

## Laboratório de DHCP Snooping

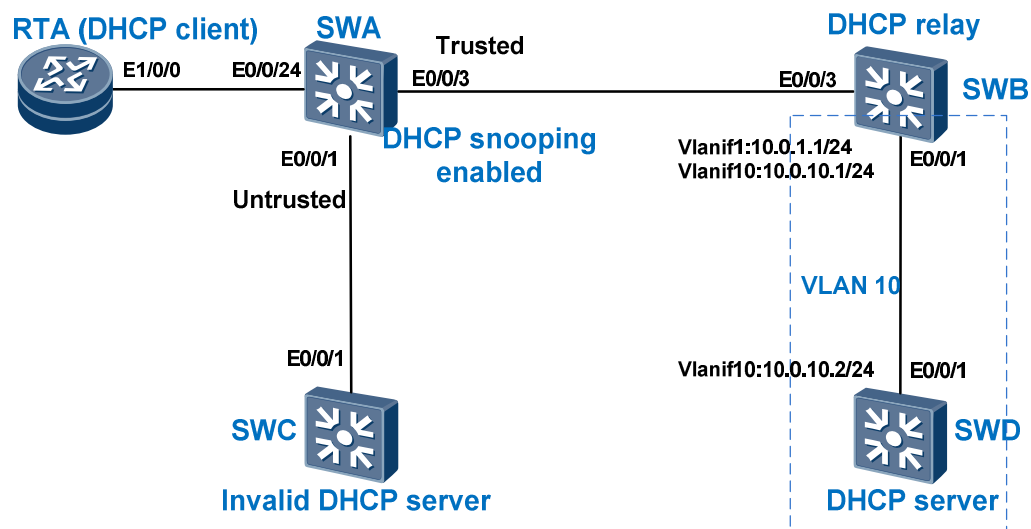
### Objetivos

Após completar este laboratório você será capaz de:

- Entender como DHCP snooping funciona.
- Configurar o DHCP Snooping nos switches SX700
- Configurar o DHCP nos switches SX700
- Configurar o DHCP relay nos switches SX700

### 1.1 Descrição da Rede

Figure 1-1 Diagrama de rede para configuração do DHCP Snooping



Como mostrado na rede anterior, o SWA funciona como um switch de acesso e o SWB como DHCP Relay, pois o servidor legítimo encontra-se na VLAN 10. O RTA pode obter um endereço IP do SWD (servidor DHCP) usando o segmento de rede 10.0.1.0/24 e o endereço de gateway 10.0.1.1. Este laboratório assume que o SWC é um servidor DHCP falso que aloca endereços IP falsos usando o segmento de rede 192.168.1.0/24 e o endereço de gateway 192.168.1.1. Neste laboratório, você precisa configurar o DHCP snooping no SWA para permitir pacotes apenas no servidor DHCP que venha pela E0/0/3 e para evitar ataques falsos ao servidor DHCP.

## 1.2 Procedimento de Configuração

### 1.2.1 Configure SWD como servidor DHCP válido.

No SWD, configure um pool de endereços DHCP 10.0.1.0/24 e o endereço de gateway 10.0.1.1. Defina o endereço IP do VLANIF 10 como 10.0.10.2/24. Configure a E0/0/1 do SWD como uma interface de acesso e adicione-o à VLAN 10 por padrão. Configurar uma rota estática para SWA no segmento de rede 10.0.1.0/24.

```
<Quidway>system-view
Enter system view, return user view with Ctrl+Z.
[Quidway]sysname SWD
[SWD]dhcp enable
[SWD]ip pool pool1
Info:It's successful to create an IP address pool.
[SWD-ip-pool-pool1]network 10.0.1.0 mask 255.255.255.0
[SWD-ip-pool-pool1]gateway-list 10.0.1.1
[SWD-ip-pool-pool1]quit
[SWD]vlan 10
[SWD-vlan10]quit
[SWD]interface vlanif 10
[SWD-Vlanif10]ip address 10.0.10.2 24
[SWD-Vlanif10]dhcp select global
[SWD-Vlanif10]quit
[SWD]interface ethernet 0/0/1
[SWD-Ethernet0/0/1]port link-type access
[SWD-Ethernet0/0/1]port default vlan 10
[SWD-Ethernet0/0/1]quit
[SWD]ip route-static 10.0.1.0 24 10.0.10.1
```

### 1.2.2 Configure SWC como o servidor DHCP inválido.

No SWC, configure um pool de endereços DHCP 192.168.1.0/24 e configure o endereço IP do VLANIF 1 como 192.168.1.1/24 e como o endereço IP do gateway.

```
<Quidway>system-view
Enter system view, return user view with Ctrl+Z.
[Quidway]sysname SWC
[SWC]dhcp enable
[SWC]ip pool illegal-pool
Info:It's successful to create an IP address pool.
[SWC-ip-pool-illegal-pool]network 192.168.1.0 mask 255.255.255.0
[SWC-ip-pool-illegal-pool]gateway-list 192.168.1.1
[SWC-ip-pool-illegal-pool]quit
[SWC]interface vlanif 1
[SWC-Vlanif1]ip address 192.168.1.1 24
[SWC-Vlanif1]dhcp select global
[SWC-Vlanif1]quit
```

### 1.2.3 Configure SWB como um DHCP Relay.

No SWB, defina o endereço IP da VLANIF 1 como 10.0.1.1/24 e ative a retransmissão DHCP na VLANIF 1. Após a conclusão das configurações, o agente de retransmissão DHCP permite que os usuários na VLAN 1 obtenham endereços IP do conjunto de endereços 10.0.1.0/24 no SWD. Configure a E0/0/1 do SWB como uma interface de acesso e adicione-o à VLAN 10 por padrão. Defina o endereço IP do VLANIF 10 como 10.0.10.1/24.

```
<Quidway>system-view
Enter system view, return user view with Ctrl+Z.
[Quidway]sysname SWB
[SWB]dhcp enable
[SWB]interface vlanif 1
[SWB-Vlanif1]ip address 10.0.1.1 24
[SWB-Vlanif1]dhcp select relay
[SWB-Vlanif1]dhcp relay server-ip 10.0.10.2
[SWB]vlan 10
[SWB-vlan10]quit
[SWB]interface ethernet 0/0/1
[SWB-Ethernet0/0/1]port link-type access
[SWB-Ethernet0/0/1]port default vlan 10
[SWB-Ethernet0/0/1]quit
[SWB]interface vlanif 10
[SWB-Vlanif10]ip address 10.0.10.1 24
[SWB-Vlanif10]quit
[SWB]
```

Teste a conectividade entre SWB e SWD.

```
[SWB]ping -a 10.0.1.1 10.0.10.2
PING 10.0.10.2: 56 data bytes, press CTRL_C to break
  Reply from 10.0.10.2: bytes=56 Sequence=1 ttl=255 time=4 ms
  Reply from 10.0.10.2: bytes=56 Sequence=2 ttl=255 time=1 ms
  Reply from 10.0.10.2: bytes=56 Sequence=3 ttl=255 time=1 ms
  Reply from 10.0.10.2: bytes=56 Sequence=4 ttl=255 time=1 ms
  Reply from 10.0.10.2: bytes=56 Sequence=5 ttl=255 time=4 ms

--- 10.0.10.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/2/4 ms
```

## 1.2.4 Testando a configuração.

Configure a E1/0/0 do RTA para obter automaticamente um endereço IP.

```
<Huawei>system-view
System View: return to User View with Ctrl+Z.
[Huawei]sysname RTA
[RTA]interface ethernet 1/0/0
[RTA-Ethernet1/0/0]ip address dhcp-alloc
```

Desligue a E0 0/1 conectando o SWA e o SWC para testar se a E1/0/0 do RTA pode obter um endereço IP correto do SWD.

```
<Quidway>system-view
Enter system view, return user view with Ctrl+Z.
[Quidway]sysname SWA
[SWA]interface ethernet 0/0/1
[SWA-Ethernet0/0/1]shutdown

[RTA]display ip interface brief
```

```
*down: administratively down
(l): loopback
(s): spoofing
Interface          IP Address          Physical Protocol    Description
Aux0                unassigned          down    down              Aux0 Inte...
.....
Ethernet1/0/0      10.0.1.253          up      up                Ethernet1...
```

A saída anterior mostra que a E1/0/0 do RTA obteve um endereço IP correto 10.0.1.253 do SWD.

Habilite a E0/0/1 do SWA e desligue a E0/0/3 para testar se a E1/0/0 do RTA pode obter um endereço IP correto do SWC.

### NOTE

You may need to restart RTA's E1/0/0 to allow RTA to re-obtain an IP address.

```
[SWA]interface ethernet 0/0/1
[SWA-Ethernet0/0/1]undo shutdown
[SWA-Ethernet0/0/1]quit
[SWA]interface ethernet 0/0/3
[SWA-Ethernet0/0/3]shutdown
[SWA-Ethernet0/0/3]

[RTA]int Ethernet 1/0/0
[RTA-Ethernet1/0/0]shutdown
[RTA-Ethernet1/0/0]undo shutdown
[RTA-Ethernet1/0/0]quit
[RTA]display ip interface brief
*down: administratively down
(l): loopback
(s): spoofing
Interface          IP Address          Physical Protocol    Description
Aux0                unassigned          down    down              Aux0 Inte...
.....
Ethernet1/0        192.168.1.254       up      up                Ethernet1...
```

A saída anterior mostra que a E1/0/0 do RTA obteve um endereço IP correto 192.168.1.254 do SWC. SWC e SWD estão configurados corretamente como servidores DHCP.

Habilite a E0/0/3 do SWA para permitir que o RTA obtenha novamente um endereço IP e mantenha on-line servidores DHCP válidos e inválidos.

```
[SWA]interface Ethernet 0/0/3
[SWA-Ethernet0/0/3]undo shutdown

[RTA-Ethernet1/0]display ip interface brief
*down: administratively down
(l): loopback
(s): spoofing
Interface          IP Address          Physical Protocol    Description
Aux0                unassigned          down    down              Aux0 Inte...
.....
Ethernet1/0        192.168.1.254       up      up                Ethernet1...
```

A saída anterior mostra que o RTA obteve um endereço IP do servidor DHCP inválido. Na maioria dos casos, o RTA pode obter endereços IP apenas do servidor DHCP inválido porque o SWC está mais próximo do RTA e envia mensagens de resposta mais rapidamente que o SWD. Situações semelhantes ocorrem em redes reais.

### 1.2.5 Configure DHCP snooping no SWA.

Habilite o DHCP e DHCP snooping no SWA. Habilite DHCP snooping na VLAN 1 e configure a E0/0/3 como a interface confiável.

```
[SWA]dhcp enable
[SWA]dhcp snooping enable
[SWA]vlan 1
[SWA-vlan1]dhcp snooping enable
[SWA-vlan1]dhcp snooping trusted interface Ethernet 0/0/3
[SWA-vlan1]display this
#
vlan 1
  dhcp snooping enable
  dhcp snooping trusted interface Ethernet0/0/3
#
```

## 1.3 Verificação da Configuração

### 1.3.1 Verifica o funcionamento do DHCP snooping.

Configure o RTA para obter novamente um endereço IP para testar se o RTA obtém um endereço IP do SWD.

```
[RTA-Ethernet1/0/0]shutdown
[RTA-Ethernet1/0/0]undo shutdown
[RTA-Ethernet1/0/0]display ip interface brief
*down: administratively down
(l): loopback
(s): spoofing
Interface          IP Address      Physical Protocol  Description
Aux0               unassigned      down    down             Aux0 Inte...
.....
Ethernet1/0/0      10.0.1.253      up       up               Ethernet1...
```

A saída anterior mostra que o RTA obteve um endereço IP 10.0.1.253 do SWD.

Desligue a e0/0/3 do SWA para desconectar o SWA do SWD para testar se o SWA obtém um endereço IP do SWC.

```
[SWA]interface ethernet 0/0/3
[SWA-Ethernet0/0/3]shutdown

[RTA-Ethernet1/0]display ip interface brief
*down: administratively down
(l): loopback
(s): spoofing
Interface          IP Address      Physical Protocol  Description
Aux0               unassigned      down    down             Aux0 Inte...
.....
```

```
Ethernet1/0/0      unassigned      up      up      Ethernet1...  
.....
```

```
[SWA-Ethernet0/0/3]undo shutdown
```

Depois que o SWA é configurado com DHCP snooping, o SWA obtém apenas endereços IP através da interface confiável E0/0/3. O SWA não obtém endereços IP de outros servidores DHCP, mesmo quando o SWD falha.

## 1.4 Configurações

### 1.4.1 SWA.

```
#  
!Software Version V100R006C00SPC500  
sysname SWA  
#  
dhcp enable  
dhcp snooping enable  
#  
#  
vlan 1  
  dhcp snooping enable  
  dhcp snooping trusted interface Ethernet0/0/3  
#
```

### 1.4.2 SWB.

```
#  
!Software Version V100R006C00SPC500  
sysname SWB  
#  
vlan batch 10  
#  
dhcp enable  
#  
#  
interface Vlanif1  
  ip address 10.0.1.1 255.255.255.0  
  dhcp select relay  
  dhcp relay server-ip 10.0.10.2  
#  
interface Vlanif10  
  ip address 10.0.10.1 255.255.255.0  
#  
interface Ethernet0/0/1  
  port link-type access  
  port default vlan 10  
#
```

### 1.4.3 SWC.

```
#
!Software Version V100R006C00SPC500
sysname SWC
#
dhcp enable
#
#
ip pool illegal-pool
#
ip pool illegal-pool
gateway-list 192.168.1.1
network 192.168.1.0 mask 255.255.255.0
#
interface Vlanif1
ip address 192.168.1.1 255.255.255.0
dhcp select global
#
```

### 1.4.4 SWD.

```
#
!Software Version V100R006C00SPC500
sysname SWD
#
dns resolve
#
vlan batch 10
#
cluster enable
ntdp enable
ntdp hop 16
ndp enable
#
dhcp enable
#
ip pool pool1
#
ip pool pool1
gateway-list 10.0.1.1
network 10.0.1.0 mask 255.255.255.0
#
interface Vlanif10
ip address 10.0.10.2 255.255.255.0
dhcp select global
#
interface Ethernet0/0/1
port link-type access
port default vlan 10
#
ip route-static 10.0.1.0 255.255.255.0 10.0.10.1
#
```

## 1.4.5 RTA.

```
#  
interface Ethernet1/0/0  
ip address dhcp-alloc  
#
```