Technical Guide

DHCP Snooping

Feature Overview and Configuration Guide

Introduction

This guide provides information about DHCP snooping for IPv4, and how to configure it on AlliedWare Plus™ switches.

Products and software version that apply to this guide

This guide applies to AlliedWare Plus products that support DHCP snooping, running version **5.4.4** or later.

However, support and implementation of DHCP snooping varies between products. To see whether a product supports a particular feature or command, see the following documents:

- The product's Datasheet
- The product's Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

Feature support may change in later software versions. For the latest information, see the above documents.

Per-VLAN mode became available for some switches in 5.4.9-2.1 and for the remaining switches in 5.5.2-0.1.

Content

DHCP Snooping

DHCP snooping provides an extra layer of security at the network edge via dynamic IP source filtering. DHCP snooping looks into DHCP packets to build up a database of which IP addresses have been allocated to clients downstream of each port. Using this database, it can determine if the source IP addresses of packets arriving from clients are valid, i.e. the IP addresses that were allocated to the clients. Additionally, DHCP snooping can prevent rogue DHCP activity in the network by filtering out DHCP packets that are arriving on the wrong ports, or with incorrect contents.

Dynamic Host Configuration Protocol (DHCP) dynamically assigns IP addresses to client devices. The use of dynamically assigned addresses requires traceability, so that a service provider can determine which clients own a particular IP address at a certain time.

With DHCP snooping, IP sources are dynamically verified, and filtered accordingly. IP packets that are not sourced from recognized IP addresses can be filtered out. This ensures the required traceability because the packets that are allowed into the network are using their officially allocated IP addresses.

With DHCP snooping, an administrator can control which packets enter the network by:

- permitting port access to DHCP issued IP addresses or known statically assigned addresses only
- dictating the number of IP clients on any given port
- passing location information about an IP client to the DHCP server
- permitting ARP packets only from clients using the correct IP addresses

Ports on the switch are classified as either trusted or untrusted:

- Trusted ports receive only messages from within your network, so traffic from DHCP servers is allowed to be received on these ports
- Untrusted ports receive messages from client devices. So, traffic that comes from DHCP servers is not allowed to be received on these ports.

DHCP snooping blocks unauthorized IP traffic from untrusted ports, and prevents it from entering the trusted network. It validates DHCP client packets from untrusted ports and forwards them to trusted ports in the VLAN.

The DHCP snooping service is disabled by default. You can enable this service in one of two modes:

- globally. This creates a global ACL and means that **all** DHCP traffic is forwarded to the CPU, no matter what VLAN it belongs to.
    - or, per-VLAN. This option minimizes the amount of DHCP traffic forwarded to the CPU. However, it creates 2 ACL entries for each VLAN that you enable DHCP snooping on. This means it is most suitable if you have a small number of VLANs.

DHCP Snooping database

When you enable DHCP snooping, the switch intercepts all DHCP packets it receives, and sends them to the Central Processing Unit (CPU), where they are verified, and relevant information is extracted from them. When you enable DHCP snooping on a VLAN, the switch automatically creates an ACL to send DHCP packets to the CPU. The DHCP snooping database stores and maintains the information extracted by the CPU. The database contains:

- entries that are automatically created by the DHCP snooping process. Current IP address leases dynamically allocated by a DHCP server, these entries record the port to which the clients are connected, and the IP addresses they have been allocated.
- entries added from the command line—typically used to add a DHCP snooping entry for a client that has a preconfigured IP address on an untrusted port.

If such a database file exists, it is loaded when the switch starts up with DHCP snooping enabled, or when DHCP snooping is subsequently enabled.

Lease entries

Each entry in the database corresponds to a DHCP IP address lease. For dynamic entries added automatically by DHCP snooping, each entry contains the:

- IP address that was allocated to that client
- MAC address of the client device
- time until expiry
- VLAN to which the client is attached
- port to which the client is attached
- IP address of the DHCP server

For static entries added from the command line, each entry contains a subset of information, which includes the:

- IP address allocated to the client
- MAC address of the client device (optional)
- VLAN to which the client is attached
- port to which the client is attached

Each entry also shows its source: Dynamic (i.e. automatically created) or Static (i.e. added from the CLI).

The maximum number of lease entries that can be stored in the DHCP snooping database for each port can be configured—the default is 1.

Expired entries

For dynamic entries, the switch receives expiry information with the client lease information in DHCP packets. Entries expire when the time left to expiry is 0 seconds. Expired entries are automatically deleted from the database. Static entries have no expiry information, and are not checked.

Database backup

Periodically, the dynamic entries in the DHCP snooping database are saved to a hidden file (**.dhcp.dsn.gz**) in Non-Volatile Storage (NVS). The device can also be configured to save them to Flash memory, SD card, or to a USB storage device.

All dynamic entries in the database are written to the backup file. Whenever DHCP snooping is enabled, the DHCP snooping database is repopulated from the backup file and any static entries in the start-up configuration file. Any entries present in the backup file that have expired are ignored.

DHCP Relay Agent Option 82

If the switch is at the edge of the network, it can be configured to insert DHCP Relay Agent Option 82 information into client-originated BOOTP/DHCP packets that it is forwarding to a DHCP server. The switch also removes DHCP Relay Agent Option 82 information from BOOTP reply packets destined for an untrusted port if the DHCP client hardware is directly attached to a port on the switch.

DHCP servers that are configured to recognize DHCP Relay Agent Option 82 may use the information to implement IP address or other parameter assignment policies, based on the network location of the client device.

Support on your switch

The switch inserts DHCP Relay Agent Option 82 (agent option) information into DHCP packets received through untrusted ports, and removes it from DHCP packets transmitted through untrusted ports. This is enabled by default, and can be disabled if required. The switch inserts the following DHCP Relay Agent Option 82 information:

- **Remote ID**: this identifies the host that is doing the inserting of the Option 82 information. By default, this is the MAC address of the current switch (sub-option1).
- **Circuit ID**: this specifies the switch port and VLAN ID that the client-originated DHCP packet was received on (sub-option2). By default, this is the VLAN ID and the Ifindex (interface number).
- **Subscriber ID** (optional): this is a string of up to 50 characters that differentiates or groups client ports on the switch (sub-option 6).

You can specify values for the Remote ID and Circuit ID sub-options of the DHCP Relay Agent Option 82 field. The Remote ID can be specified as an alphanumeric (ASCII) string, 1 to 63 characters in length. The Circuit ID can be specified as the VLAN ID and port number. Subscriber IDs can be configured for ports, and if they have been configured, they are inserted in DHCP packets as part of the DHCP Relay Agent Option 82 information.

Regardless of whether DHCP Relay Agent Option 82 is enabled for DHCP snooping, if the switch receives a BOOTP/DHCP request packet on a trusted port, and the packet contains DHCP Relay Agent Option 82 information, it does not update the DHCP Relay Agent Option 82 information for the receiver port. By default, if it receives a DHCP request packet containing DHCP Relay Agent Option 82 information on an untrusted port, it drops the packet. However, if the switch is connected via untrusted ports to edge switches that insert DHCP Relay Agent Option 82 information into DHCP packets, you may need to allow these DHCP packets through the untrusted ports—the switch can be configured to forward these packets.

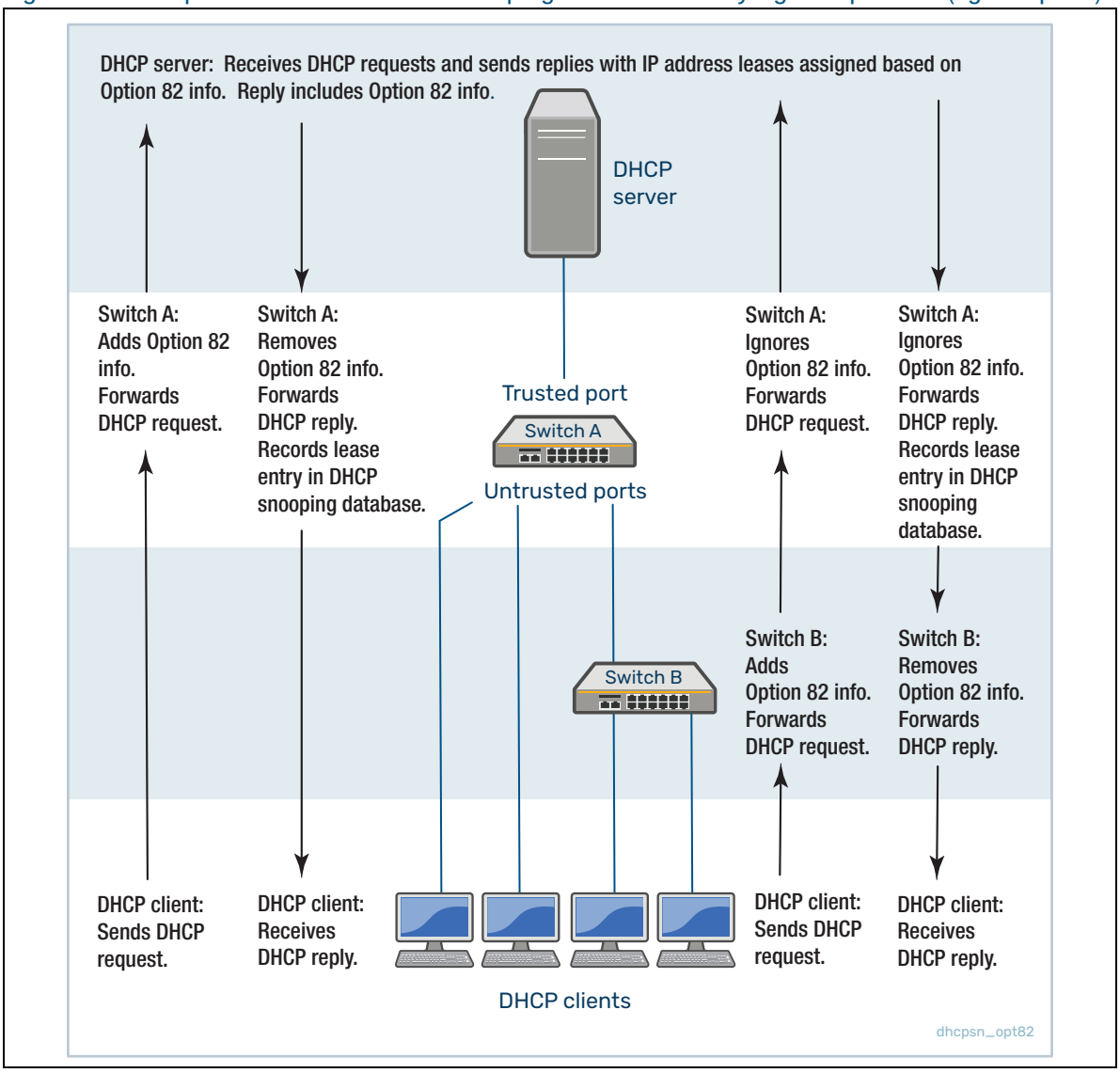
Note that the DHCP Relay Agent Option 82 agent information inserted by the DHCP snooping differs from the information added by DHCP Relay. If you configure both DHCP Snooping and DHCP Relay on the switch, you cannot use DHCP Relay to insert Option 82 information. You must use DHCP snooping to insert it instead.

Operation

Figure 1 shows DHCP packet flow between DHCP clients and server, where:

- Switch A has DHCP snooping enabled. The DHCP server is connected to a trusted port on Switch A; DHCP clients and Switch B are connected to untrusted ports.
- Switch A is configured to add and remove DHCP Relay Agent Option 82 information.
- Switch A is configured to forward DHCP packets that already contain DHCP Relay Agent Option 82 information without changing it.
- Switch B is Layer 2 switching traffic from downstream DHCP clients, and adds and removes DHCP Relay Agent Option 82 information.

Figure 1: DHCP packet flow with DHCP snooping and DHCP Relay Agent Option 82 (agent option)



For more information about DHCP Relay Agent Option 82, see RFC 3046, DHCP Relay Agent Information Option.

Traffic filtering with DHCP Snooping

DHCP filtering prevents IP addresses from being falsified or ‘spoofed’. This guarantees that users cannot avoid detection by spoofing IP addresses that are not actually allocated to them. With DHCP filtering, the switch permits packets to enter over a specific port if their source IP address is currently allocated to a client connected to that port.

Support on your switch

You can create Access Control Lists (ACLs) based on DHCP snooping to filter IP packets. For instance, IP traffic on untrusted ports can be limited to packets matching valid DHCP lease information stored in the DHCP snooping database.

Note that ACLs for DHCP filtering are additional to the ACL or ACLs that the switch creates automatically when you enable DHCP snooping on a VLAN.

The DHCP snooping feature is enabled or disabled per VLAN, and several of the related configuration settings are applied per port. If multiple VLANs on the same port have DHCP snooping enabled, all the VLANs will be subject to the same per-port settings.

ARP Security

ARP security prevents ARP spoofing. ARP spoofing occurs when devices send fake, or 'spoofed', ARP messages to an Ethernet LAN. This makes it possible for an unauthorized host to claim to be an authorized host. The unauthorized host can then intercept traffic intended for the authorized host, and can access the wider network.

Spoofed ARP messages contain the IP address of an authorized host, with a MAC address which does not match the real MAC address of the host. When ARP security is enabled for DHCP snooping, the switch checks ARP packets sourced from untrusted ports against the entries in the DHCP snooping binding database. If it finds a matching entry, it forwards the ARP packet as normal. If it does not find a matching entry, it drops the ARP packet. This ensures that only trusted clients (with a recognized IP address and MAC address combination) can generate ARP packets into the network. ARP security is not applied to packets received on trusted ports.

ARP security is disabled by default, and can be enabled on VLANs to ensure that on untrusted ports, only trusted clients (with a recognized IP address and MAC address) can generate ARP packets into the network. ARP security is applied to both dynamic and static DHCP snooping entries. For static DHCP entries without a MAC address defined, ARP security compares only the IP address details.

MAC address verification

When MAC address verification is enabled, the switch forwards DHCP packets received on untrusted ports only if the source MAC address and client hardware address fields in the packet match. MAC address verification is enabled by default.

DHCP Snooping violations

Packets violating DHCP snooping or ARP security checks (if these are enabled) are automatically dropped. The switch can also be configured to send SNMP notifications (atDhcpsnTrap and atArpsecTrap), to generate log messages, or to shut down the link on which the packet was received.

If the switch is configured to send notifications for DHCP snooping or ARP security violations, the rate is limited to one notification per second. If there are any further violations within a second, no notifications are sent for them. After one second, the switch only sends further notifications if the source MAC address and/or the violation reason are different from previous notifications. (If log messages are also generated for ARP security and DHCP snooping violations, you can see a record of all violations in the log, even if notifications were not sent for all of them.)

Operation

Table 1 on page 9 shows the filtering that is applied by DHCP snooping on a switch with the following DHCP filtering configuration for untrusted ports:

- DHCP snooping is enabled on all VLANs.
- ARP security is enabled on all VLANs
- MAC address verification is enabled on the switch (enabled by default), and all DHCP clients are directly connected to the switch.
- Access Control Lists allow IP packets that match the source IP address and MAC address of a valid lease entry in the DHCP snooping database, and deny other IP packets.
- DHCP requests containing DHCP Relay Agent Option 82 info are not allowed (this is the default setting).
- Log messages and SNMP notifications are enabled for DHCP snooping and ARP security violations.

Table 1: DHCP filtering on the switch

WHEN THE SWITCH ...	AND ...	THEN THE SWITCH ...
DHCP packets		
Receives a DHCP BOOTP packet on a trusted port		Forwards the DHCP packet.
	The packet contains a valid IP address lease for a client, and the maximum number of leases for the client port has not been reached.	Adds or updates a lease entry in the DHCP snooping database.
	The maximum number of leases for the client port has been reached.	Drops the DHCP packet, generates a log message for the violation, generates an SNMP notification (trap), and does not add a lease entry to the database.
A lease entry in the DHCP snooping database expires		Removes the expired entry from the database.
Receives a DHCP BOOTP request packet on an untrusted port	The source MAC address and client hardware address do not match.	Drops the packet, generates a log message for the violation, and sends an SNMP notification (trap).
Receives a DHCP BOOTP request packet on an untrusted port	The packet contains DHCP Relay Agent Option 82 info.	Drops the DHCP packet, generates a log message for the violation, and sends an SNMP notification (trap).
Receives a DHCP BOOTP reply packet on an untrusted port		Drops the DHCP packet, generates a log message for the violation, and sends an SNMP notification (trap).
IP packets		
Receives an IP packet on a trusted port		Forwards the IP packet.
Receives an IP packet on an untrusted port	Its source MAC address, IP address, and receiving port match a valid lease entry in the DHCP snooping database.	Forwards the IP packet.
Receives an IP packet on an untrusted port	Its source MAC address, IP address, and receiving port do not match a valid lease entry in the DHCP snooping database.	Drops the packet. Does not generate a log message or an SNMP notification.
ARP packets		
Receives an ARP request on a trusted port		Forwards the ARP packet.
Receives an ARP request on an untrusted port	Its source MAC address, IP address, and receiving port match a valid entry in the DHCP snooping database	Forwards the ARP packet.
Receives an ARP request on an untrusted port	Its source MAC address, IP address, and receiving port do not match an entry in the DHCP snooping database	Drops the packet, generates a log message for the violation, and sends an SNMP notification (trap).

ARP security on a per-port basis

From version 5.4.9-1.1, you can use the **arp security drop link-local-arps** command to allow ARP security to ignore link-local ARP probes on a per-port basis. This means that IPv4 link-local ARPs will be dropped without causing an ARP security violation when received.

Hosts that implement RFC 3927 may automatically assign themselves link-local IPv4 addresses in the subnet 169.254.0.0/16, if they are configured to learn their IP addresses via DHCP but are unable to contact a DHCP server. In an attempt to avoid IP address collision with other devices on the local network, the host will broadcast ARP probes for its randomly selected link-local IP address.

By default, ARP security will treat these ARP probes as violations and carry out the configured violation action on the port they are received on. If the violation action is configured as link-down, this will result in the host being disconnected from the network which will interrupt any DHCP IP address discovery that was in progress.

The **arp security drop link-local-arps** command allows you to configure ARP Security to drop these ARP probes, and any other ARPs that contain link-local IP addresses, without raising a violation on the affected port.

You can use the **show arp security statistics detail** command to see the status of ARPs dropped.

Interactions with Other Features

DHCP snooping interacts with other switch features as follows:

- **Ports in trunk mode**

  The DHCP snooping feature is enabled or disabled per VLAN, and several of the related configuration settings are applied to ports. If there are multiple DHCP-snooping VLANs on a port, all the VLANs will be subject to the same per-port settings.

- **Authentication**

  DHCP snooping cannot be enabled on a switch that is configured for web authentication, roaming authentication, or guest VLAN authentication, or vice versa. This means the Web Authentication virtual DHCP server and DHCP snooping cannot be enabled at the same time.

- **Stacking**

  If DHCP snooping is enabled in a stack, the DHCP snooping database and its backup file are automatically synchronized across all stack members, so that a new stack master can reinstate this database.

- **Link aggregations**

  DHCP snooping can operate over switch ports, and over static and dynamic (LACP) link aggregations (channel groups). If a switch port is added to an aggregation, DHCP snooping configuration is applied to the aggregation; configuration of the original switch port is not preserved. If the switch port is then removed from the aggregation, it returns to default DHCP snooping settings.

- **AMF guestnodes**

  The Allied Telesis Management Framework™ (AMF) can use DHCP snooping to dynamically detect AMF guestnodes. AMF guestnodes are devices on your network that either do not run the AlliedWare plus operating system or run a version that does not support AMF. Essentially any device that has an IPV4 or IPV6 address can become an AMF guest.

  For more information see the AMF Guestnode chapter in the AMF Feature Overview and Configuration Guide.

- **Private VLANs**

  DHCP snooping and private VLANs can be used together, but:

  - DHCP snooping must be enabled on all private VLANs
  - ARP security is not supported
  - the DHCP snooping trusted port must match the promiscuous port.

- **VLAN Stacking (also called VLAN double-tagging and Q-in-Q)**

  On the SBx8100 Series, version 5.5.1-1.1 and later support VLAN Stacking with DHCP snooping. In the 802.1Q header, the switch sets these fields:

  - Drop Eligible Indicator (DEI): 0
  - Priority tag (PCP) of the outer VLAN: 5
  - Priority tag (PCP) of the inner VLAN: the value the packet is received with

Configuration

This section provides general configuration procedures for DHCP snooping.

Configuring DHCP Snooping - basic configuration

A minimal DHCP snooping configuration involves enabling the DHCP snooping service and then enabling DHCP snooping on the required VLANs. Use the following commands.

Step 1: **Enable the DHCP snooping service**

```
awplus#configure terminal
awplus(config)#service dhcp-snooping
```

Step 2: **Enable DHCP snooping on the required VLANs**

```
awplus(config)#interface <vid-list>
awplus(config-if)#ip dhcp snooping
```

If you have an external DHCP server, you need to also configure a trusted port. You can also turn on additional DHCP snooping features to increase security, and change various settings to be different than their defaults. For information about these optional settings, see the next section.

Configuring DHCP Snooping - advanced configuration

This section describes various DHCP snooping options that you may need or want to use, depending on your network.

Note that if a port in trunk mode has multiple VLANs attached, then the DHCP snooping configuration settings for the port apply to all the VLANs.

Configure DHCP snooping in per-VLAN mode

This mode minimizes the amount of DHCP traffic forwarded to the CPU. However, it creates 2 ACL entries for each VLAN that DHCP snooping is enabled on, so it is most suitable if you have a small number of VLANs. Use the **show platform classifier statistics utilization brief** command to see the number of ACLs available for your switch.

1. Enter Global Configuration mode.

   ```
   awplus# configure terminal
   ```

2. Enable DHCP snooping on the switch, in per-VLAN mode.

   ```
   awplus(config)# service dhcp-snooping per-vlan
   ```

3. Enter Interface Configuration mode for the VLANs to enable DHCP snooping on.

   ```
   awplus(config)# interface <vid-list>
   ```

4. Enable DHCP snooping on these VLANs.

   ```
   awplus(config-if)# ip dhcp snooping
   ```

5. Return to Global Configuration mode.

   ```
   awplus(config-if)# exit
   ```

6. Optionally, disable L2 flooding of DHCP packets on the other VLANs.

```
awplus(config)# interface <non-snooping-vid-list>
awplus(config-if)# ip dhcp snooping disable-l2-flooding
```

You need to do this if you enable snooping on a subset of your VLANs and you are using Q-in-Q (VLAN stacking or VLAN double-tagging). Otherwise, the switch may forward two copies of some DHCP packets on the non-snooping VLANs, with one copy being single-tagged instead of double-tagged.

7. Return to Global Configuration mode.

```
awplus(config-if)# exit
```

Configure trusted ports

If you are using an external DHCP server(s), the port(s) connected to the DHCP server(s) must be configured as trusted ports. If you are using the DHCP server on your switch, you do not need trusted ports.

1. Enter Interface Configuration mode for ports connected to the trusted network.

```
awplus(config-if)# interface <port-list>
```

2. Set these ports to be trusted ports.

```
awplus(config-if)# ip dhcp snooping trust
```

3. Return to Global Configuration mode.

```
awplus(config-if)# exit
```

4. If you want to allow more than one DHCP lease for any ports, enter Interface Configuration mode for the required ports.

```
awplus(config)# interface <port-list>
```

The default of 1 is likely to be suitable for edge ports; on an aggregation switch, you may need to increase the maximum number of leases for ports connected to other switches and/or for multiple VLANs. Note that you cannot change this setting once DHCP snooping ACLs are attached to these interfaces.

5. Change the maximum number of leases for these ports, if required.

```
awplus(config-if)# ip dhcp snooping max-bindings <0-520>
```

6. Return to Global Configuration mode.

```
awplus(config-if)# exit
```

Configure DHCP filtering

1. Create a hardware access list, and enter Hardware Access List Configuration mode to configure it. See the **access-list hardware (*name*)** command.

```
awplus(config)# access-list hardware <name>
```

Note that this ACL is additional to the ACLs that the switch creates automatically when you enable DHCP snooping on a VLAN.

2. EITHER, configure the hardware access list to permit traffic with **source IP address** matching valid entries in the DHCP snooping database, and to deny other traffic. (The last filter applied to the ports by any access list must be the filter that denies all other traffic.)

```
awplus(config-ip-hw-acl)# [<seqnum>] permit ip dhcpsnooping any
awplus(config-ip-hw-acl)# [<seqnum>] deny ip any any
```

OR, configure the hardware access list to permit traffic with **source MAC address** matching valid entries in the DHCP snooping database, and to deny other traffic. (The last filter applied to the ports by any access list must be the filter that denies all other traffic.)

```
awplus(config-ip-hw-acl)# [<seqnum>] permit mac dhcpsnooping any
awplus(config-ip-hw-acl)# [<seqnum>] deny mac any any
```

See the **access-list hardware IP protocol filter** command.

3. Return to Global Configuration mode.

```
awplus(config-ip-hw-acl)# exit
```

4. Enter Interface Configuration mode for the ports to add the DHCP snooping access list to. Typically this would be all untrusted ports.

```
awplus(config)# interface <port-list>
```

5. Add the hardware-based access list(s) to these ports. The ***name*** in this command is the name of the access list specified at the beginning of this subsection.

```
awplus(config-if)# access-group <name>
```

6. Return to Global Configuration mode.

```
awplus(config-if)# exit
```

Configure ARP security

1. Enter Interface Configuration mode for the VLANs to enable ARP security on.

```
awplus(config)# interface <vid-list>
```

2. Enable ARP security on particular VLANs if required. On untrusted ports, ARP security forwards ARP packets that have a source IP address and MAC address matching a dynamic entry in the DHCP snooping database, or an IP address matching a static entry. It drops other ARP packets, and treats them as ARP security violations.

```
awplus(config-if)# arp security
```

3. Return to Global Configuration mode.

```
awplus(config-if)# exit
```

Configure DHCP Relay Agent Option 82

1. If you do not want the switch to insert DHCP Relay Agent Option 82 information into DHCP packets received on untrusted ports, or to remove this information from DHCP packets transmitted on untrusted ports, disable the DHCP Relay Agent Option 82 agent option. By default, it is enabled if DHCP snooping is enabled.

```
awplus(config)# no ip dhcp snooping agent-option
```

Note - this feature is not available on all switches. See your switch's Command Reference to check availability.

2. If there are edge switches that add the DHCP Relay Agent Option 82 information to DHCP packets, and that are connected to untrusted ports on the switch, you may wish to enable the switch to forward these packets, and the associated DHCP reply packets, without changing the DHCP Relay Agent Option 82 information in them.

```
awplus(config)# ip dhcp snooping agent-option allow-untrusted
```

3. Enter Interface Configuration mode for one or more ports to add a Subscriber ID for.

```
awplus(config)# interface <port-list>
```

4. Add the Subscriber ID for these ports. The Subscriber ID is included in DHCP Relay Agent Option 82 information.

```
awplus(config-if)# ip dhcp snooping subscriber-id [<sub-id>]
```

5. Enter Interface Configuration mode for one or more VLANs to add a Circuit ID for.

```
awplus(config)# interface <interface-list>
```

6. If desired, specify the Circuit ID for the VLAN or group of VLANs as the VLAN ID and port number. The default is the VLAN ID and Ifindex number.

```
awplus(config-if)# ip dhcp snooping agent-option circuit-id
vlantriplet
```

7. Enter Interface Configuration mode for one or more VLANs to add a Remote ID for.

```
awplus(config)# interface <interface-list>
```

8. If desired, specify the Remote ID for the VLAN or group of VLANs as an alphanumeric (ASCII) string, 1 to 63 characters in length. The default is the switch's MAC address.

```
awplus(config-if)# ip dhcp snooping agent-option remote-id <remote-id>
```

9. Return to Global Configuration mode.

```
awplus(config-if)# exit
```

Configure MAC address verification

1. If not required, disable MAC address verification. It is enabled by default.

```
awplus(config)# no ip dhcp snooping verify mac-address
```

Configure the DHCP snooping database

1. If required, change the location of the file to which the switch writes the dynamic entries from the DHCP snooping database.
   The default is NVS (non-volatile storage) or for switches without NVS, flash memory.

```
awplus(config)# ip dhcp snooping database {nvs|flash|card|usb}
```

2. By default, the switch deletes DHCP lease entries from the DHCP snooping database when it receives matching DHCP release messages. Disable these deletions if required, so that lease entries remain in the database until they expire.

```
awplus(config)# no ip dhcp snooping delete-by-client
```

3. If required, set the switch to delete dynamic entries from the DHCP snooping database when their ports go down. By default, entries remain if links go down.

```
awplus(config)# ip dhcp snooping delete-by-linkdown
```

4. You can actively add, modify, or remove static entries from the DHCP snooping database.

```
awplus(config)# ip source binding <ipaddr> [<macaddr>] vlan <vid>
interface <port>
```

5. You can actively add or remove dynamic entries from the DHCP snooping database. These changes affect the current database and backup file, but are not stored in the running configuration.

```
awplus# ip dhcp snooping binding <ipaddr> [<macaddr>] vlan <vid>
interface <port> expiry <expiry-time>
```

Configure violation actions

1. Enter Interface Configuration mode for the ports for which you want to configure actions in response to DHCP snooping or ARP security violations.

```
awplus(config)# interface <port-list>
```

2. If required, set the switch to generate an SNMP notification (trap), to generate a log message, and/or to block traffic on the port on which a violation is detected.

   By default, if a packet does not match the DHCP snooping and ARP security restrictions, the packet is dropped, but no other action is taken.

```
awplus(config)# ip dhcp snooping violation {log|trap|link-down} ...
awplus(config)# arp security violation {log|trap|link-down} ...
```

3. Return to Global Configuration mode.

```
awplus(config)# exit
```

4. In order to send SNMP notifications:

   - set the action for violations to trap
   - configure SNMP
   - set the SNMP server to enable DHCP snooping notifications (by default notifications are disabled on the SNMP server).

   The port connecting the switch to the SNMP manager should be set as a trusted port.

```
awplus(config)# snmp-server enable trap dhcpsnooping
```

5. Return to Privileged Exec mode.

```
awplus(config)# exit
```

Check the configuration

1. Check the DHCP snooping configuration.

```
awplus# show ip dhcp snooping
awplus# show ip dhcp snooping interface [<port-list>]
awplus# show ip dhcp snooping acl
awplus# show arp security
awplus# show arp security interface [<port-list>]
awplus# show running-config dhcp
```

Troubleshooting DHCP snooping

1. Check all entries in the DHCP snooping database.

```
awplus# show ip dhcp snooping binding
```

2. Check the static entries in the DHCP snooping database.

```
awplus# show ip source binding
```

3. Check DHCP snooping statistics.

```
awplus# show ip dhcp snooping statistics [detail] [interface
<interface-list>]
awplus# clear ip dhcp snooping statistics [interface <port-list>]
```

4. Check ARP security statistics.

```
awplus# show arp security statistics [detail] [interface <port-list>]
awplus# clear arp security statistics [interface <port-list>]
```

5. Enable debug output for DHCP snooping and/or ARP security.

```
awplus# debug ip dhcp snooping {all|acl|db|packet [detail]}
awplus# show debugging ip dhcp snooping
awplus# debug arp security
awplus# show debugging arp security
```

6. If you have not already set the switch to log DHCP snooping and ARP security violations, you can do this for troubleshooting purposes. See "Configure violation actions" on page 16.

7. Display the contents of the buffered log, including any DHCP snooping log and debug messages.

```
awplus# show log
```

Disabling DHCP Snooping

Disabling DHCP snooping removes all DHCP snooping configuration from the running configuration, except for

- any DHCP snooping maximum bindings settings (**ip dhcp snooping max-bindings**), and
- any additional DHCP snooping-based ACLs you have created for filtering on untrusted ports.

You must remove any such additional DHCP snooping-based ACLs, using the **no access-group** command. This is because these ACLs block all traffic except for traffic that matches DHCP snooping entries. Once you have disabled DHCP snooping, these ACLs will block all traffic. Note that if you disable DHCP snooping on particular VLANs (using the **no ip dhcp snooping** command), you need to make sure you remove any additional filtering ACLs that apply to those VLANs.

C613-22061-00 REV F

Allied Telesis NETWORK SMARTER

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com