Chapter 23: **DHCP Snooping**

Alpha Bridge Technologies

Contents

Chapter 23 DHCP Snooping

23.1 DHCP Snooping Overview

For the sake of security, the IP addresses used by online DHCP clients need to be tracked forthe administrator to verify the corresponding relationship between the IP addresses the DHCPclients obtained from DHCP servers and the MAC addresses of the DHCP clients. Switches can track DHCP client IP addresses through the DHCP snooping function, which monitors DHCP broadcast packets.

DHCP snooping monitors the following two types of packets to retrieve the IP addresses the DHCP clients obtain from DHCP servers and the MAC addresses of the DHCP clients:

DHCP-ACK packet

DHCP-REQUEST packet

When an unauthorized DHCP server exists in the network, a DHCP client may obtains an illegal IP address. To ensure that the DHCP clients obtain IP addresses from valid DHCP servers, you can specify a port to be a trust port or an untrusted port by the DHCP snooping function:

Trusted ports can be used to connect DHCP servers or ports of other Switches. Untrusted ports can be used to connect DHCP clients or networks.

Untrusted ports drop the DHCP-ACK and DHCP-OFFER packets received from DHCP servers.Trusted ports forward any received DHCP packets to ensure that DHCP clients can obtain IP addresses from valid DHCP servers.

Trusted vlan: untrusted port will not drop the DHCP-ACK and DHCP-Offer.

23.2 Configure DHCP Snooping

23.2.1 DHCP Snooping Configuration List

Configuration Task	Description	Detailed Configuration
Enable DHCP Snooping	Required	23.2.2
Configure DHCP Snooping Trust port	Required	23.2.3
Configure Max Clients Number	Optional	23.2.4
Configure Link-Down Operation	Optional	23.2.5
Configure IP-Source-Guard	Optional	23.2.6
DHCP Snooping Display and Maintenance	Optional	23.2.7

23.3.2 Enable DHCP Snooping

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable DHCP Snooping	**dhcp-snooping**	
Disable DHCP Snooping	**undo dhcp-snooping**	Disabled by default

23.2.3 Configure DHCP Snooping Trust port

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable interface mode	**interface ethernet** *interface-num*	
Configer trust port	**dhcp-snooping trust**	
Delete trust port	**undo dhcp-snooping trust**	

23.2.4 Configure Max Clients Number

If the attacker exists, it will disguise as multiple users to ask DHCP Server for address to use up the Server allocable address. As a consequence, Server has no address to allocate to the user who needs the IP address. For this problem, network administrator can take the followingmeasures:

Restrict the DHCP-Client number connected to Switch port. In this case, only the clientsconnected to the same port with the attacker will suffer the attack.

Restrict the DHCP-Client number in specified VLAN. In this case, only the clients in the sameVLAN with the attacker will suffer the attack.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Enable interface mode	**interface ethernet interface-num**	
Configure max DHCP-Client number connected to Switch port	**dhcp-snooping max-clients num**	
Enter vlan configuration mode	**vlan vlan-id**	
Configure max DHCP-Client number in specified VLAN	**dhcp-snooping max-clients num**	

23.2.5 Configure Link-Down Operation

When the link is down, you can perform the following actions on the dynamic entries whichDhcp-snooping has learned:

enable fast-remove to delete Dhcp-snooping dynamic entries immediately when the port isdown.

disable fast-remove to normally age the dynamic entries according to the tenancy term insteadof deleting the Dhcp-snooping dynamic entries immediately when the port is down.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	

Configure link-down operation of the	**dhcp-snooping port-down-action**	
port	**fast-remove**	
Delete link-down operation of the port	**undo dhcp-snooping port-down-action** **fast-remove**	

23.2.6 Configure IP-Source-Guard

IP Source Guard provides source IP address filtering on a Layer 2 port to prevent a maliciousghost from impersonating a legitimate host by assuming the legitimate host's IP address. The feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts on untrusted Layer 2 access ports. When using IP-Source-Guard, pay attention:

DHCP-Snooping has been

enabledUse this function

in Trust port

After enabling IP-Source-Guard, all traffic with that IP source address is permitted from that trusted client. Traffic from other hosts is denied. This filtering limits a host's ability to attack thenetwork by claiming a neighbor host's IP address. The filtering info can be source MAC, sourceIP and source port number.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	-
Configure IP-source-guard bind table	**ip-source-guardbind** { **ip** *ip-address* | **mac** *mac-address* | **interface ethernet** *interface-num* }	-
Enter interface configuration mode	**interface ethernet** *interface-num*	-
Enable IP-Source-Guard on Trust port	**ip-source-guard**	By default, ip-source-guard
		on port is disabled.

23.2.7 DHCP Snooping Display and Maintenance

Operation	Command	Remarks
Display DHCP-Snooping clients	**display dhcp-snooping clients**	
Display DHCP-Snooping status in interface	**display dhcp-snooping interface** [ethernet *interface-num*]	
Display DHCP-Snooping status in VLAN	**display dhcp-snooping vlan**	
Display IP-Source-Guard status in interface	**display ip-source-guard**	
Display source IP binding table of IP-Source-Guard	**display ip-source-guard bind** [ip *ip-address*]	