queste situazioni:

- Un pacchetto da un server DHCP, ad esempio un pacchetto DHCP, DHCPcopper, DHCPcACK, DHCPnak o DHCPLEASEQUERY, viene ricevuto dall'esterno della rete o del

firewall.

- Un pacchetto viene ricevuto su un'interfaccia non attendibile e l'indirizzo MAC di origine e l'indirizzo hardware del client DHCP non corrispondono.
- Lo switch riceve un messaggio di trasmissione DHCPRELEASE o DHCPDECLINE con un indirizzo MAC nel database di binding dello snooping DHCP, ma le informazioni di interfaccia nel database di binding non corrispondono all'interfaccia su cui è stato ricevuto il messaggio.
- Un agente di inoltro DHCP inoltra un pacchetto DHCP, che include un indirizzo IP dell'agente di inoltro diverso da 0.0.0.0, oppure inoltra un pacchetto che include informazioni sull'opzione 82 a una porta non attendibile.

Per le linee guida su come configurare lo snooping DHCP, consultare il documento [DHCP Snooping Configuration Guidelines](#).

Nota: per il corretto funzionamento dello snooping DHCP, tutti i server DHCP devono essere connessi allo switch tramite interfacce attendibili.

Nota: in uno stack di switch con switch Catalyst 3750, lo snooping DHCP viene gestito sul dispositivo master. Quando un nuovo switch viene inserito nello stack, lo switch riceve la configurazione dello snooping DHCP dal dispositivo master. Quando un membro lascia lo stack, tutti i binding di snooping DHCP associati alla durata dello switch vengono eliminati.

Nota: per garantire che la durata del lease nel database sia precisa, Cisco consiglia di abilitare e configurare il protocollo NTP. Se NTP è configurato, lo switch scrive le modifiche del binding nel file di binding solo quando l'orologio di sistema dello switch è sincronizzato con NTP.

I server DHCP non autorizzati possono essere mitigati dalle funzionalità di snooping DHCP. Il comando **ip dhcp snooping** viene emesso per abilitare DHCP a livello globale sullo switch. Se configurate con lo snooping DHCP, tutte le porte nella VLAN non sono attendibili per le risposte DHCP. In questo caso, solo l'interfaccia Fast Ethernet 1/0/3 connessa al server DHCP è configurata come attendibile.

Snooping DHCP

```
Cat3750#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
Cat3750(config)#ip dhcp snooping
!--- Enables DHCP snooping on the switch.
Cat3750(config)#ip dhcp snooping vlan 1
!--- DHCP snooping is not active until DHCP snooping is
enabled on a VLAN. Cat3750(config)#no ip dhcp snooping
information option
!--- Disable the insertion and removal of the option-82
field, if the !--- DHCP clients and the DHCP server
reside on the same IP network or subnet.
Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip dhcp snooping trust
!--- Configures the interface connected to the DHCP
server as trusted. Cat3750#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit
```



```

(pps)
-----
-
FastEthernet1/0/3          yes          unlimited
!--- Displays the DHCP snooping configuration for the
switch. Cat3750#show ip dhcp snooping binding
MacAddress                IpAddress                Lease(sec)  Type
VLAN  Interface
-----
00:11:85:A5:7B:F5        10.0.0.2                 86391      dhcp-
snooping 1      FastEtheret1/0/1
00:11:85:8D:9A:F9        10.0.0.3                 86313      dhcp-
snooping 1      FastEtheret1/0/2
Total number of bindings: 2
!--- Displays the DHCP snooping binding entries for the
switch. Cat3750# !--- DHCP server(s) connected to the
untrusted port will not be able !--- to assign IP
addresses to the clients.

```

Per ulteriori informazioni, consultare il documento sulla [configurazione delle funzionalità DHCP](#).

[Ispezione ARP dinamica](#)

L'ispezione ARP dinamica è una funzione di sicurezza che convalida i pacchetti ARP in una rete. Intercetta, registra ed elimina i pacchetti ARP con binding IP-MAC non validi. Questa funzionalità protegge la rete da alcuni attacchi man-in-the-middle.

L'ispezione ARP dinamica garantisce che vengano inoltrate solo le richieste e le risposte ARP valide. Lo switch esegue le seguenti attività:

- Intercetta tutte le richieste e le risposte ARP su porte non attendibili
- Verifica che ciascuno di questi pacchetti intercettati disponga di un binding di indirizzi IP-MAC valido prima di aggiornare la cache ARP locale o prima di inoltrare il pacchetto alla destinazione appropriata
- Elimina i pacchetti ARP non validi

L'ispezione ARP dinamica determina la validità di un pacchetto ARP in base alle associazioni di indirizzi IP-MAC valide archiviate in un database attendibile, il database di associazione dello snooping DHCP. Questo database è creato dallo snooping DHCP se lo snooping DHCP è abilitato sulle VLAN e sullo switch. Se il pacchetto ARP viene ricevuto su un'interfaccia attendibile, lo switch lo inoltra senza alcun controllo. Sulle interfacce non attendibili, lo switch inoltra il pacchetto solo se è valido.

In ambienti non DHCP, l'ispezione ARP dinamica può convalidare i pacchetti ARP sugli ACL ARP configurati dall'utente per gli host con indirizzi IP configurati staticamente. È possibile usare il comando di configurazione globale **arp access-list** per definire un ACL ARP. Gli ACL ARP hanno la precedenza sulle voci nel database di binding dello snooping DHCP. Lo switch usa gli ACL solo se si usa il comando di configurazione globale **ip arp selection filter vlan** per configurare gli ACL. Innanzitutto, lo switch confronta i pacchetti ARP con ACL ARP configurati dall'utente. Se l'ACL ARP rifiuta il pacchetto ARP, lo switch rifiuta anche il pacchetto, anche se esiste un binding valido nel database popolato dallo snooping DHCP.

Per le linee guida su come configurare l'ispezione ARP dinamica, consultare [Linee guida di configurazione dell'ispezione ARP dinamica](#).

Il comando di configurazione globale **ip arp Inspection vlan** viene emesso per abilitare l'ispezione ARP dinamica per singola VLAN. In questo caso, solo l'interfaccia Fast Ethernet 1/0/3 connessa al server DHCP è configurata come attendibile con il comando **ip arp Inspection trust**. Lo snooping DHCP deve essere abilitato per consentire i pacchetti ARP con indirizzi IP assegnati dinamicamente. Per informazioni sulla configurazione dello snooping DHCP, vedere la sezione [Snooping DHCP](#) di questo documento.

Ispezione ARP dinamica

```
Cat3750#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Cat3750(config)#ip arp inspection vlan 1
!--- Enables dynamic ARP inspection on the VLAN.
Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip arp inspection trust
!--- Configures the interface connected to the DHCP
server as trusted. Cat3750#show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan    Configuration      Operation    ACL Match
Static ACL
-----
-----
     1    Enabled          Active
-----

Vlan    ACL Logging           DHCP Logging
-----
     1    Deny             Deny
!--- Verifies the dynamic ARP inspection configuration.
Cat3750#
```

Per ulteriori informazioni, consultare il documento sulla [configurazione dell'ispezione ARP dinamica](#).

Protezione origine IP

IP source Guard è una funzione di sicurezza che filtra il traffico in base al database di binding dello snooping DHCP e ai binding di origine IP configurati manualmente in modo da limitare il traffico IP su interfacce di layer 2 non indirizzate. È possibile utilizzare IP source guard per prevenire gli attacchi al traffico causati quando un host tenta di utilizzare l'indirizzo IP del router adiacente. La protezione dell'origine IP impedisce lo spoofing IP/MAC.

È possibile abilitare la protezione dell'origine IP quando lo snooping DHCP è abilitato su un'interfaccia non attendibile. Dopo aver abilitato IP source guard su un'interfaccia, lo switch blocca tutto il traffico IP ricevuto sull'interfaccia, ad eccezione dei pacchetti DHCP consentiti dallo snooping DHCP. All'interfaccia viene applicato un ACL della porta. L'ACL della porta consente solo il traffico IP con un indirizzo IP di origine nella tabella di binding dell'origine IP e nega tutto il resto del traffico.

La tabella di binding dell'origine IP contiene binding appresi dallo snooping DHCP o configurati manualmente (binding di origine IP statici). Una voce di questa tabella ha un indirizzo IP, l'indirizzo MAC associato e il numero VLAN associato. Lo switch utilizza la tabella di binding dell'origine IP

solo quando è abilitato IP source guard.

È possibile configurare IP source guard con il filtro degli indirizzi IP di origine o con il filtro degli indirizzi IP e MAC di origine. Quando con questa opzione viene abilitato IP source guard, il traffico IP viene filtrato in base all'indirizzo IP di origine. Lo switch inoltra il traffico IP quando l'indirizzo IP di origine corrisponde a una voce nel database di binding dello snooping DHCP o a un binding nella tabella di binding dell'origine IP. Quando con questa opzione è abilitato IP source guard, il traffico IP viene filtrato in base agli indirizzi IP e MAC di origine. Lo switch inoltra il traffico solo quando gli indirizzi IP e MAC di origine corrispondono a una voce nella tabella di binding dell'origine IP.

Nota: IP source guard è supportato solo sulle porte di livello 2, incluse le porte di accesso e trunk.

Per le linee guida su come configurare IP Source Guard, consultare il documento [Guide alla configurazione di IP Source Guard](#).

Qui, IP source guard con filtro IP di origine è configurato sull'interfaccia Fast Ethernet 1/0/1 con il comando **ip verify source**. Quando la protezione IP dell'origine con il filtro IP di origine è abilitata su una VLAN, lo snooping DHCP deve essere abilitato sulla VLAN di accesso a cui appartiene l'interfaccia. Usare il comando **show ip verify source** per verificare la configurazione IP source guard sullo switch.

```
Protezione origine IP

Cat3750#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
Cat3750(config)#ip dhcp snooping
Cat3750(config)#ip dhcp snooping vlan 1
!--- See the DHCP Snooping section of this document for
!--- DHCP snooping configuration information.
Cat3750(config)#interface fastEthernet 1/0/1
Cat3750(config-if)#ip verify source
!--- Enables IP source guard with source IP filtering.
Cat3750#show ip verify source
Interface  Filter-type  Filter-mode  IP-address
Mac-address      Vlan
-----
-----
Fa1/0/1      ip              active       10.0.0.2
1
!--- For VLAN 1, IP source guard with IP address
filtering is configured !--- on the interface and a
binding exists on the interface. Cat3750#
```

per ulteriori informazioni, fare riferimento a [Descrizione di IP Source Guard](#).

[Verifica](#)

Attualmente non è disponibile una procedura di verifica per questa configurazione.

[Risoluzione dei problemi](#)

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa

configurazione.

Informazioni correlate

- [Protezione delle reti con VLAN private e Access Control List VLAN](#)
- [Supporto dei prodotti LAN](#)
- [Supporto della tecnologia di switching LAN](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)