

Contents

Introduction	1
Prerequisites	1
Example: Configuring DHCP snooping	1
Network configuration	1
Analysis	2
Applicable hardware and software versions.....	2
Restrictions and guidelines	4
Procedures	4
Configuring Device A	4
Configuring Device B	5
Configuring Device C	6
Configuring Device D	6
Verifying the configuration	7
Configuration files	7

Introduction

This document provides DHCP snooping configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of DHCP.

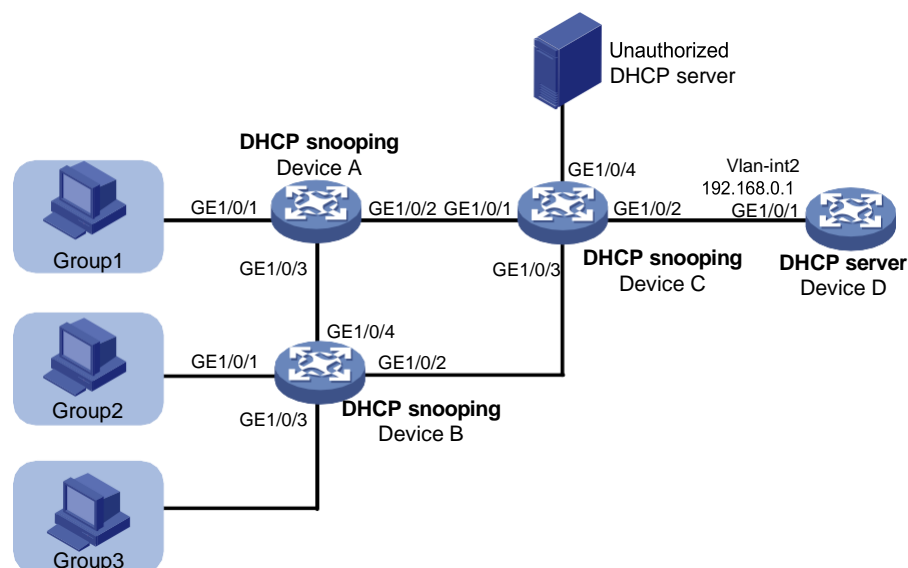
Example: Configuring DHCP snooping

Network configuration

As shown in [Figure 1](#), three groups of hosts are connected to the DHCP server through the DHCP snooping devices. Configure DHCP snooping and DHCP server to meet the following requirements:

- Hosts in each group obtain IP addresses from the address range assigned to the group. Assign address ranges to the groups as follows:
 - Address range 192.168.0.2 to 192.168.0.39 for Group 1.
 - Address range 192.168.0.40 to 192.168.0.99 for Group 2.
 - Address range 192.168.0.100 to 192.168.0.200 for Group 3.
- The hosts can obtain IP addresses only from the authorized DHCP server.
- The hosts cannot access the network through IP addresses that are manually configured.

Figure 1 Network diagram

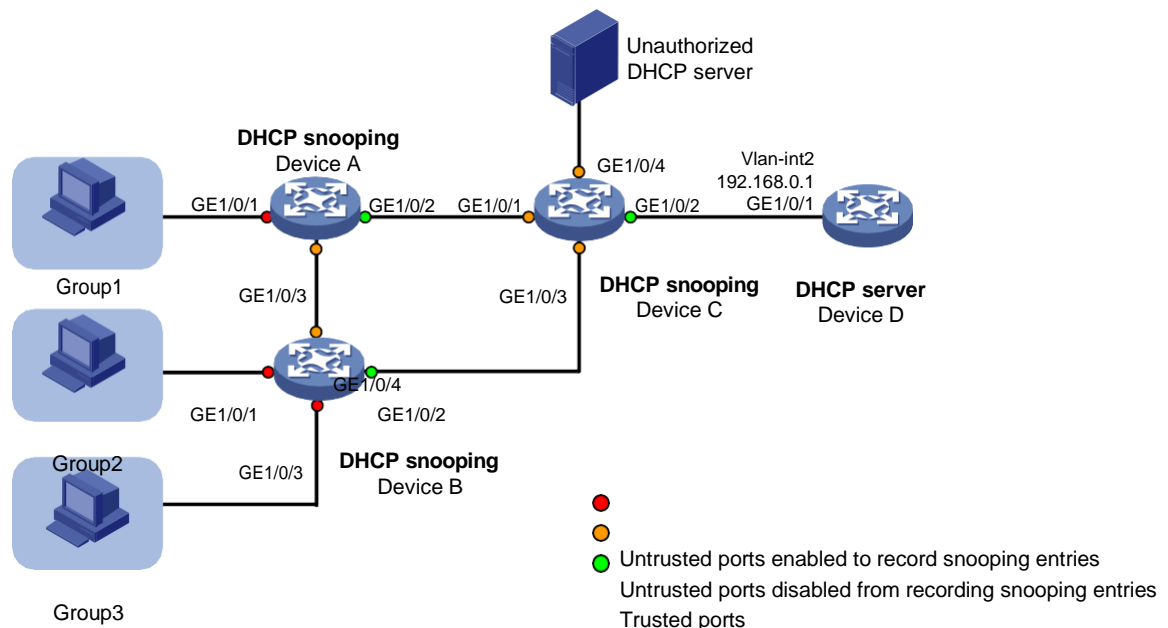


Analysis

To meet the network requirements, you must perform the following tasks:

- To make sure the hosts in each group obtain IP addresses from the address range assigned to the group, perform the following tasks:
 - Configure Option 82 on the DHCP snooping devices.
 - Create DHCP user classes for the groups and configure match rules based on Option 82 to match the groups on the DHCP server.
- To make sure the hosts obtain addresses only from the authorized DHCP server, configure ports facing the server as trusted and other ports as untrusted, as shown in [Figure 2](#).
- To prevent illegal users from using manually configured IP addresses to access the network, perform the following tasks:
 - Enable ARP detection in the VLANs where the groups reside to check user validity based on DHCP snooping entries.
 - Enable recording of client information in DHCP snooping entries. To save system resources, you can enable only untrusted ports directly connected to hosts to record DHCP snooping entries, as shown in [Figure 2](#).

Figure 2 Trusted and untrusted ports



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

SC 3570 switch series	Release 11xx
SC 5525 switch series	Release 63xx, Release 65xx, and Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, and Release 6615Pxx, Release 6628Pxx
SC 3170 switch series	Release 11xx
SC 3130 switch series	Release 63xx

Restrictions and guidelines

To ensure correct DHCP address allocation by using Option 82, you must perform Option 82 configuration on the DHCP server and the DHCP snooping devices.

Procedures

Configuring Device A

Enable DHCP snooping.

```
<DeviceA> system-view
[DeviceA] dhcp snooping enable
```

Enable recording of client information in DHCP snooping entries on interface GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] dhcp snooping binding record
```

Enable DHCP snooping to support Option 82 on GigabitEthernet 1/0/1. Configure the padding content for the Circuit ID sub-option as **group1**.

```
[DeviceA-GigabitEthernet1/0/1] dhcp snooping information enable
[DeviceA-GigabitEthernet1/0/1] dhcp snooping information circuit-id string group1
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trusted port.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] dhcp snooping trust
[DeviceA-GigabitEthernet1/0/2] quit
```

Enable ARP attack detection for user validity check.

```
[DeviceA] vlan 1
[DeviceA-vlan1] arp detection enable
[DeviceA-vlan1] quit
```

Configure GigabitEthernet 1/0/2 as an ARP trusted port. By default, an interface is an ARP untrusted port.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] arp detection trust
[DeviceA-GigabitEthernet1/0/2] quit
```

Configuring Device B

Enable DHCP snooping.

```
<DeviceB> system-view
[DeviceB] dhcp snooping enable
```

Enable recording of client information in DHCP snooping entries on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] dhcp snooping binding record
```

Enable DHCP snooping to support Option 82 on interface GigabitEthernet 1/0/1. Configure the padding content for the Circuit ID sub-option as **group2**.

```
[DeviceB-GigabitEthernet1/0/1] dhcp snooping information enable
[DeviceB-GigabitEthernet1/0/1] dhcp snooping information circuit-id string group2
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure gigabitethernet 1/0/2 as a trusted port.

```
[DeviceB] interface GigabitEthernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] dhcp snooping trust
[DeviceB-GigabitEthernet1/0/2] quit
```

Enable recording of client information in DHCP snooping entries on GigabitEthernet 1/0/3.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] dhcp snooping binding record
```

Enable DHCP snooping to support Option 82 on GigabitEthernet 1/0/3. Configure the padding content for the Circuit ID sub-option as **group3**.

```
[DeviceB-GigabitEthernet1/0/3] dhcp snooping information enable
[DeviceB-GigabitEthernet1/0/3] dhcp snooping information circuit-id string group3
[DeviceB-GigabitEthernet1/0/3] quit
```

Enable ARP attack detection for user validity check.

```
[DeviceB] vlan 1
[DeviceB-vlan1] arp detection enable
[DeviceB-vlan1] quit
```

Configure GigabitEthernet 1/0/2 as an ARP trusted port. By default, an interface is an ARP untrusted port.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] arp detection trust
[DeviceB-GigabitEthernet1/0/2] quit
```

Configuring Device C

Enable DHCP snooping.

```
<DeviceC> system-view
[DeviceC] dhcp snooping enable
```

Configure GigabitEthernet 1/0/2 as a trusted port.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] dhcp snooping trust
[DeviceC-GigabitEthernet1/0/2] quit
```

Configuring Device D

Assign GigabitEthernet 1/0/1 to VLAN 2.

```
<DeviceD> system-view
[DeviceD] vlan 2
[DeviceD-vlan2] port gigabitethernet 1/0/1
[DeviceD-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[DeviceD] interface vlan-interface 2
[DeviceD-Vlan-interface2] ip address 192.168.0.1 24
[DeviceD-Vlan-interface2] quit
```

Enable DHCP.

```
[DeviceD] dhcp enable
```

Enable DHCP server on VLAN-interface 2.

```
[DeviceD] interface vlan-interface 2
[DeviceD-Vlan-interface2] dhcp select server
[DeviceD-Vlan-interface2] quit
```

Create DHCP user class **group1** for hosts in Group 1. Configure a match rule to match DHCP requests in which the third to eighth bytes of Option 82 is 0x67726F757031. The string 0x67726F757031 indicates that the content of the Circuit ID sub-option is **group1**.

```
[DeviceD] dhcp class group1
[DeviceD-dhcp-class-group1] if-match option 82 hex 67726F757031 offset 2 length 6
[DeviceD-dhcp-class-group1] quit
```

Create DHCP user class **group2** for hosts in Group 2. Configure a match rule to match DHCP requests in which the third to eighth bytes of Option 82 is 0x67726F757032. The string 0x67726F757032 indicates that the content of the Circuit ID sub-option is **group2**.

```
[DeviceD] dhcp class group2
[DeviceD-dhcp-class-group2] if-match option 82 hex 67726F757032 offset 2 length 6
[DeviceD-dhcp-class-group2] quit

# Create DHCP user class group3 for hosts in Group 3. Configure a match rule to match DHCP
requests in which the third to eighth bytes of Option 82 is 0x67726F757033. The string
0x67726F757033 indicates that the content of the Circuit ID sub-option is group3.

[DeviceD] dhcp class group3
[DeviceD-dhcp-class-group3] if-match option 82 hex 67726F757033 offset 2 length 6
[DeviceD-dhcp-class-group3] quit

# Create a DHCP address pool.

[DeviceD] dhcp server ip-pool 1

# Specify the subnet for dynamic address allocation.

[DeviceD-dhcp-pool-1] network 192.168.0.0 mask 255.255.255.0

# Specify address range 192.168.0.2 to 192.168.0.39 for DHCP user class group1.

[DeviceD-dhcp-pool-1] class group1 range 192.168.0.2 192.168.0.39

# Specify address range 192.168.0.40 to 192.168.0.99 for DHCP user class group2.

[DeviceD-dhcp-pool-1] class group2 range 192.168.0.40 192.168.0.99

# Specify address range 192.168.0.100 to 192.168.0.200 for DHCP user class group3.

[DeviceD-dhcp-pool-1] class group3 range 192.168.0.100 192.168.0.200

# Apply the DHCP address pool to VLAN-interface 2.

[DeviceD] interface vlan-interface 2
[DeviceD-Vlan-interface2] dhcp server apply ip-pool 1
[DeviceD-Vlan-interface2] quit
```

Verifying the configuration

Verify that the hosts in each group can obtain IP addresses from the address range assigned to the group. This example uses a host in Group 2 to verify the configuration.

```
C:\Documents and Settings\Administrator>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter bb:
```

```
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.0.44
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Manually assign IP address 192.168.0.66 to a host in Group 2, and verify that it cannot access the external network. (Details not shown.)

Configuration files



IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

- **Device A:**

```
#
    dhcp snooping enable
#
vlan 1
    arp detection enable
#
interface GigabitEthernet1/0/1
    dhcp snooping binding record
    dhcp snooping information enable
    dhcp snooping information circuit-id string group1
#
interface GigabitEthernet1/0/2
    arp detection trust
    dhcp snooping trust
#
```

- **Device B:**

```
#
    dhcp snooping enable
#
vlan 1
    arp detection enable
#
interface GigabitEthernet1/0/1
    dhcp snooping binding record
    dhcp snooping information enable
    dhcp snooping information circuit-id string group2
#
interface GigabitEthernet1/0/2
    arp detection trust
    dhcp snooping trust
#
interface GigabitEthernet1/0/3
    dhcp snooping binding record
    dhcp snooping information enable
    dhcp snooping information circuit-id string group3
#
```

- **Device C:**

```
#
    dhcp snooping enable
#
interface GigabitEthernet1/0/2
    dhcp snooping trust
#
```

- **Device D:**

```
#
    dhcp enable
```



```

#
vlan 2
#
dhcp class group1
    if-match option 82 hex 67726f757031 offset 2 length 6
#
dhcp class group2
    if-match option 82 hex 67726f757032 offset 2 length 6
#
dhcp class group3
    if-match option 82 hex 67726f757033 offset 2 length 6
#
dhcp server ip-pool 1
    network 192.168.0.0 mask 255.255.255.0
    class group1 range 192.168.0.2 192.168.0.39
    class group2 range 192.168.0.40 192.168.0.99
    class group3 range 192.168.0.100 192.168.0.200
#
interface Vlan-interface2
    ip address 192.168.0.1 255.255.255.0
    dhcp server apply ip-pool 1
#

```