Layer 2 security functies op Cisco Catalyst Layer 3 Vaste Configuration Switches

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor een aantal van Layer 2-beveiligingsfuncties, zoals poortbeveiliging, DHCP-snooping, Dynamic Admission Protocol (ARP)-inspectie en IP-bronbeveiliging, die kunnen worden geïmplementeerd op vaste switches van Cisco Catalyst Layer 3.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de Cisco Catalyst 3750 Series Switch met versie 12.2(25)SEC2.

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Deze configuratie kan ook worden gebruikt bij deze hardware:

- Cisco Catalyst 3550 Series Switches
- Cisco Catalyst 3560 Series Switches
- Cisco Catalyst 3560-E Series Switches
- Cisco Catalyst 3750-E Series Switches

Conventies

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

Achtergrondinformatie

Overeenkomstig met routers hebben zowel Layer 2 als Layer 3 switches hun eigen sets netwerkbeveiligingsvereisten. Switches zijn vatbaar voor veel van dezelfde Layer 3-aanvallen als routers. Switches en Layer 2 van het OSI-referentiemodel in het algemeen zijn echter op verschillende manieren onderworpen aan netwerkaanvallen. Deze omvatten:

- **Content Adresseerbare Geheugen (CAM)-tabel overflow**Content Adresseerbare Memory (CAM)-tabellen zijn beperkt in omvang. Als er genoeg boekingen in de CAM-tabel worden ingevoerd voordat andere boekingen zijn verlopen, vult de CAM-tabel tot het punt dat geen nieuwe boekingen kunnen worden geaccepteerd. Meestal wordt de switch door een netwerkindringer overspoeld met een groot aantal ongeldige MAC-adressen (Source Media Access Control) totdat de CAM-tabel wordt ingevuld. Als dat gebeurt, overspoelt de switch alle poorten met inkomend verkeer omdat het niet het poortnummer voor een bepaald MAC-adres in de CAM-tabel kan vinden. De switch gedraagt zich in essentie als een hub. Als de indringer de stroom van ongeldige bron MAC adressen niet handhaaft, maakt de switch uiteindelijk de oudere MAC adreangen uit de CAM tabel uit en begint opnieuw als een switch te handelen. CAM-tabel overflow alleen overstromingen in het lokale VLAN zodat de indringer alleen verkeer ziet binnen het lokale VLAN waarop hij of zij is aangesloten.De CAM-aanval op tabel kan worden verzacht door poortbeveiliging op de switch te configureren. Deze optie bepaalt of de specificatie van de MAC-adressen op een bepaalde switch poort of de specificatie van het aantal MAC-adressen die door een switch-poort kunnen worden aangeleerd. Wanneer een ongeldig MAC-adres in de poort wordt gedetecteerd, kan de switch het aangetaste MAC-adres blokkeren of de poort sluiten. De specificatie van MAC-adressen op switches is veel te onhandig voor een productieomgeving. Een limiet van het aantal MAC-adressen op een switch poort is hanteerbaar. Een meer administratief schaalbare oplossing is de implementatie van dynamische havenveiligheid in de switch. Om dynamische poortbeveiliging uit te voeren, specificeert u een maximum aantal MAC-adressen die zullen worden aangeleerd.
- **Media Access Control (MAC)-adresomzetting**De spoofing-aanvallen van Media Access Control (MAC) omvatten het gebruik van een bekend MAC-adres van een andere host om te

proberen de target switch voorwaartse frames te maken die bestemd zijn voor de externe host van de netwerkaanvaller. Wanneer één enkel kader met het bron Ethernet adres van de andere gastheer wordt verzonden, overschrijft de netwerkaanvaller de ingang van de CAM tabel zodat de switch voorwaarts pakketten die voor de gastheer aan de netwerkaanvaller bestemd zijn. Totdat de gastheer verkeer verstuurt, ontvangt hij geen verkeer. Wanneer de host verkeer verstuurt, wordt de CAM-tabelingang opnieuw geschreven, zodat deze teruggaat naar de oorspronkelijke poort.Gebruik de havenveiligheidsfunctie om MAC spoofing aanvallen te verlichten. Poortbeveiliging biedt de mogelijkheid om het MAC-adres van het systeem te specificeren dat is aangesloten op een bepaalde poort. Dit voorziet ook in de mogelijkheid om een actie te specificeren om te ondernemen als er een schending van de havenveiligheid optreedt.

- **Protocol voor adresoplossing (ARP)**ARP wordt gebruikt om IP-adressering in kaart te brengen naar MAC-adressen in een segment van het lokale netwerk waar hosts van hetzelfde type wonen. Normaal, stuurt een gastheer een uitzending ARP verzoek om het adres van MAC van een andere gastheer met een bepaald IP adres te vinden, en een ARP antwoord komt van de gastheer wiens adres het verzoek aanpast. De verzoekende host slaat dan deze ARP-respons op. Binnen het ARP-protocol wordt een andere bepaling opgenomen voor hosts om ongevraagde ARP-antwoorden te kunnen uitvoeren. De ongevraagde ARP-antwoorden worden Gratuitous ARP (GARP) genoemd. GARP kan door een aanvaller oneigenlijk worden geëxploiteerd om de identiteit van een IP-adres in een LAN-segment te achterhalen. Dit wordt normaal gebruikt om de identiteit tussen twee hosts of al het verkeer naar en van een standaardgateway in een "man-in-the-middle" -aanval te bekrachtigen.Wanneer een ARP antwoord wordt gemaakt, kan een netwerkaanvaller zijn of haar systeem maken lijken de doelhost te zijn die door de zender wordt gezocht. Het ARP antwoord veroorzaakt dat de zender het MAC adres van het systeem van de netwerkaanvaller in het ARP cache opslaat. Dit MAC-adres wordt ook door de switch opgeslagen in de CAM-tabel. Op deze manier heeft de netwerkaanvaller het MAC-adres van zijn of haar systeem in zowel de switch CAM-tabel als het ARP-cache van de zender ingevoegd. Dit laat de netwerkaanvaller toe om kaders te onderscheppen die voor de gastheer bestemd zijn dat hij of zij spoofing is.Houd-down timers in het interface configuratie menu kan worden gebruikt om ARP spoofing aanvallen te verzachten door de lengte van tijd in te stellen een ingang in het ARP cache zal blijven. Houden-down timers zijn op zichzelf echter onvoldoende. Aanpassing van de ARP cache expiratie tijd op alle eindsystemen is vereist, evenals statische ARP-vermeldingen. Een andere oplossing die kan worden gebruikt om verschillende op ARP gebaseerde netwerkexplosies te verzachten is het gebruik van DHCP-sneoping samen met dynamische ARP-inspectie. Deze Catalyst functies valideren ARP-pakketten in een netwerk en staan de interceptie, vastlegging en verwijdering van ARP-pakketten met een ongeldig MAC-adres aan IP-adresbindingen toe.DHCP-snooping filters vertrouwde DHCP-berichten om beveiliging te bieden. Vervolgens worden deze berichten gebruikt om een DHCP-snooping-bindende tabel te maken en onderhouden. DHCP-snooping beschouwt DHCP-berichten die afkomstig zijn van een gebruikersgerichte poort die geen DHCP-serverpoort is als onbetrouwbaar. Vanuit een DHCP-sneoping-perspectief mogen deze onvertrouwde, gebruikersgerichte poorten geen DHCP-servertype-reacties verzenden, zoals DHCP-server-type, DHCPACK of DHCPNAK. De DHCP-snooping-bindende tabel bevat het MAC-adres, IP-adres, leasetijd, bindend type, VLAN-nummer en interfaceinformatie die overeenkomt met de lokale onvertrouwde interfaces van een switch. De DHCP-snooping-bindende tabel bevat geen informatie over hosts die onderling verbonden zijn met een vertrouwde interface. Een onvertrouwde interface is een interface die is ingesteld om berichten van buiten het netwerk of de firewall te ontvangen. Een

vertrouwde interface is een interface die is ingesteld om alleen berichten van binnen het netwerk te ontvangen. De DHCP-snooping-bindende tabel kan zowel dynamisch als statisch MAC-adres aan IP-adresbindingen bevatten.Dynamische ARP-inspectie bepaalt de geldigheid van een ARP-pakket dat is gebaseerd op het geldige MAC-adres voor IP-adresbindingen die zijn opgeslagen in een DHCP-spionagedatabase. Bovendien kan dynamische ARP-inspectie ARP-pakketten valideren op basis van door de gebruiker ingestelde toegangscontrolelijsten (ACL's). Dit staat voor de inspectie van ARP pakketten voor hosts toe die statistisch geconfigureerde IP-adressen gebruiken. Dynamische ARP-inspectie maakt het gebruik van per-poorts en VLAN Access Control Lists (PACL's) mogelijk om ARP-pakketten voor specifieke IP-adressen te beperken tot specifieke MAC-adressen.

- **Dynamic Host Configuration Protocol (DHCP)-start**Een DHCP-startaanval werkt door de uitzending van DHCP-verzoeken met gespoofde MAC-adressen. Als genoeg verzoeken worden verzonden, kan de netwerkaanvaller de adresruimte uitputten die voor de servers van DHCP beschikbaar is voor een periode. De netwerkaanvaller kan dan een beroerte DHCP-server op zijn of haar systeem instellen en reageren op nieuwe DHCP-verzoeken van klanten op het netwerk. Met de plaatsing van een schurkenserver van DHCP op het netwerk kan een netwerkaanvaller cliënten van adressen en andere netwerkinformatie voorzien. Omdat DHCP-reacties meestal de standaardgateway en DNS-serverinformatie omvatten, kan de netwerkaanvaller zijn of haar eigen systeem als standaardgateway en DNS-server leveren. Dit leidt tot een man-in-the-middle aanval. De uitlaat van alle DHCP-adressen is echter niet vereist om een robuuste DHCP-server te introduceren.Aanvullende functies in de Catalyst-familie van switches, zoals het DHCP-snooping, kunnen worden gebruikt om u te helpen beschermen tegen een DHCP-startaanval. DHCP-snooping is een beveiligingsfunctie die onvertrouwde DHCP-berichten filtert en een DHCP-snooping-bindende tabel bouwt en onderhoudt. De bindende tabel bevat informatie zoals het MAC-adres, IP-adres, leasetijd, bindend type, VLAN-nummer en de interfaceinformatie die overeenkomt met de lokale onvertrouwde interfaces van een switch. De onvertrouwde berichten zijn die ontvangen van buiten het netwerk of de firewall. Onvertrouwde switch interfaces zijn bedoeld om dergelijke berichten van buiten het netwerk of de firewall te ontvangen.Andere eigenschappen van de switch van de Catalyst, zoals IP bron Guard, kunnen extra defensie tegen aanvallen zoals de hongersnood van DHCP en IP spoofing verstrekken. Overeenkomstig met DHCP-snooping is IP-bronbeveiliging ingeschakeld op onvertrouwde Layer 2-poorten. Al IP-verkeer is aanvankelijk geblokkeerd, behalve voor DHCP-pakketten die door het DHCP-spionageproces worden opgenomen. Zodra een client een geldig IP-adres van de DHCP-server ontvangt, wordt een PACL-toegangscontrolelijst op de poort toegepast. Dit beperkt het client-IP-verkeer tot de bron-IP-adressen die in de band zijn ingesteld. Elk ander IP-verkeer met een bronadres dat niet de adressen in de band is, wordt gefilterd.

Configureren

In deze sectie, wordt u voorgesteld met de informatie om de eigenschappen van de Port Security, DHCP Snooping, Dynamische ARP Inspectie en IP Source Guard te configureren.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

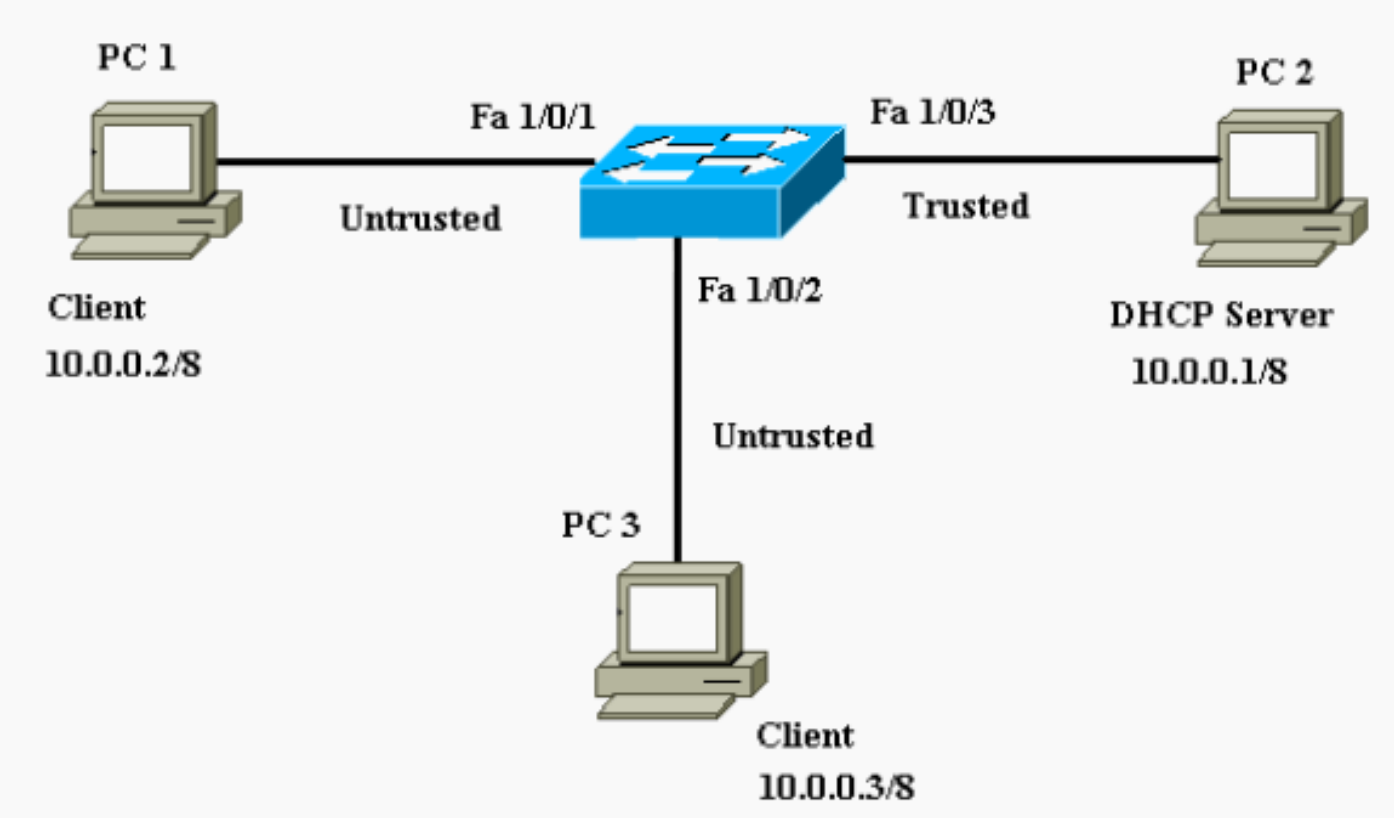
De configuraties van de Catalyst 3750 Switch bevatten deze:

- Poortbeveiliging
- DHCP-optie
- Dynamische ARP-inspectie
- IP-bronbewaking

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:

- PC 1 en PC 3 zijn klanten verbonden met de switch.
- PC 2 is een DHCP-server die is aangesloten op de switch.
- Alle poorten van de switch zijn in hetzelfde VLAN (VLAN 1).
- DHCP-server is ingesteld om IP-adressen aan de clients toe te wijzen op basis van hun MAC-adressen.



Poortbeveiliging

U kunt de havenveiligheidsfunctie gebruiken om de adressen van MAC van de stations te beperken en te identificeren die toegang tot de haven hebben. Dit beperkt de invoer naar een interface. Wanneer u veilige MAC-adressen aan een beveiligde poort toewijst, wordt de poort niet met bronadressen buiten de groep van gedefinieerde adressen verzonden. Als u het aantal beveiligde MAC-adressen beperkt tot één en één beveiligd MAC-adres toewijst, is het werkstation dat aan die poort is gekoppeld, verzekerd van de volledige bandbreedte van de poort. Als een poort is ingesteld als een beveiligde poort en het maximale aantal beveiligde MAC-adressen wordt bereikt, wanneer het MAC-adres van een station dat probeert de poort te bereiken verschilt van een van de geïdentificeerde beveiligde MAC-adressen, gebeurt er een schending van de beveiliging. Als een station met een beveiligd MAC-adres ingesteld is of op een beveiligde poort geleerd heeft, probeert u toegang te krijgen tot een andere beveiligde poort, dan wordt een schending gemarkeerd. Standaard wordt de poort afgesloten als het maximale aantal beveiligde MAC-adressen is overschreden.

Opmerking: Wanneer een Catalyst 3750-Switch zich bij een stapel voegt, ontvangt de nieuwe switch de geconfigureerde beveiligde adressen. Alle dynamische beveiligde adressen worden gedownload door het nieuwe stapellid van de andere stapelleden.

Raadpleeg de Configuratierichtlijnen voor de richtlijnen over het configureren van poortbeveiliging.

Hier wordt de poortbeveiligingsfunctie weergegeven in de FastEthernet 1/0/2 interface. Standaard is het maximale aantal beveiligde MAC-adressen voor de interface één. U kunt de **show port-security interface** opdracht uitgeven om de port security status voor een interface te controleren.

Poortbeveiliging

```
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
```

Opmerking: Dezelfde MAC-adressen mogen niet worden geconfigureerd als veilig en statisch MAC-adres in verschillende poorten van een switch.

Wanneer een IP-telefoon met een switch wordt verbonden door de switchpoort die voor spraak VLAN is geconfigureerd, verstuurt de telefoon niet-gelabelde CDP-pakketten en gelabelde spraak CDP-pakketten. Het MAC-adres van de IP-telefoon wordt dus op zowel de PVID als de VID geleerd. Als het juiste aantal beveiligde adressen niet is geconfigureerd, kunt u een foutmelding krijgen zoals in dit bericht:

```
%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_addrs <= psecure_sb->max_addrs:
```

U moet de maximum toegestane beveiligde adressen op de poort op twee instellen (voor IP-telefoon) plus het maximum aantal beveiligde adressen die op het toegangsVLAN zijn toegestaan om deze kwestie op te lossen.

Zie Port Security configureren voor meer informatie.

DHCP-optie

DHCP-snooping werkt als een firewall tussen onvertrouwde hosts en DHCP-servers. U gebruikt DHCP-simulatie om te onderscheiden tussen onvertrouwde interfaces die zijn aangesloten op de eindgebruiker en vertrouwde interfaces die zijn aangesloten op de DHCP-server of een andere switch. Wanneer een switch een pakje op een onvertrouwde interface ontvangt en de interface tot een VLAN behoort dat DHCP-snooping heeft ingeschakeld, vergelijkt de switch het bron-MAC-adres en het DHCP-client-hardwareadres. Als de adressen overeenkomen (het standaard), stuurt de switch het pakket door. Als de adressen niet overeenkomen, laat de switch het pakje vallen. De switch druppelt een DHCP-pakket in wanneer een van deze situaties zich voordoet:

- Een pakket van een server van DHCP, zoals een DHCPOFFER, DHCPACK, DHCPNAK, of het pakket DHCPLEASEQUERY, wordt ontvangen van buiten het netwerk of de firewall.
- Een pakket wordt ontvangen op een onvertrouwde interface en het bron-MAC-adres en het DHCP-client-hardwareadres komen niet overeen.

- De switch ontvangt een DHCPRELEASE- of DHCPDECLINE-uitzendbericht dat een MAC-adres in de DHCP-snooping-bindende database heeft, maar de interface-informatie in de bindende database komt niet overeen met de interface waarop het bericht werd ontvangen.
- Een DHCP-relais agent zendt een DHCP-pakket door, dat een relais-agent IP adres bevat dat niet 0.0.0.0 is, of de relais agent zendt een pakket toe dat optie-82 informatie aan een onvertrouwde poort bevat.

Raadpleeg de DHCP-configuratierichtlijnen voor de richtlijnen voor de configuratie van DHCP-opties.

Opmerking: voor een correcte werking van DHCP-spionage moeten alle DHCP-servers via vertrouwde interfaces op de switch worden aangesloten.

Opmerking: In een switch stapel met Catalyst 3750 Switches wordt DHCP-sneoping op de stackmodule beheerd. Wanneer een nieuwe switch zich bij de stapel aansluit, ontvangt de switch DHCP-sneoping configuratie van de stackmodule. Wanneer een lid de stapel verlaat, alle DHCP-snooping bindings geassocieerd met de switch leeftijd buiten.

Opmerking: om ervoor te zorgen dat de leasetijd in de database nauwkeurig is, raadt Cisco u aan NTP in te schakelen en te configureren. Als NTP wordt ingesteld, schrijft de switch bindende veranderingen in het bindingsbestand alleen wanneer de klok van het switch systeem met NTP gesynchroniseerd is.

DHCP-servers kunnen worden verzacht door DHCP-sneoping-functies. De opdracht **IP-communicatie** op **IP-communicatie** wordt gegeven om DHCP wereldwijd op de switch in te schakelen. Wanneer geconfigureerd met DHCP-snooping, zijn alle poorten in VLAN onvertrouwd voor DHCP-antwoorden. Hier wordt alleen de FastEthernet interface 1/0/3 die op de DHCP-server is aangesloten, geconfigureerd als vertrouwd.

DHCP-optie
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.
```

Zie DHCP-functies configureren voor meer informatie.

Dynamische ARP-inspectie

Dynamische ARP-inspectie is een beveiligingsfunctie die ARP-pakketten in een netwerk ondersteunt. Het onderschept, logt, en verwerpt ARP pakketten met ongeldige IP-to-MAC adresbindingen. Dit vermogen beschermt het netwerk tegen bepaalde man-in-het-midden aanvallen.

Dynamische ARP-inspectie garandeert dat alleen geldige ARP-verzoeken en -antwoorden worden doorgegeven. De switch voert deze activiteiten uit:

- Intercepteert alle ARP-verzoeken en antwoorden op onvertrouwde poorten
- Verifieert dat elk van deze onderschepte pakketten een geldig IP-naar-MAC adresband heeft voordat het het lokale ARP cache bijwerkt of voordat het pakket naar de juiste bestemming wordt doorgestuurd
- Verlaat ongeldige ARP-pakketten

Dynamische ARP-inspectie bepaalt de geldigheid van een ARP-pakket op basis van geldige IP-naar-MAC-adresbindingen die zijn opgeslagen in een vertrouwde database, de DHCP-snooping-bindende database. Deze database is gebouwd door DHCP-spionage als DHCP-snooping is ingeschakeld op de VLAN's en op de switch. Als het ARP-pakket op een vertrouwde interface wordt ontvangen, stuurt de switch het pakket zonder controles door. Op onvertrouwde interfaces stuurt de switch het pakket alleen door als het geldig is.

In niet-DHCP-omgevingen kan dynamische ARP-inspectie ARP-pakketten valideren tegen door de gebruiker ingesteld ARP ACL's voor hosts met statisch geconfigureerde IP-adressen. U kunt het **arp access-list** mondiaal configuratiebevel uitgeven om een ARP te definiëren. ARP ACL's hebben voorrang op items in de DHCP-snooping-bindende database. De switch gebruikt alleen ACL's als u de globale configuratie van de ACL's uitvoert van het IP-IP-**IP**-controlefilter. De switch vergelijkt eerst ARP-pakketten met door de gebruiker ingestelde ARP-ACL's. Als ARP het ARP-pakket ontkent, ontkent de switch het pakket ook, zelfs als er een geldige binding bestaat in de database die wordt bevolkt door DHCP-opties.

Raadpleeg de Richtlijnen voor configuratie van Dynamische ARP-inspectie voor de richtlijnen voor de configuratie van dynamische ARP-inspectie.

Het wereldwijd configuratiebevel van de **ip arp inspectie vlan** wordt uitgegeven om dynamische

ARP inspectie op een basis per-VLAN toe te staan. Hier wordt alleen de Fast Ethernet interface 1/0/3 die op de DHCP-server is aangesloten, geconfigureerd als vertrouwd met de opdracht **IP-**inspectierust. DHCP-sneoping moet worden ingeschakeld om ARP-pakketten toe te staan die dynamisch IP-adressen hebben toegewezen. Zie het gedeelte DHCP-optie van dit document voor informatie over de configuratie van DHCP-snooping.

Dynamische ARP-inspectie

```
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#
```

Zie Dynamische ARP-inspectie configureren voor meer informatie.

IP-bronbewaking

IP bron Guard is een beveiligingsfunctie die het verkeer filtert op basis van de DHCP-simulatie-bindende database en op handmatig ingestelde IP-bronverbindingen om IP-verkeer op niet-routed Layer 2-interfaces te beperken. U kunt IP bron Guard gebruiken om verkeersaanvallen te voorkomen die worden veroorzaakt wanneer een host probeert het IP-adres van zijn buurman te gebruiken. IP-bronbeveiliging voorkomt IP/MAC-spoofing.

U kunt IP-bronbeveiliging inschakelen wanneer DHCP-opties zijn ingeschakeld op een onvertrouwde interface. Nadat IP bron Guard op een interface is ingeschakeld, blokkeert de switch al het IP-verkeer dat op de interface wordt ontvangen, behalve de DHCP-pakketten die door DHCP zijn toegestaan. Een poort-ACL wordt toegepast op de interface. De poort ACL staat alleen IP-verkeer met een bron-IP-adres in de IP bron-bindende tabel toe en ontkent alle ander verkeer.

De IP bron-bindende tabel heeft bindingen die door DHCP-snuffelen worden geleerd of die handmatig worden ingesteld (statische IP-bronbindingen). Een ingang in deze tabel heeft een IP-adres, het bijbehorende MAC-adres en het bijbehorende VLAN-nummer. De switch gebruikt de IP bron-bindende tabel alleen wanneer IP bron-beveiliging is ingeschakeld.

U kunt IP bron Guard configureren met bronIP-adresfiltering of met bronIP- en MAC-adresfiltering.

Wanneer IP bron Guard met deze optie wordt ingeschakeld, wordt IP-verkeer gefilterd op basis van het IP-bronadres. De switch voorwaarts IP verkeer wanneer het bron IP-adres overeenkomt met een ingang in de DHCP-snooping-bindende database of een binding in de IP-bronbindende tabel. Wanneer IP bron Guard met deze optie wordt geactiveerd, wordt IP-verkeer gefilterd op basis van de bron IP- en MAC-adressen. De switch voorwaarts verkeer slechts wanneer de bron IP en MAC adressen een ingang in de IP bron verbindende tabel overeenkomen.

Opmerking: IP bron **Guard** wordt alleen ondersteund op Layer 2 poorten, wat toegang en boomstampoorten omvat.

Raadpleeg de IP Source Guard Configuration voor richtlijnen voor de configuratie van IP-bronbeveiliging.

Hier wordt IP bron Guard met bronIP-filtering ingesteld op de FastEthernet 1/0/1 interface met de **ip verify-**bronopdracht. Wanneer IP-bronbescherming met IP-bronfiltering op een VLAN is ingeschakeld, moet DHCP-spionage worden ingeschakeld op het toegangsVLAN waartoe de interface behoort. Geef de opdracht **show ip verify-bron** uit om de configuratie van de IP-bronbewaking in de switch te controleren.

IP-bronbewaking

```
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#
```

Raadpleeg Inzicht op IP-bronbewaking voor meer informatie.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Netwerkbeveiliging met Private VLAN's en VLAN-toegangscontrolelijsten
- LAN-productondersteuning
- Ondersteuning voor LAN-switching technologie
- Technische ondersteuning en documentatie – Cisco Systems