Fehlerbehebung bei dynamischer ARP-Inspektion (DAI) und IP Source Guard (IPSG) in Catalyst Switches

Inhalt

Einleitung

In diesem Dokument wird die Funktionsweise von Dynamic ARP Inspection (DAI) und IP Source Guard (IPSG) sowie deren Validierung in Catalyst Switches der Serie 9000 beschrieben.

DHCP-Snooping und verwandte Funktionen

Bevor Sie sich mit DAI und IPSG befassen, müssen Sie kurz über DHCP-Snooping sprechen, das eine Voraussetzung für DAI und IPSG ist.

Dynamic Host Configuration Protocol (DHCP) ist ein Client/Server-Protokoll, das einem Internet Protocol (IP)-Host automatisch seine IP-Adresse und andere zugehörige Konfigurationsinformationen wie die Subnetzmaske und den Standard-Gateway bereitstellt. Die RFCs 2131 und 2132 definieren DHCP als IETF-Standard (Internet Engineering Task Force) auf Basis des Bootstrap Protocol (BOOTP), einem Protokoll, mit dem DHCP viele Implementierungsdetails teilt. Mit DHCP können Hosts die erforderlichen TCP/IP-Konfigurationsdaten von einem DHCP-Server abrufen.

DHCP-Snooping ist eine Sicherheitsfunktion, die wie eine Firewall zwischen nicht vertrauenswürdigen Hosts und vertrauenswürdigen DHCP-Servern fungiert. Die DHCP-Snooping-Funktion führt folgende Aktivitäten aus:

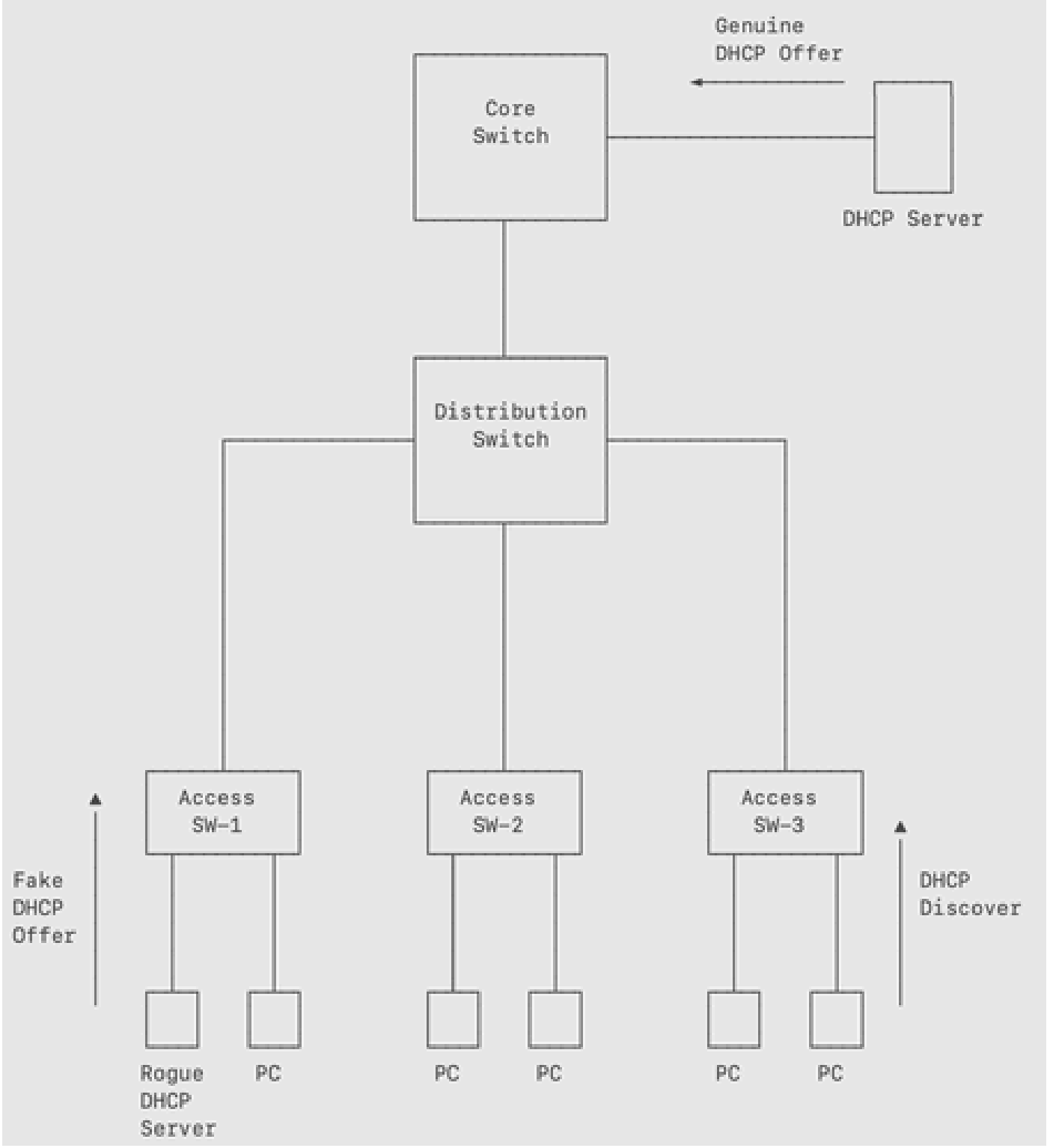
- Validiert DHCP-Nachrichten, die von nicht vertrauenswürdigen Quellen empfangen wurden, und filtert ungültige Nachrichten heraus.
- Rate - schränkt den DHCP-Datenverkehr von vertrauenswürdigen und nicht

vertrauenswürdigen Quellen ein.
- Erstellt und verwaltet die DHCP-Snooping-Bindungsdatenbank, die Informationen über nicht vertrauenswürdige Hosts mit geleasten IP-Adressen enthält.
- Nutzt die Datenbank für die DHCP-Snooping-Bindung, um nachfolgende Anfragen von nicht vertrauenswürdigen Hosts zu validieren.

DAI ist eine Sicherheitsfunktion, die ARP-Pakete (Address Resolution Protocol) in einem Netzwerk validiert. Mit DAI können Netzwerkadministratoren ARP-Pakete mit ungültigen MAC-Adressen abfangen, protokollieren und verwerfen, um sie an IP-Adressen zu binden. Diese Funktion schützt das Netzwerk vor bestimmten Man-in-the-Middle-Angriffen.

IPSG ist eine Sicherheitsfunktion, die den IP-Datenverkehr an nicht gerouteten Layer-2-Schnittstellen beschränkt, indem der Datenverkehr auf Basis der DHCP-Snooping-Bindungsdatenbank und manuell konfigurierter IP-Quell-Bindungen gefiltert wird. Sie können IPSG verwenden, um Datenverkehrsangriffe zu verhindern, wenn ein Host versucht, die IP-Adresse seines Nachbarn zu verwenden.

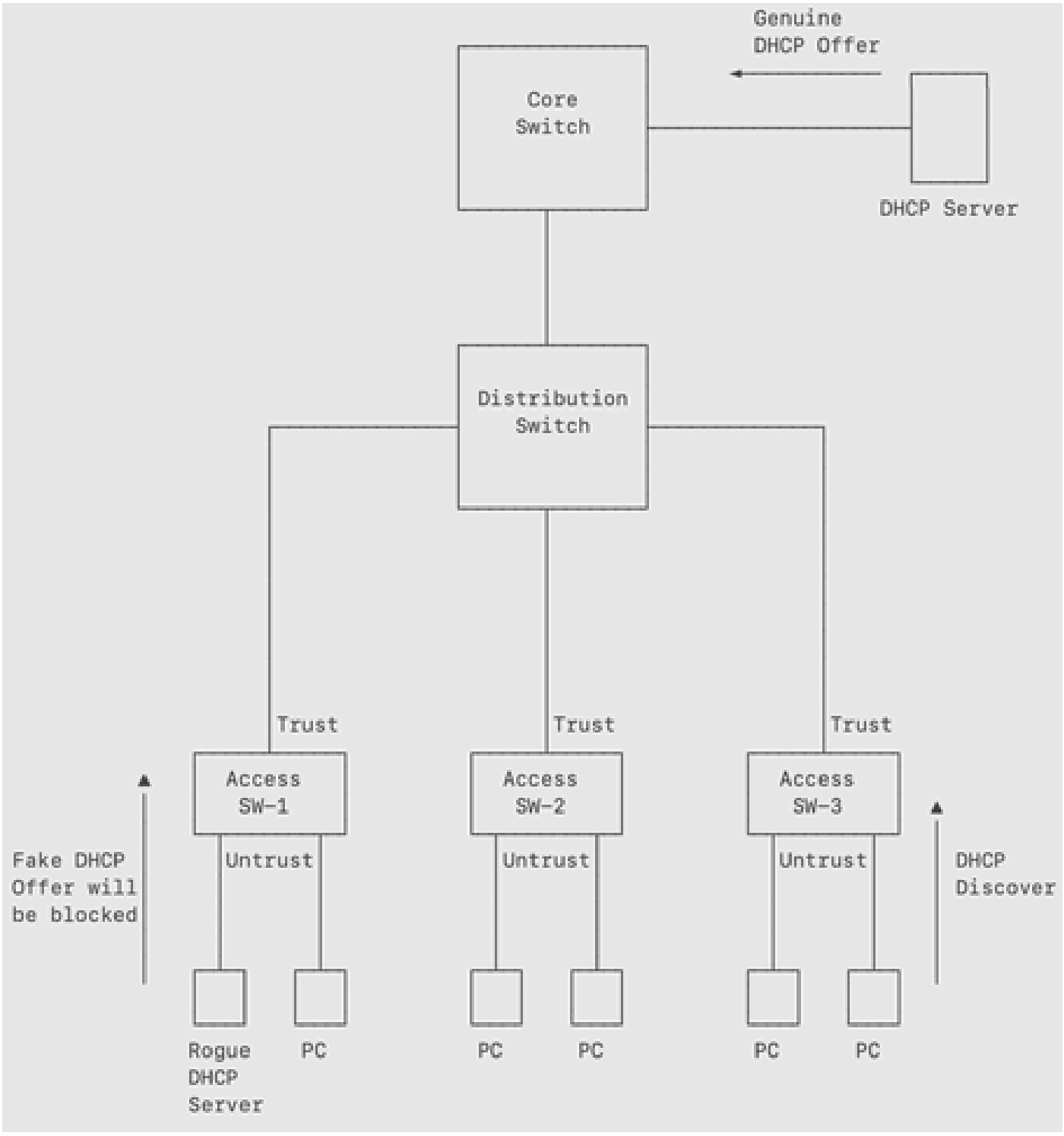
Szenario ohne DHCP-Snooping



1. In diesem Diagramm können Sie sehen, dass mehrere Clients eine IP-Adresse vom DHCP-Server erhalten möchten, der mit dem Core-Switch verbunden ist.
2. Es gibt jedoch einen bösartigen/nicht autorisierten DHCP-Server, der mit einem der Access-Layer-Switches verbunden ist, der die DHCP-Erkennung empfangen und DHCP-Angebote schneller senden kann als der eigentliche DHCP-Server.
3. Der Angreifer kann die Gateway-Adresse in der Offertnachricht so einstellen, dass er den gesamten Datenverkehr vom Client empfangen kann und somit die Vertraulichkeit der Kommunikation kompromittiert.

4. Dies ist bekannt als der Man In The Middle Angriff.

Szenario mit DHCP-Snooping

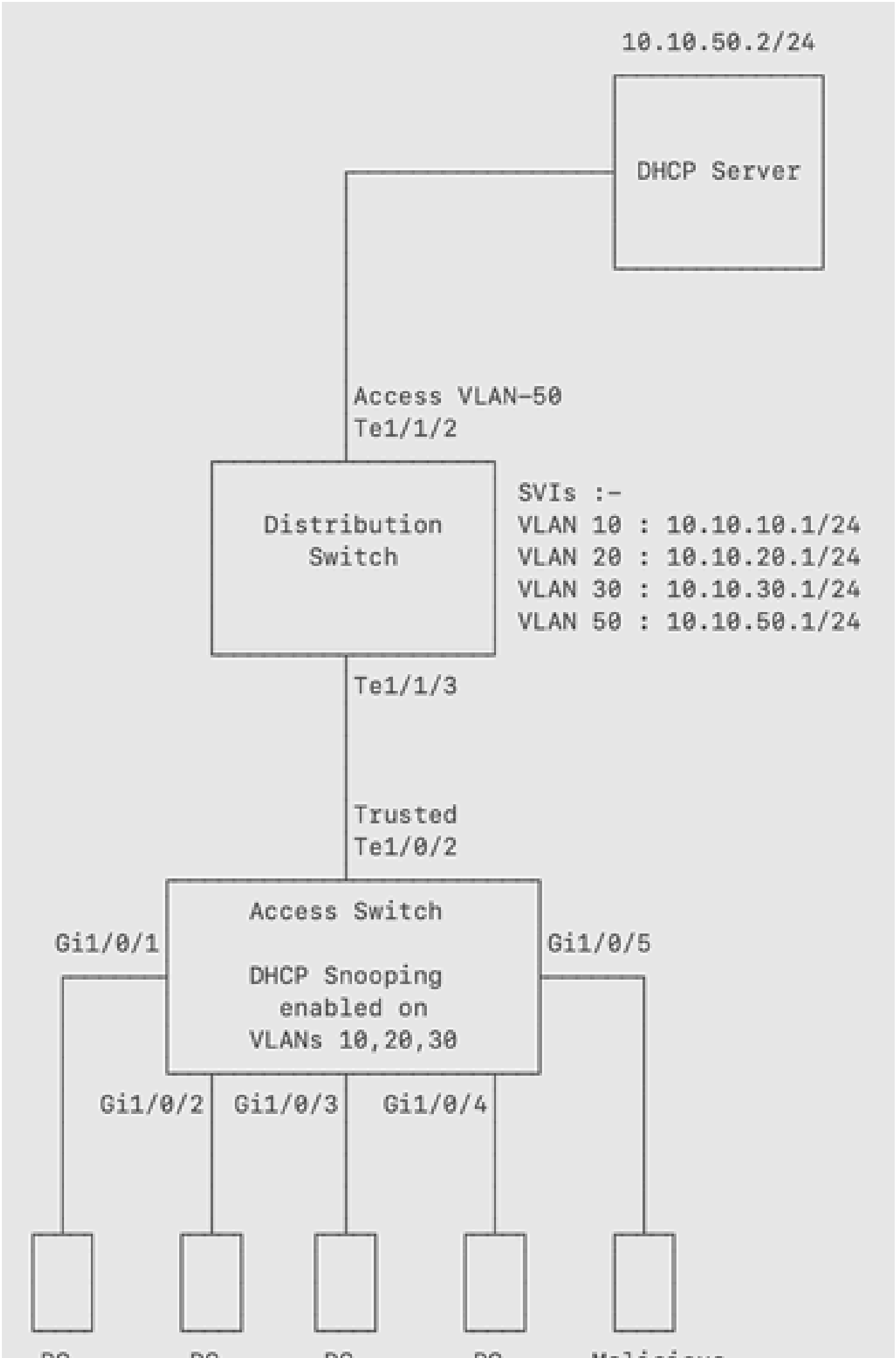


1. Durch Aktivieren von DHCP-Snooping auf den Access Switches konfigurieren Sie den Switch so, dass er DHCP-Datenverkehr abhört und alle schädlichen DHCP-Pakete stoppt, die an nicht vertrauenswürdigen Ports empfangen werden.
2. Sobald Sie DHCP-Snooping im Switch aktivieren, werden alle Schnittstellen automatisch nicht mehr vertrauenswürdig.
3. Lassen Sie die mit den Endgeräten verbundenen Ports nicht vertrauenswürdig, und

konfigurieren Sie die mit dem echten DHCP-Server verbundenen Ports als vertrauenswürdig.
4. Eine nicht vertrauenswürdige Schnittstelle blockiert DHCP-Angebotsmeldungen. DHCP-Angebotsmeldungen sind nur für vertrauenswürdige Ports zulässig.
5. Sie können die Anzahl der DHCP-Ermittlungspakete begrenzen, die End-Hosts pro Sekunde an eine nicht vertrauenswürdige Schnittstelle senden können. Dies ist ein Sicherheitsmechanismus, der den DHCP-Server vor einer ungewöhnlich hohen Anzahl eingehender DHCP-Entdeckungen schützt, die den Pool in kürzester Zeit aufbrauchen können.

In diesem Abschnitt wird erläutert, wie DHCP-Snooping in einem Switched Network konfiguriert wird:

Topologie:


10.10.50.2/24
DHCP Server
Access VLAN-50
Te1/1/2
Distribution Switch
SVIs :-
VLAN 10 : 10.10.10.1/24
VLAN 20 : 10.10.20.1/24
VLAN 30 : 10.10.30.1/24
VLAN 50 : 10.10.50.1/24
Te1/1/3
Trusted
Te1/0/2
Access Switch
DHCP Snooping enabled on VLANs 10,20,30
Gi1/0/1
Gi1/0/5
Gi1/0/2
Gi1/0/3
Gi1/0/4

```
ip dhcp snooping vlan 10,20,30
```

Schritt 2: Konfigurieren Sie DHCP-Snooping Trust auf allen Schnittstellen des Access Switches, die DHCP-Angebote von echten DHCP-Servern empfangen. Die Anzahl dieser Schnittstellen hängt vom Netzwerkdesign und der Anordnung der DHCP-Server ab. Dies sind die Schnittstellen, die zum echten DHCP-Server führen.

Access Switch

```
interface TenGigabitEthernet1/0/2
switchport mode trunk
ip dhcp snooping trust
```

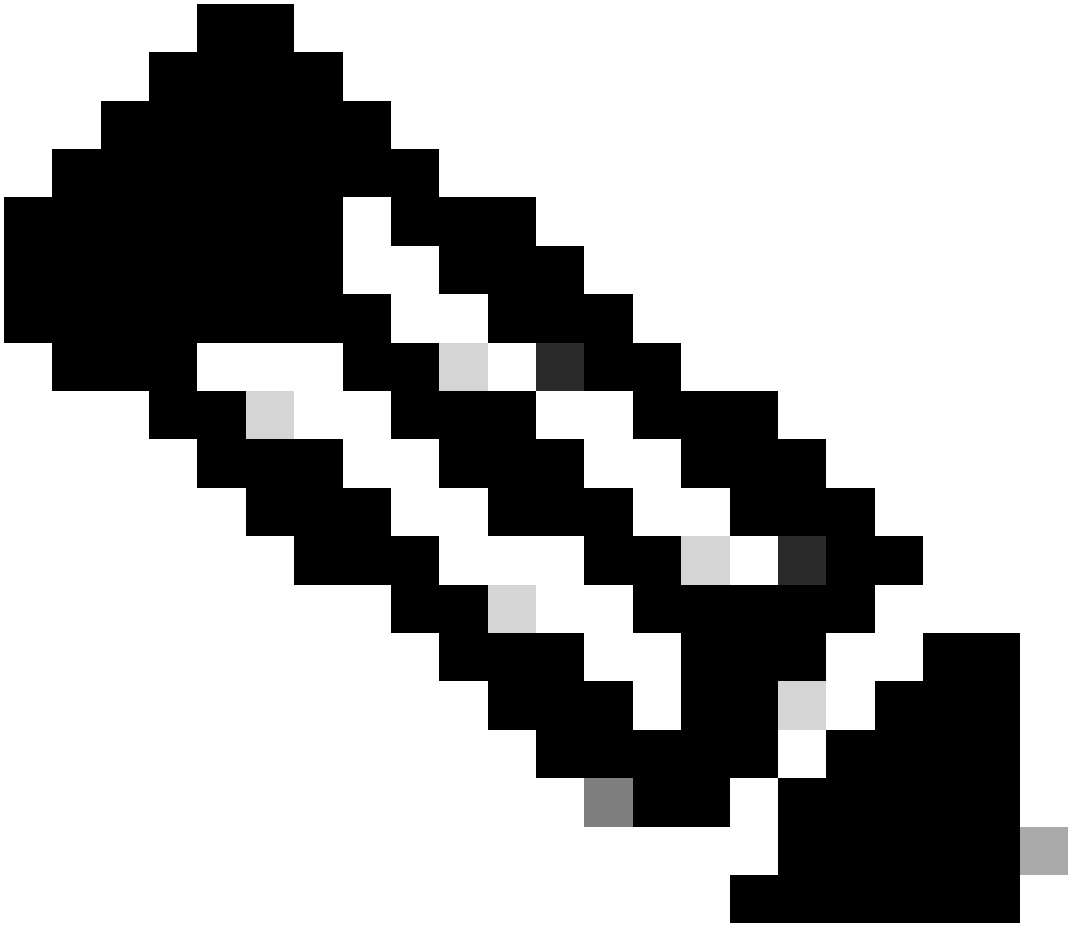
Schritt 3: Wenn Sie das DHCP-Snooping global konfigurieren, werden alle Ports im Switch automatisch nicht mehr vertrauenswürdig (mit Ausnahme der Ports, denen Sie manuell vertrauen, wie zuvor gezeigt). Sie können jedoch die Anzahl der DHCP-Erkennungspakete konfigurieren, die Endhosts pro Sekunde an nicht vertrauenswürdige Schnittstellen senden können.
Dies ist ein Sicherheitsmechanismus, der den DHCP-Server vor einer ungewöhnlich hohen Anzahl eingehender DHCP-Entdeckungen schützt, die den Pool in kürzester Zeit aufbrauchen können.

```
interface range Gi1/0/1-5
ip dhcp snooping limit rate 10
```

Überprüfen:

```
Access_SW#show ip dhcp snooping

Switch DHCP snooping is enabled

Switch DHCP gleaning is disabled

DHCP snooping is configured on following VLANs:

10,20,30

DHCP snooping is operational on following VLANs:

10,20,30

DHCP snooping is configured on the following L3 Interfaces:
```

```
Insertion of option 82 is disabled
   circuit-id default format: vlan-mod-port
   remote-id: 00fc.ba9e.3980 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:


Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
GigabitEthernet1/0/1             no         no              10
  Custom circuit-ids:
GigabitEthernet1/0/2             no         no              10
  Custom circuit-ids:
GigabitEthernet1/0/3             no         no              10
  Custom circuit-ids:
GigabitEthernet1/0/4             no         no              10
  Custom circuit-ids:
GigabitEthernet1/0/5             no         no              10
  Custom circuit-ids:
TenGigabitEthernet1/0/2          yes        yes             unlimited
  Custom circuit-ids:
```



Hinweis: Wenn Sie sich diese Ausgabe ansehen, sehen Sie, dass Gi1/0/5, das mit dem Malicious DHCP Server verbunden ist, in der **show ip dhcp snooping** Ausgabe als nicht vertrauenswürdig aufgeführt wird.

DHCP Snooping führt also alle Prüfungen für diese Ports durch.

Dadurch werden beispielsweise alle eingehenden DHCP-Angebote an diesem Port (Gi1/0/5) verworfen.

Die Tabelle mit der DHCP-Snooping-Bindung zeigt die IP-Adresse, die MAC-Adresse und die Schnittstelle für 3 Clients auf Gi1/0/1, Gi1/0/2 und Gi1/0/3:

```
Access_SW#show ip dhcp snooping binding
MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
00:FC:BA:9E:39:82 10.10.10.2 62488 dhcp-snooping 10 GigabitEthernet1/0/1
00:FC:BA:9E:39:A6 10.10.20.2 62492 dhcp-snooping 20 GigabitEthernet1/0/2
```

00:FC:BA:9E:39:89 10.10.30.3 62492 dhcp-snooping 30 GigabitEthernet1/0/3
Total number of bindings: 3

Zu Demonstrationszwecken wird dieip dhcp snooping trust Konfiguration unter Te1/0/2 im Access Switch entfernt. Bitte sehen Sie sich die im Switch generierten Protokolle an:

Access_SW#sh cdp neigh
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID Local Intrfce Holdtme Capability Platform Port ID
Dist_SW Ten 1/0/2 175 R S I C9300-48U Ten 1/1/3

Total cdp entries displayed : 1

Access_SW#show run int Te1/0/2
Building configuration...

Current configuration : 64 bytes
!
interface TenGigabitEthernet1/0/2
switchport mode trunk

*Apr 4 01:12:47.149: %DHCP_SNOOPING-5-DHCP_SNOOPING_UNTRUSTED_PORT: DHCP_SNOOPING drop message on untrusted port, message
*Apr 4 01:14:07.161: %DHCP_SNOOPING-5-DHCP_SNOOPING_UNTRUSTED_PORT: DHCP_SNOOPING drop message on untrusted port, message
*Apr 4 01:29:30.634: %DHCP_SNOOPING-5-DHCP_SNOOPING_UNTRUSTED_PORT: DHCP_SNOOPING drop message on untrusted port, message
*Apr 4 01:30:03.286: %DHCP_SNOOPING-5-DHCP_SNOOPING_UNTRUSTED_PORT: DHCP_SNOOPING drop message on untrusted port, message

- Wie Sie sehen, verwirft der Access Switch eingehende DHCP-Offer-Pakete auf Te1/0/2, da er nicht mehr vertrauenswürdig ist.
- Die MAC-Adressen in den Protokollen gehören zu den SVIs der VLANs 10, 20 und 30, da sie diese Angebote vom DHCP-Server an diese Clients senden.

ARP-Vergiftung

ARP stellt IP-Kommunikation innerhalb einer Layer-2-Broadcast-Domäne bereit, indem es eine IP-Adresse einer MAC-Adresse zuordnet. Es handelt sich um ein einfaches Protokoll, das jedoch anfällig für einen Angriff ist, der als ARP-Vergiftung bezeichnet wird.

ARP Poisoning ist ein Angriff, bei dem ein Angreifer gefälschte ARP-Antwortpakete an das Netzwerk sendet.

Ein böswilliger Benutzer kann mit Ihrem Layer-2-Netzwerk verbundene Hosts, Switches und Router angreifen, indem er die ARP-Caches der

mit dem Subnetz verbundenen Systeme vergiftet und den Datenverkehr abfängt, der für andere Hosts im Subnetz bestimmt ist

Das ist der klassische Man-in-the-Middle-Angriff.

Präventionsmechanismen

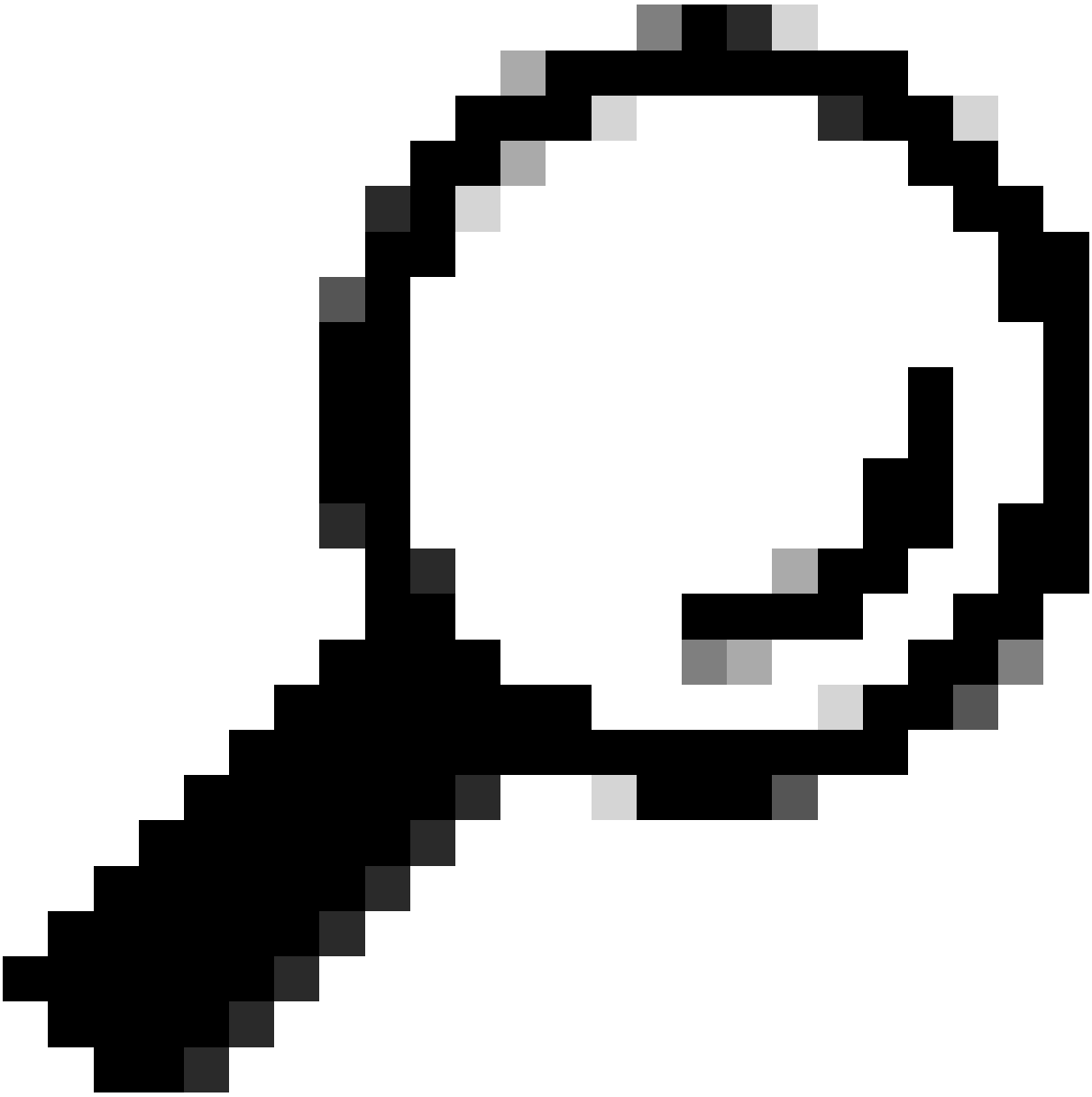
Dynamic ARP Inspection (DAI)

Dynamische ARP-Inspektion ist eine Sicherheitsfunktion, die ARP-Pakete in einem Netzwerk validiert. Er fängt ARP-Pakete mit ungültigen IP-MAC-Adressbindungen ab, protokolliert sie und verwirft sie. Diese Funktion schützt das Netzwerk vor bestimmten Man-in-the-Middle-Angriffen.

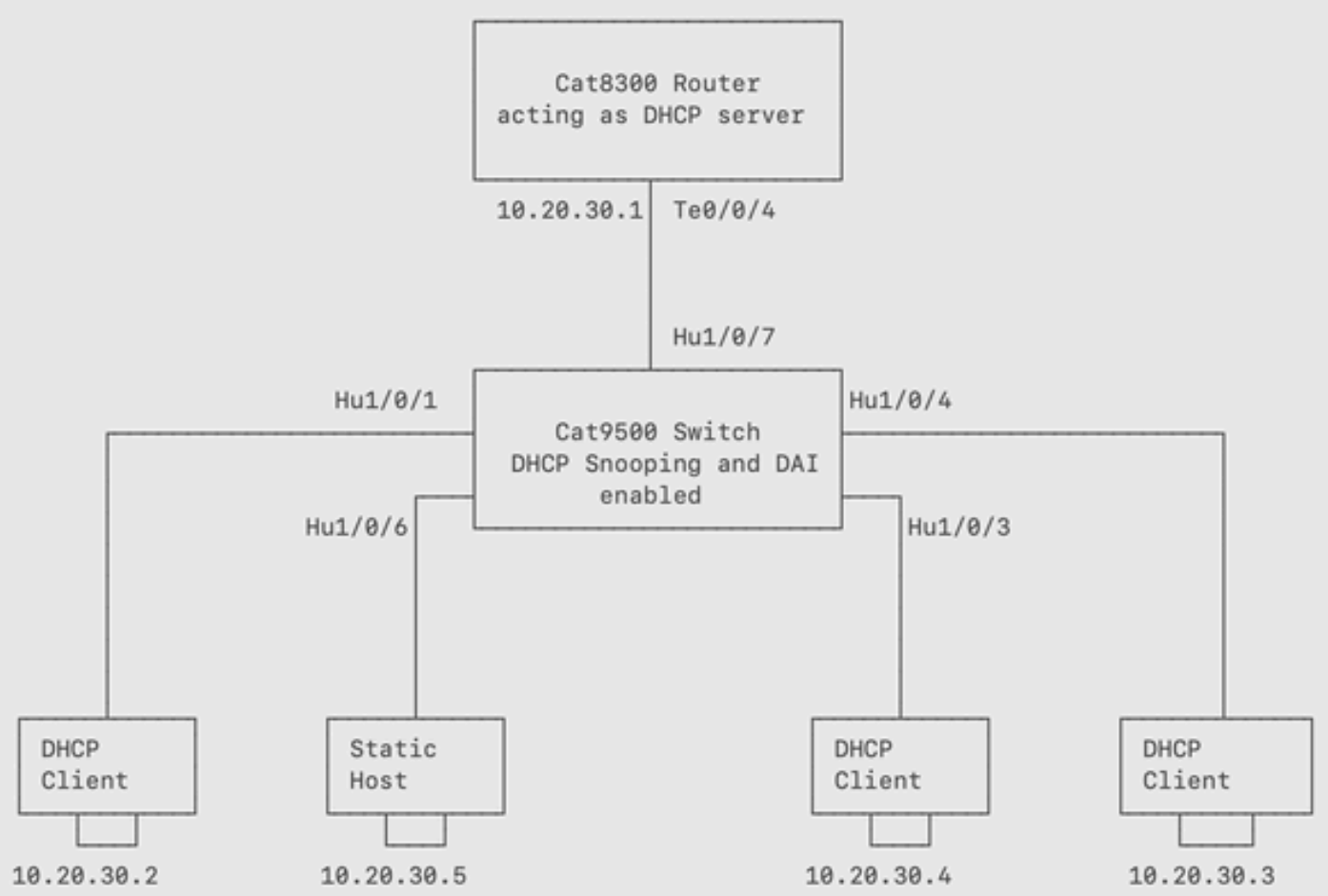
Durch die dynamische ARP-Inspektion wird sichergestellt, dass nur gültige ARP-Anfragen und -Antworten weitergeleitet werden. Der Switch führt folgende Aktivitäten aus:

- Abfangen aller ARP-Anfragen und -Antworten an nicht vertrauenswürdigen Ports
- Überprüft, ob jedes dieser abgefangenen Pakete über eine gültige IP-MAC-Adressbindung verfügt, bevor der lokale ARP-Cache aktualisiert oder das Paket an das entsprechende Ziel weitergeleitet wird.
- Löscht ungültige ARP-Pakete

Die dynamische ARP-Inspektion bestimmt die Gültigkeit eines ARP-Pakets auf der Grundlage gültiger IP-MAC-Adressbindungen, die in einer vertrauenswürdigen Datenbank, der DHCP-Snooping-Bindungsdatenbank, gespeichert sind.
Diese Datenbank wird durch DHCP-Snooping erstellt, wenn DHCP-Snooping auf den VLANs und auf dem Switch aktiviert ist. Wenn das ARP-Paket über eine vertrauenswürdige Schnittstelle empfangen wird, leitet der Switch das Paket ohne Prüfungen weiter.
Bei nicht vertrauenswürdigen Schnittstellen leitet der Switch das Paket nur weiter, wenn es gültig ist.



Tipp: Siehe https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/configuration_guide/sec/b_179_sec_9300_cg/configuring_dynamic_arp_inspection.html



Dieses Bild zeigt den Cat9500-Switch, der mit vier Hosts verbunden ist, von denen drei Hosts DHCP-Clients sind und ein Host eine statische IP-Adresse (10.20.30.5) hat. Der DHCP-Server ist ein Router der Serie Cat8300, der mit einem DHCP-Pool konfiguriert ist.

Die Topologie oben zeigt, wie DAI ungültige ARP-Anforderungen an einer Schnittstelle erkennt und das Netzwerk vor böswilligen Angreifern schützt.

Konfiguration:

Schritt 1: DHCP-Snooping und DAI global im Switch konfigurieren

```
F241.24.02-9500-1#sh run | i dhcp
ip dhcp snooping vlan 10
no ip dhcp snooping information option
ip dhcp snooping
```

```
F241.24.02-9500-1#sh run | i ip arp
ip arp inspection vlan 10
```

Schritt 2: Konfigurieren Sie die Schnittstelle Hu1/0/7, die als vertrauenswürdiger Port mit dem DHCP-Server verbunden ist. So können die DHCP-Angebote die Schnittstelle nutzen und anschließend die DHCP-Clients erreichen.

```
F241.24.02-9500-1#sh run int Hu1/0/7
Building configuration...

Current configuration : 85 bytes
!
interface HundredGigE1/0/7
switchport access vlan 10
ip dhcp snooping trust
end
```

Schritt 3: Konfigurieren Sie die mit den DHCP-Clients verbundenen Ports als Zugriffsports, die VLAN 10 zulassen.

```
F241.24.02-9500-1#sh run int Hu1/0/3
Building configuration...

Current configuration : 61 bytes
!
interface HundredGigE1/0/3
switchport access vlan 10
end
```

```
F241.24.02-9500-1#sh run int Hu1/0/4
Building configuration...

Current configuration : 61 bytes
!
interface HundredGigE1/0/4
switchport access vlan 10
end
```

```
F241.24.02-9500-1#sh run int Hu1/0/1
Building configuration...

Current configuration : 61 bytes
!
interface HundredGigE1/0/1
switchport access vlan 10
end
```

```
F241.24.02-9500-1#sh run int Hu1/0/6
Building configuration...

Current configuration : 85 bytes
!
```

```
interface HundredGigE1/0/6
switchport access vlan 10
end
```

Schritt 4: Überprüfen Sie, ob die DHCP-Clients eine IP-Adresse vom DHCP-Server aus der Bindungstabelle für DHCP-Snooping auf dem Cat9500 erhalten haben.

```
F241.24.02-9500-1#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
78:72:5D:1B:7F:3F   10.20.30.2       85046       dhcp-snooping   10    HundredGigE1/0/1
5C:71:0D:CD:EE:0C   10.20.30.3       85065       dhcp-snooping   10    HundredGigE1/0/4
2C:4F:52:01:AA:CC   10.20.30.4       85085       dhcp-snooping   10    HundredGigE1/0/3
Total number of bindings: 3
```

Sie können die Bindungen auch im DHCP-Server überprüfen.

```
DHCP_Server#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/              Lease expiration        Type       State      Interface
                Hardware address/
                User name
10.20.30.2      0063.6973.636f.2d37.    Apr 08 2024 07:04 AM    Automatic  Active     TenGigabitEthernet0/0/4
                3837.322e.3564.3162.
                2e37.6633.662d.4875.
                312f.302f.31
10.20.30.3      0063.6973.636f.2d35.    Apr 08 2024 07:04 AM    Automatic  Active     TenGigabitEthernet0/0/4
                6337.312e.3064.6364.
                2e65.6530.632d.5465.
                312f.302f.35
```

10.20.30.4 0063.6973.636f.2d32. Apr 08 2024 07:05 AM Automatic Active TenGigabitEthernet0/0/4

6334.662e.3532.3031.

2e61.6163.632d.5465.

312f.302f.35

Schritt 5: Ändern Sie die IP-Adresse des Hosts, der mit Hu1/0/6 verbunden ist, von 10.20.30.5 in 10.20.30.2, und senden Sie einen Ping an die anderen DHCP-Clients von diesem Host.

```
Static_Host#ping 10.20.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Static_Host#ping 10.20.30.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.4, timeout is 2 seconds:
.....
```

Die folgenden ungültigen ARP-Protokolle sind auf dem Cat9500-Switch zu sehen:

```
F241.24.02-9500-1#
*Apr 7 09:29:24.520: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*Apr 7 09:29:26.520: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*Apr 7 09:29:28.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*Apr 7 09:29:30.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*Apr 7 09:29:32.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
F241.24.02-9500-1#
*Apr 7 09:29:47.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*Apr 7 09:29:49.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*Apr 7 09:29:51.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*Apr 7 09:29:53.522: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*Apr 7 09:29:55.523: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
```

- Wie Sie sehen können, können Sie vom Static_Host aus keinen Ping an 10.20.30.3 und 10.20.30.4 senden.
Obwohl Static_Host versucht hat, die IP-Adresse des legitimen DHCP-Clients zu fälschen, war dies nicht möglich, da alle ARP-Pakete, die auf Hu1/0/6 eintreffen, vom Switch überprüft und mit den Daten in der Tabelle mit der DHCP-Snooping-Bindung verglichen werden.

- Die nachfolgenden Protokolle vom Cat9500-Switch bestätigen, dass die ARP-Anforderungen, die vom Static_Host an die DHCP-Clients gesendet werden, verworfen werden.

- Der Cat9500-Switch erreicht dies durch Verweis auf die Datenbank für die DHCP-Snooping-Bindung.

- Wenn eine ARP-Anforderung Hu1/0/6 mit der Quell-MAC-IP-Adresse eingeht, die nicht mit den Werten in der Datenbank für die DHCP-Snooping-Bindung übereinstimmt, verwirft der Switch die ARP-Anforderung.

Schritt 6: Überprüfen:

F241.24.02-9500-1#show ip arp inspection

Source Mac Validation : Disabled

Destination Mac Validation : Disabled

IP Address Validation : Disabled

Vlan	Configuration	Operation	ACL Match	Static ACL
10	Enabled	Active	DAI	No

Vlan	ACL Logging	DHCP Logging	Probe Logging
10	Deny	Deny	Off

Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops
10	9	39	39	0

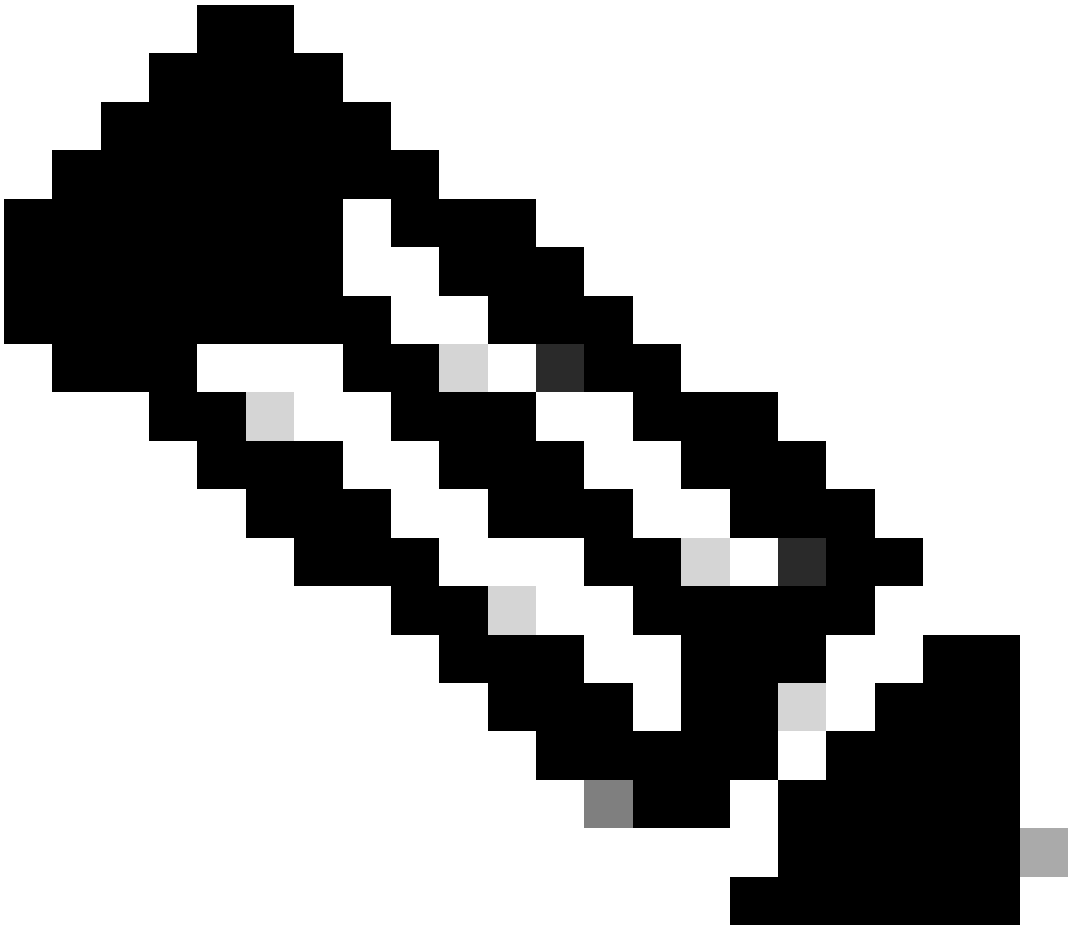
Vlan	DHCP Permits	ACL Permits	Probe Permits	Source MAC Failures
10	6	3	0	0

Vlan Dest MAC Failures IP Validation Failures Invalid Protocol Data

---- ---------- ---------- ----------

10 0 0 0

In dieser Ausgabe sehen Sie die Anzahl der wegen DAI blockierten und zulässigen Pakete im VLAN 10 des Cat9500-Switches.



Hinweis: Ein sehr wichtiges Szenario könnte ein legitimer Host im Netzwerk sein, dem eine statische IP-Adresse (z. B. 10.20.30.5) zugewiesen ist?

Der Host versucht zwar nicht, irgendetwas zu manipulieren, ist jedoch vom Netzwerk isoliert, da seine MAC-IP-Bindungsdaten nicht in der Datenbank für die DHCP-Snooping-Bindung vorhanden sind.

Der Grund hierfür ist, dass der statische Host DHCP nie zum Empfang der IP-Adresse verwendet hat, da er ihm statisch zugewiesen wurde.

Es gibt einige Problemumgehungen, die implementiert werden können, um Verbindungen mit legitimen Hosts bereitzustellen, die über statische IP-Adressen verfügen.

Option 1:

Konfigurieren Sie die Schnittstelle, die mit dem Host verbunden ist, mit ip arp inspection trust.

```
F241.24.02-9500-1#sh run int HundredGigE 1/0/6
Building configuration...

Current configuration : 110 bytes
!
interface HundredGigE1/0/6
switchport access vlan 10
switchport mode access
ip arp inspection trust
end
```

```
Static_Host#ping 10.20.30.4
*Apr 7 18:44:45.299 JST: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (192.168.1.5)
F241.24.02-9300-STACK#ping 10.20.30.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

Static_Host#ping 10.20.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

Static_Host#ping 10.20.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Option 2:

Zulassen des statischen Hosts mithilfe einer ARP-Zugriffsliste:

```
F241.24.02-9500-1#sh run | s arp access-list
arp access-list DAI
permit ip host 10.20.30.5 mac host 7035.0956.7ee4

F241.24.02-9500-1#sh run | i ip arp ins
ip arp inspection filter DAI vlan 10
```

```
Static_Host#ping 10.20.30.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

```
Static_Host#ping 10.20.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

```
Static_Host#ping 10.20.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Option 3.

Konfigurieren Sie einen Bindungstabelleneintrag für den statischen Host.

```
F241.24.02-9500-1#sh run | i binding
ip source binding 7035.0956.7EE4 vlan 10 10.20.30.5 interface Hu1/0/6
```

```
F241.24.02-9500-1#show ip source binding
MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
78:72:5D:1B:7F:3F 10.20.30.2 80640 dhcp-snooping 10 HundredGigE1/0/1
5C:71:0D:CD:EE:0C 10.20.30.3 80659 dhcp-snooping 10 HundredGigE1/0/4
70:35:09:56:7E:E4 10.20.30.5 infinite static 10 HundredGigE1/0/6
2C:4F:52:01:AA:CC 10.20.30.4 80679 dhcp-snooping 10 HundredGigE1/0/3
Total number of bindings: 4
```

```
Static_Host#ping 10.20.30.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

```
Static_Host#ping 10.20.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

```
Static_Host#ping 10.20.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Zusätzliche Optionen bei DAI:

```
F241.24.02-9500-1(config)#ip arp inspection validate ?
dst-mac Validate destination MAC address
ip Validate IP addresses
src-mac Validate source MAC address
```

Bei src-mac überprüfen Sie die Quell-MAC-Adresse im Ethernet-Header mit der Absender-MAC-Adresse im ARP-Body. Diese Prüfung wird für ARP-Anforderungen und -Antworten durchgeführt. Wenn diese Funktion aktiviert ist, werden Pakete mit unterschiedlichen MAC-Adressen als ungültig klassifiziert und verworfen

Für dst-mac überprüfen Sie die Ziel-MAC-Adresse im Ethernet-Header anhand der Ziel-MAC-Adresse im ARP-Body. Diese Prüfung wird für ARP-Antworten durchgeführt. Wenn diese Funktion aktiviert ist, werden Pakete mit unterschiedlichen MAC-Adressen als ungültig klassifiziert und verworfen.

Überprüfen Sie den ARP-Text für IP auf ungültige und unerwartete IP-Adressen. Die Adressen umfassen 0.0.0.0, 255.255.255.255 und alle IP-Multicast-Adressen. Absender-IP-Adressen werden in allen ARP-Anforderungen und -Antworten geprüft, und Ziel-IP-Adressen werden nur in ARP-Antworten geprüft.

Sie können auch die ARP-Ratenbegrenzung konfigurieren. Standardmäßig sind für ARP-Datenverkehr an nicht vertrauenswürdigen Schnittstellen 15 pps zulässig:

```
Switch(config)#interface Gigabitethernet<>
Switch(config-if)#ip arp inspection limit rate 10
```

IP-Quellschutz

- IPSG ist eine Sicherheitsfunktion, die den IP-Datenverkehr an nicht gerouteten Layer-2-Schnittstellen beschränkt, indem der Datenverkehr anhand der DHCP-Snooping-Bindungsdatenbank und manuell konfigurierter IP-Quell-Bindungen gefiltert wird.

- Sie können IPSG verwenden, um Datenverkehrsangriffe zu verhindern, wenn ein Host versucht, die IP-Adresse seines Nachbarn zu verwenden.

- Sie können IPSG aktivieren, wenn DHCP-Snooping auf einer nicht vertrauenswürdigen Schnittstelle aktiviert ist. Nachdem IPSG an einer Schnittstelle aktiviert wurde, blockiert der Switch den gesamten IP-Datenverkehr, der an der Schnittstelle empfangen wurde, mit Ausnahme der DHCP-Pakete, die durch DHCP-Snooping zugelassen wurden.

- Der Switch verwendet eine Quell-IP-Lookup-Tabelle in der Hardware, um IP-Adressen an Ports zu binden. Für die IP- und MAC-Filterung wird eine Kombination aus Quell-IP- und Quell-MAC-Suche verwendet. IP-Datenverkehr mit einer Quell-IP-Adresse in der Bindungstabelle ist zulässig, der gesamte andere Datenverkehr wird abgelehnt.

- Die IP-Quellbindungstabelle enthält Bindungen, die vom DHCP-Snooping abgerufen oder manuell konfiguriert werden (statische IP-Quellbindungen). Ein Eintrag in dieser Tabelle enthält eine IP-Adresse, die zugehörige MAC-Adresse und die zugehörige VLAN-Nummer. Der Switch verwendet die IP-Quellbindungstabelle nur, wenn IP Source Guard aktiviert ist.

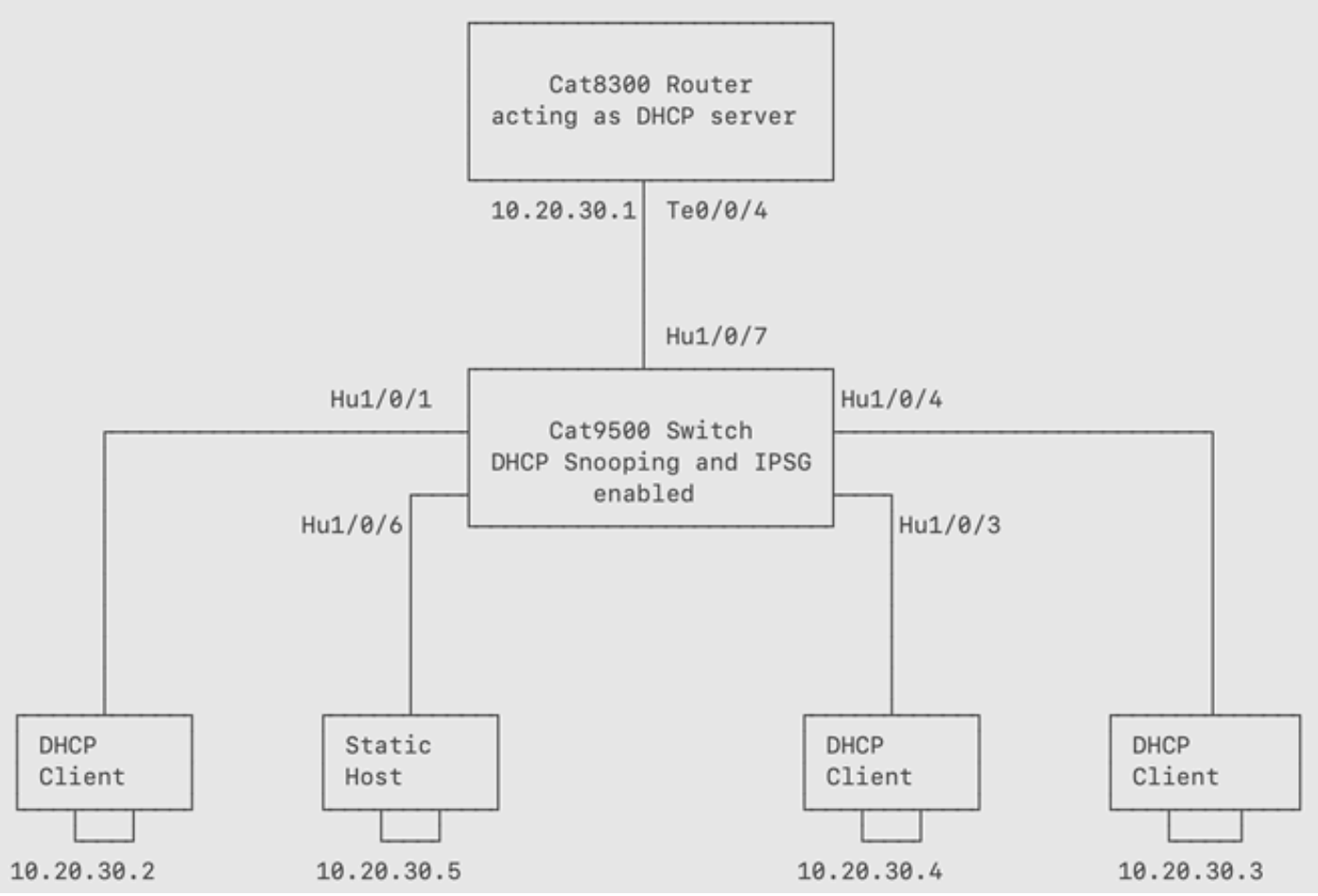
- Sie können IPSG mit einer Quell-IP-Adressfilterung oder mit einer Quell-IP- und MAC-Adressfilterung konfigurieren.

IPSG für statische Hosts

- IPSG für statische Hosts ermöglicht IPSG die Arbeit ohne DHCP. IPSG für statische Hosts benötigt Einträge in der Nachverfolgungstabelle von IP-Geräten, um Port-ACLs zu installieren. Der Switch erstellt statische Einträge basierend auf ARP-Anfragen oder anderen IP-Paketen, um die Liste der gültigen Hosts für einen bestimmten Port zu verwalten.

Referenz:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/configuration_guide/sec/b_179_sec_9300_cg/configuring_ip_source_guard.html



Der Cat9500-Switch ist mit vier Hosts verbunden, von denen drei Hosts DHCP-Clients sind und ein Host eine statische IP-Adresse hat. Der DHCP-Server ist ein Router der Serie Cat8300, der mit einem DHCP-Pool konfiguriert ist.
Mit dieser Topologie können Sie zeigen, wie IPSG Datenverkehr von Hosts erkennt und blockiert, deren MAC-IP-Bindungen nicht in der Datenbank für die DHCP-Snooping-Bindung vorhanden sind.

Konfiguration:

Schritt 1: Globales Konfigurieren von DHCP-Snooping auf dem Cat9500-Switch

F241.24.02-9500-1#sh run | i dhcp
ip dhcp snooping vlan 10
no ip dhcp snooping information option
ip dhcp snooping

Schritt 2: Konfigurieren Sie die Schnittstelle Te1/0/7, die als vertrauenswürdiger Port mit dem DHCP-Server verbunden ist. Dadurch können die DHCP-Angebote die Schnittstelle aufrufen und anschließend die DHCP-Clients erreichen.

F241.24.02-9500-1#sh run int Hu1/0/7

Building configuration...

Current configuration : 85 bytes

```
!
interface HundredGigE1/0/7
switchport access vlan 10
ip dhcp snooping trust
end
```

Schritt 3: Konfigurieren Sie die mit den DHCP-Clients verbundenen Ports als Zugriffsports, die VLAN 10 zulassen.

```
F241.24.02-9500-1#sh run int Hu1/0/3
Building configuration...

Current configuration : 61 bytes
!
interface HundredGigE1/0/3
switchport access vlan 10
end

F241.24.02-9500-1#sh run int Hu1/0/4
Building configuration...

Current configuration : 61 bytes
!
interface HundredGigE1/0/4
switchport access vlan 10
end

F241.24.02-9500-1#sh run int Hu1/0/1
Building configuration...

Current configuration : 61 bytes
!
interface HundredGigE1/0/1
switchport access vlan 10
end

F241.24.02-9500-1#sh run int Hu1/0/6
Building configuration...

Current configuration : 85 bytes
!
interface HundredGigE1/0/6
switchport access vlan 10
end
```

Schritt 4: Überprüfen Sie, ob die DHCP-Clients die IP-Adresse vom DHCP-Server erhalten haben.

```
F241.24.02-9500-1#sh ip dhcp snooping binding
MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
78:72:5D:1B:7F:3F 10.20.30.2 85046 dhcp-snooping 10 HundredGigE1/0/1
5C:71:0D:CD:EE:0C 10.20.30.3 85065 dhcp-snooping 10 HundredGigE1/0/4
```

2C:4F:52:01:AA:CC 10.20.30.4 85085 dhcp-snooping 10 HundredGigE1/0/3
Total number of bindings: 3

F241.24.02-9500-1#show ip source binding
MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
78:72:5D:1B:7F:3F 10.20.30.2 64764 dhcp-snooping 10 HundredGigE1/0/1
5C:71:0D:CD:EE:0C 10.20.30.3 64783 dhcp-snooping 10 HundredGigE1/0/4
2C:4F:52:01:AA:CC 10.20.30.4 64803 dhcp-snooping 10 HundredGigE1/0/3
Total number of bindings: 3

DHCP_Server#show ip dhcp binding

Bindings from all pools not associated with VRF:

IP address Client-ID/ Lease expiration Type State Interface

Hardware address/

User name

10.20.30.2 0063.6973.636f.2d37. Apr 08 2024 07:04 AM Automatic Active TenGigabitEthernet0/0/4

3837.322e.3564.3162.

2e37.6633.662d.4875.

312f.302f.31

10.20.30.3 0063.6973.636f.2d35. Apr 08 2024 07:04 AM Automatic Active TenGigabitEthernet0/0/4

6337.312e.3064.6364.

2e65.6530.632d.5465.

312f.302f.35

10.20.30.4 0063.6973.636f.2d32. Apr 08 2024 07:05 AM Automatic Active TenGigabitEthernet0/0/4

6334.662e.3532.3031.

2e61.6163.632d.5465.

312f.302f.35

Schritt 5: Konfigurieren Sie IPSG unter den mit allen End-Hosts verbundenen Schnittstellen (3 DHCP-Clients und 1 Host mit statischer IP-Adresse).

```
F241.24.02-9500-1#sh run int Hu1/0/3
Building configuration...

Current configuration : 79 bytes
!
interface HundredGigE1/0/3
switchport access vlan 10
ip verify source
end

F241.24.02-9500-1#sh run int Hu1/0/4
Building configuration...

Current configuration : 79 bytes
!
interface HundredGigE1/0/4
switchport access vlan 10
ip verify source
end

F241.24.02-9500-1#sh run int Hu1/0/1
Building configuration...

Current configuration : 79 bytes
!
interface HundredGigE1/0/1
switchport access vlan 10
ip verify source
end

F241.24.02-9500-1#sh run int Hu1/0/6
Building configuration...

Current configuration : 103 bytes
!
interface HundredGigE1/0/6
switchport access vlan 10
ip verify source
end
```

Überprüfen:

```
F241.24.02-9500-1#show ip verify source

Interface  Filter-type  Filter-mode  IP-address       Mac-address       Vlan

---------  -----------  -----------  ---------------  ----------------  ----

Hu1/0/1    ip          active       10.20.30.2                     10

Hu1/0/3    ip          active       10.20.30.4                     10

Hu1/0/4    ip          active       10.20.30.3                     10
```

Hu1/0/6 ip active deny-all 10

Von dieser Ausgabe aus können Sie sehen, dass das Feld "IP Address" (IP-Adresse) für Hu1/0/6 auf "deny-all" (Alle verweigern) gesetzt ist, da in der Tabelle mit den DHCP-Snooping-Bindungen keine dieser Schnittstelle entsprechende MAC-IP-Bindung vorhanden ist.

Schritt 6: Versuchen Sie, die DHCP-Clients mit den IP-Adressen 10.20.30.2, 10.20.30.3 und 10.20.30.4 vom Static_Host aus zu pingen.

Static_Host#ping 10.20.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Static_Host#ping 10.20.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Static_Host#ping 10.20.30.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.4, timeout is 2 seconds:
.....

F241.24.02-9500-1(config)# ip source binding <mac-address-of-static-host> vlan 10 10.20.30.5 interface Hu1/0/6

F241.24.02-9500-1#show run int Hu1/0/6

*Apr 7 15:13:48.449: %SYS-5-CONFIG_I: Configured from console by console

F241.24.02-9500-1#show ip verify source

Interface Filter-type Filter-mode IP-address Mac-address Vlan

--------- ----------- ----------- --------------- ----------------- ----

Hu1/0/1 ip active 10.20.30.2 10

Hu1/0/3 ip active 10.20.30.4 10

Hu1/0/4 ip active 10.20.30.3 10

Hu1/0/6 ip active 10.20.30.5 10

F241.24.02-9500-1#show ip source binding

MacAddress IpAddress Lease(sec) Type VLAN Interface

------------------ --------------- ---------- ------------- ---- --------------------

78:72:5D:1B:7F:3F 10.20.30.2 62482 dhcp-snooping 10 HundredGigE1/0/1

5C:71:0D:CD:EE:0C 10.20.30.3 62501 dhcp-snooping 10 HundredGigE1/0/4

70:35:09:56:7E:E4 10.20.30.5 infinite static 10 HundredGigE1/0/6

2C:4F:52:01:AA:CC 10.20.30.4 62521 dhcp-snooping 10 HundredGigE1/0/3

Total number of bindings: 4

Verification:

Static_Host#ping 10.20.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Static_Host#ping 10.20.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Static_Host#ping 10.20.30.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Weitere Optionen, die mit IPSG verfügbar sind:

IPSG filtert eingehenden Datenverkehr standardmäßig auf nicht vertrauenswürdigen Ports, die nur auf IP-Adressen basieren.

Wenn Sie die Filterung sowohl nach IP- als auch nach MAC-Adresse durchführen möchten, gehen Sie wie folgt vor.

F241.24.02-9500-1#sh run int Hu1/0/1
Building configuration...

Current configuration : 89 bytes
!
interface HundredGigE1/0/1
switchport access vlan 10
ip verify source mac-check
end

```
F241.24.02-9500-1#sh run int Hu1/0/3
Building configuration...

Current configuration : 89 bytes
!
interface HundredGigE1/0/3
switchport access vlan 10
ip verify source mac-check
end

F241.24.02-9500-1#sh run int Hu1/0/4
Building configuration...

Current configuration : 89 bytes
!
interface HundredGigE1/0/4
switchport access vlan 10
ip verify source mac-check
end

F241.24.02-9500-1#sh run int Hu1/0/6
Building configuration...

Current configuration : 113 bytes
!
interface HundredGigE1/0/6
switchport access vlan 10
switchport mode access
ip verify source mac-check
end
```

```
F241.24.02-9500-1#show ip verify source

Interface  Filter-type  Filter-mode  IP-address      Mac-address       Vlan

---------  -----------  -----------  ---------------  -----------------  ----

Hu1/0/1    ip-mac       active       10.20.30.2       78:72:5D:1B:7F:3F   10

Hu1/0/3    ip-mac       active       10.20.30.4       2C:4F:52:01:AA:CC   10

Hu1/0/4    ip-mac       active       10.20.30.3       5C:71:0D:CD:EE:0C   10

Hu1/0/6    ip-mac       active       deny-all         deny-all            10
```

In dieser Ausgabe können Sie sehen, dass der Filtertyp ip-mac ist. Daher filtert der Switch nun die eingehenden Pakete an diesen Schnittstellen sowohl auf Basis der Quell-IP- als auch der MAC-Adresse.

Tipps zur Fehlerbehebung für DAI und IPSG

- Als Erstes sollten Sie bei der Behebung von Problemen im Zusammenhang mit DAI und IPSG überprüfen, ob die Bindungstabelle

für DHCP-Snooping korrekt ausgefüllt wurde.

- Bevor Sie diese Funktionen aktivieren, behandeln Sie die Endpunkte mit statischen IP-Adressen. Wenn die Erreichbarkeit dieser Geräte nicht beeinträchtigt werden soll, konfigurieren Sie statische Bindungen, oder wenden Sie eine der zuvor genannten Methoden an, damit der Switch diesen Endgeräten vertraut.

- Aktivieren Sie bei der Konfiguration von DAI oder IPSG in einer Umgebung, in der DHCP-Snooping noch nicht aktiviert ist und Clients bereits IPs vom DHCP-Server erhalten haben, zunächst DHCP-Snooping, und führen Sie einen der beiden Schritte aus:

    - Bounce der mit dem Client verbundenen Schnittstellen, sodass diese ihre Lease verlängern.

    - Warten Sie, bis der Lease-Zeitraum für die Clients automatisch verlängert wird. Dies kann mehr Zeit in Anspruch nehmen, erspart Ihnen jedoch den Aufwand, alle mit dem Client verbundenen Ports manuell zurückzurufen.

- Wenn Sie einen der beiden oben genannten Schritte ausführen, wird eine neue DORA-Transaktion ausgelöst. Der Switch durchsucht die DORA-Pakete und aktualisiert die Bindungstabelle. Ist dies nicht der Fall und DAI oder IPSG wird nach der Konfiguration von DHCP-Snooping sofort aktiviert, kann es zu einem Problem kommen, bei dem alle DHCP-Clients im Netzwerk die Verbindung zum Netzwerk verlieren.

- Stellen Sie bei der Behebung von Verbindungsproblemen in einer Umgebung, in der DAI oder IPSG konfiguriert ist, sicher, dass die Bindungstabelle für DHCP-Snooping nicht beschädigt ist. Stellen Sie sicher, dass der Switch auf die Datenstruktur zugreifen kann, in der diese Tabelle gespeichert ist.

- Es kann vorkommen, dass die Bindungstabelle auf ein Medium exportiert wird, das nach dem Hochfahren des Switches eine gewisse Zeit benötigt, um initialisiert zu werden, oder dass der Switch aus irgendeinem Grund nicht mehr darauf zugreifen kann. Möglicherweise haben Sie in solchen Szenarien Verbindungsprobleme beobachtet.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.