

AlliedWare™ OS

How To | Use DHCP Snooping, Option 82, and Filtering on AT-8800, AT-8600, AT-8700XL, Rapier, and Rapier i Series Switches

Introduction

It has increasingly become a legal requirement for service providers to identify which of their customers were using a specific IP address at a specific time. This means that service providers must be able to:

- Know which customer was allocated an IP address at any time.
- Guarantee that customers cannot avoid detection by spoofing an IP address that was not actually allocated to them.

These security features provide a traceable history in the event of an official query. Three components are used to provide this traceable history:

- DHCP snooping
- DHCP Option 82
- DHCP filtering

With DHCP snooping an administrator can control port-to-IP connectivity by:

- permitting port access to specified IP addresses only
- permitting port access to DHCP issued IP addresses only
- dictating the number of IP clients on any given port
- passing location information about an IP client to the DHCP server
- permitting only known IP clients to ARP

This document explains each feature and provides the minimum configuration to enable them. There are also two configuration examples that make advanced use of the features.

This document contains the following contents:

Introduction	1
Which products and software version does this information apply to?	2
Related How To Notes	3
DHCP snooping	3
Minimum configuration	3
The database	4
Trusted and non-trusted ports	6
Enabling DHCP snooping	6
Static binding	6
Completely removing the DHCP snooping database	7
DHCP Option 82	8
Protocol details	9
Configuring Option 82	10
DHCP filtering	11
Configuring filtering	11
ARP security	12
Resource considerations	12
Configuration examples	14
Configuring the switch for DHCP snooping, filtering and Option 82, when it is acting as a layer 2 switch	14
Configuring the switch for DHCP snooping, filtering, and Option 82, when it is acting as a layer 3 BOOTP Relay Agent	17
Troubleshooting	20
No trusted ports configured	20
The DHCP client continually sends requests instead of a discover	21
Switch is dropping ARPs	22
Displaying log entries	24
Appendix 1: ISC DHCP server	25

Which products and software version does this information apply to?

The information provided in this document applies to the following switches, running AlliedWare version 2.7.6 and above:

- AT-8800 series
- AT-8600 series
- AT-8700XL series
- Rapier and Rapier i series

Related How To Notes

The following How To Note describes DHCP snooping on AT-9900, x900-48 and AT-8948 series switches:

- *How To Use DHCP Snooping, Option 82, and Filtering on AT-9900 and x900-48 Series Switches*

The following How To Notes also use DHCP snooping in their solutions:

- *How To Use MAC-Forced Forwarding with DHCP Snooping to Create Enhanced Private VLANs*
- *How To Create A Secure Network With Allied Telesis Managed Layer 3 Switches*
- *How To Use DHCP Snooping and ARP Security to Block ARP Poisoning Attacks*

How To Notes are available from the library at www.alliedtelesis.com/resources/literature/howto.aspx.

DHCP snooping

DHCP snooping forces all DHCP packets to be sent up to the switch CPU before forwarding. The switch CPU then keeps a database of the IP addresses that are currently allocated to downstream clients and the switch ports that the relevant clients are attached to.

Note: The switch CPU does not store a history log. The DHCP server does this.

DHCP snooping performs two main tasks:

- Keeping a record of which IP addresses are currently allocated to hosts downstream of the ports on the switch.
- Deciding which packets are candidates for having Option 82 information inserted, and actively filtering out packets that are deemed to be invalid DHCP packets (according to criteria described below).

Note: Option 82 must be enabled separately.

Minimum configuration

The following output shows the minimum configuration required to use DHCP snooping and provide filtered connectivity. With this configuration a client will be able to receive a DHCP address, and access the IP network. If the client manually changes its IP, it will not be permitted access to the IP network. The administrator will also be able to see the current valid entries in the DHCP snooping database.

```
# DHCP Snooping configuration
enable dhcpsnooping
set dhcpsnooping port=24 trusted=yes
```

The database

The switch watches the DHCP packets that it is passing back-and-forth. It also maintains a database that lists the DHCP leases it knows are being held by devices downstream of its ports.

Each lease in the database holds the following information:

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

When inserting Option 82 information into the DHCP packets, the switch uses the information it has stored in the database for filtering and for filling in the fields.

DHCP snooping database time-out

The CPU will time-out database entries if the lease, also stored in the database, expires.

Database survival across reboots

The database is periodically saved as a .dsn file into non-volatile storage. Therefore the database will survive a reboot.

Verifying the status of snooped users

To verify the status of snooped users, use the command **show dhcpsnooping database**.

```

Manager > show dhcpsnooping database

DHCP Snooping Binding Database
-----
Full Leases/Max Leases ... 1/52
Check Interval ..... 60 seconds
Database Listeners ..... CLASSIFR

Current valid entries
MAC Address      IP Address      Expires(s)  VLAN  Port      ID      Source
-----
00-03-47-6b-a5-7a  10.11.67.50    56           48     16         3        Dynamic
-----
Entries with client lease but no listeners
MAC Address      IP Address      Expires(s)  VLAN  Port      ID      Source
-----
None...
-----
Entries with no client lease and no listeners
MAC Address      IP Address      Expires(s)  VLAN  Port      ID      Source
-----
None...

```

List of terms:

MAC Address: The MAC address of the snooped DHCP client.

IP Address: The IP address that has been allocated to the snooped DHCP client.

Expires: The time, in seconds, until the DHCP client entry will expire.

VLAN: The VLAN to which the snooped DHCP client is connected.

Port: The port to which the snooped DHCP client is connected.

ID: The unique ID for the entry in the DHCP snooping database. This ID is dynamically allocated to all clients. (The same ID can be seen in **show dhcpsnooping filter**.)

Database Listeners: These are switch features (or modules) that have registered to listen to the Binding Database. Database listeners are informed when an entry is **added** or **deleted** from the database. In this case the Classifier module will be informed so the dynamic classifiers can be updated.

Source: How the DHCP binding was entered into the database:

- User = static
- File = read from bindings. dsn (usually at boot time)
- Dynamic = it was snooped

To see port details, use the commands **show dhcpsnooping port** and **show dhcpsnooping count**.

```
Manager > show dhcpsnooping port=16
```

```
DHCP Snooping Port Information:
```

```
-----
Port ..... 16
  Trusted ..... No
  Full Leases/Max Leases ... 1/1
  Subscriber-ID .....
```

```
Manager > show dhcpsnooping count
```

```
DHCP Snooping Counters
```

```
-----
DHCP Snooping
  InPackets ..... 1751
  InBootpRequests ..... 908
  InBootpReplies ..... 843
  InDiscards ..... 0
```

```
ARP Security
  InPackets ..... 0
  InDiscards ..... 0
  NoLease ..... 0
  Invalid ..... 0
-----
```

Trusted and non-trusted ports

The concept of trusted and non-trusted ports is fundamental to the operation of DHCP snooping:

- Trusted ports connect to a trusted entity in the network, and are under the complete control of the network manager.
- Non-trusted ports connect an untrusted entity to the trusted network.
- Non-trusted ports can connect to non-trusted ports.

In general, trusted ports connect to the network core, and non-trusted ports connect to subscribers.

DHCP snooping will make forwarding decisions based on the trust status of ports:

- BOOTP packets that contain Option 82 information received on untrusted ports will be dropped
- If Option 82 is enabled, the switch will insert Option 82 information into BOOTP REQUEST packets received from an untrusted port.
- BOOTP REQUEST packets that contain Option 82 information received on trusted ports will *not* have the Option 82 information updated with information for the receive port. It will be kept.
- BOOTP REPLY packets (from servers) should come from a trusted source.
- The switch will remove Option 82 information from BOOTP REPLY packets destined to an untrusted port.
- BOOTP REPLY packets received on non-trusted ports will be dropped.

Enabling DHCP snooping

DHCP snooping is enabled globally by the command **enable dhcpsnooping**. All ports are untrusted by default. For DHCP snooping to do anything useful, at least one port must be trusted.

Static binding

If there is a device with a statically set IP attached to a port in the DHCP snooping port range, then, with filtering enabled it is necessary to statically bind it to the port. This will ensure the device's IP connectivity to the rest of the network.

If a device with the IP **172.16.1.202** and MAC address **00-00-00-00-00-ca** is attached to VLAN 1 on port 2 then a static binding is configured by adding the following command to the basic DHCP configuration (see "[Minimum configuration](#)" on page 3):

```
add dhcpsnooping binding=00-00-00-00-00-CA interface=vlan1 ip=172.16.1.202
    port=2
```

Adding a static binding uses a lease on the port. If the maximum leases on the port is 1 (the default), the static binding means that no device on the port can acquire an address by DHCP.

Completely removing the DHCP snooping database

To completely remove the database, it is necessary to delete the file **nvs:bindings.dsn**.

```

Manager > delete fi=nvs:bindings.dsn
nvs:bindings.dsn successfully deleted
1 file deleted.

Info (1056003): Operation successful.

Manager > enable dhcpsnooping
DHCPSPN_DB: Reloading static entries...

Info (1137057): DHCPSPNOOPING has been enabled.

Manager > DHCPSPN_DB: Reading entries from file...
DHCPSPN_DB: Full file name is: (nvs:bindings.dsn)
DHCPSPN_DB: File nvs:bindings.dsn not present on device, nothing to load.

```

So the database is empty:

```

Manager > show dhcpsnooping database

DHCP Snooping Binding Database
-----
Database Version ..... 1
Full Leases/Max Leases ... 0/151
Check Interval ..... 60 seconds
Database Listeners ..... CLASSIFR

Current valid entries
MAC Address      IP Address      Expires(s)  VLAN  Port      ID      Source
-----
None...
-----
Entries with client lease but no listeners
MAC Address      IP Address      Expires(s)  VLAN  Port      ID      Source
-----
None...
-----
Entries with no client lease and no listeners
MAC Address      IP Address      Expires(s)  VLAN  Port      ID      Source
-----
None...
-----

```

DHCP Option 82

DHCP Relay Agent Information Option 82 is an extension to the Dynamic Host Configuration Protocol (DHCP), and is defined in RFC 3046 and RFC 3993.

DHCP Option 82 can be used to send information about DHCP clients to the authenticating DHCP server. DHCP Option 82 will identify the VLAN number, port number and, optionally a customer ID of a client, during any IP address allocation. When DHCP Option 82 is enabled on the switch, it inserts the above information into the DHCP packets as they pass through the switch on their way to the DHCP server. The DHCP server stores the IP allocation record.

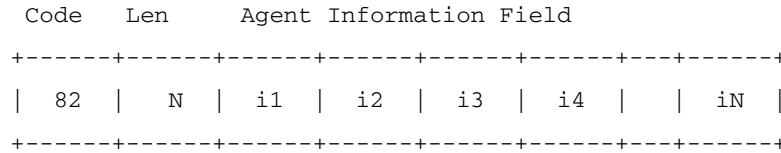
DHCP Option 82 can work in either layer 2 forwarding or layer 3 routing modes. There are significant differences in operation and configuration of these two modes – the latter needing BOOTP Relay support. Some configuration examples and operation descriptions are provided in a later section of this document.

Although Option 82 is titled the DHCP Relay Agent Information Option, the device that inserts the Option 82 information into a DHCP packet does not *have* to be acting as DHCP relay. A layer 2 switch can insert the Option 82 information into the DHCP packets (if snooping is enabled). The Option 82 information needs to be inserted into the DHCP packets by a switch at the edge of the network, because only the edge switch knows the information that uniquely identifies the subscriber that the IP address was allocated to.

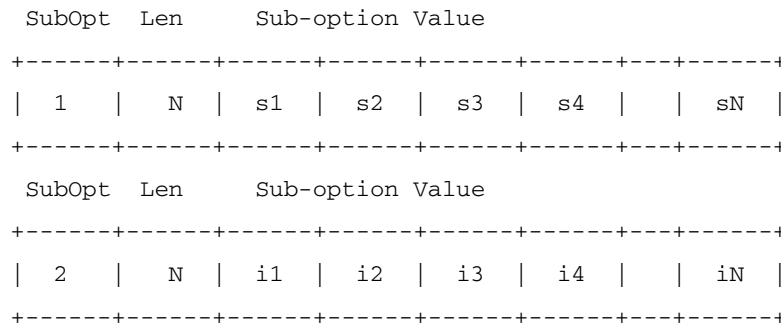
It is quite likely that the edge switch will be a layer 2 switch, rather than a DHCP-relaying layer 3 switch.

Protocol details

In the DHCP packet, the Option 82 segment is organized as a single DHCP option containing one or more sub-options that convey information known by the relay agent. The format of the option is shown below:



The sub-options within the DHCP option are constructed as follows:



The following table shows a list of the sub-options that are used for identifying the subscriber that the IP address was allocated to:

Sub-option	RFC	Description
1	RFC 3046	Agent Circuit ID sub-option – used for defining the switch port and VLAN number of the port user(s).
2	RFC 3046	Agent Remote ID sub-option – used for defining the MAC address of the switch that added the Option 82 information.
6	RFC 3993	Subscriber-ID sub-option – optionally configured per port using set dhcpsnooping port=x subscriberid=x – can define port customer name, or switch name.

Example Packet

The following shows an extract of a DHCP Request packet that includes Option 82 details:

```

DHCP Message Type = DHCP Request
Bootstrap Protocol
Option 82 - Agent Information (Option)
0000: 52 20 01 06 00 04 00 30 00 05 02 08 00 06 00 00 R .....
0010: CD 11 B2 52 06 0C 55 73 65 72 49 64 30 31 32 33 ...R..UserId0123
0020: 34 35                                         45
    
```

Analysis

The following table provides an analysis of the strings in the above DHCP Request packet extract:

Text Colour	Analysis
Green	This is the Agent Circuit ID
Blue	This is the Agent
Red	This is the subscriber ID sub-option

The Agent circuit ID string **00 30 00 05** translates as:

30 = vlan48

05 = switch port 5

Configuring Option 82

Different commands are used to turn on Option 82 depending on whether the switch is performing DHCP snooping or DHCP relay. For the DHCP snooping, the command is:

```
enable dhcpsnooping option82
```

The subscriber ID to be used on any given port can be set using the command:

```
set dhcpsnooping port=x subscriberid="xxxx"
```

If the switch is acting as a DHCP relay and there is no requirement to also maintain a DHCP snooping database, then the DHCP relay process can be configured to insert option 82 information into the relayed packets:

```
enable bootp relay option82
```

The subscriber ID to be used on any given port can be configured with:

```
set bootp relay option82 subscriberid="xxxx"
```

Note: The use of BOOTP relay without DHCP snooping will not be discussed any further in this document.

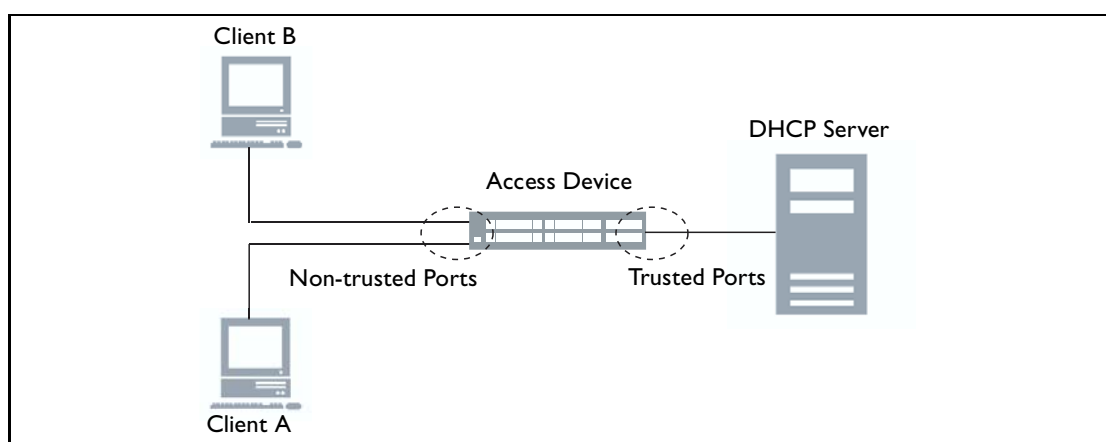
Agent Circuit ID and **Agent Remote ID** are sub-options that are also sent as part of the Option 82 data but they are not configurable.

DHCP filtering

The purpose of DHCP filtering is to prevent IP addresses from being falsified or ‘spoofed’. This guarantees that customers cannot avoid detection by spoofing an IP address that was not actually allocated to them.

DHCP filtering is achieved by creating dynamic classifiers. The dynamic classifiers are configured with DHCP snooping placeholders for the source IP address (and possibly source MAC address), to match on.

The dynamic classifiers are attached to filters, which are applied to a port. Only those packets with a source IP address that matches one of the IP addresses allocated to the devices connected to that port are allowed through.



Configuring filtering

The switch can be configured to block all packets arriving from clients, unless their source addresses are those known by the switch to have been allocated to the clients by DHCP.

Note: The filtering does not, of course, block DHCP packets. In fact, the DHCP snooping process creates a filter which forces DHCP packets to the CPU before any other filters can process the packet.

► To configure how many times the filters or flowgroups will be replicated:

```
set dhcpsnooping port=<port-list> maxlease=<number>
```

When DHCP snooping is enabled, one blocking filter rule is set up on each port. Then, a permit rule for each client is set up in the switch’s hardware filtering table after a DHCP exchange is successfully completed. These dynamic filtering rules are added for each unique DHCP client until there are **maxlease** number of entries on that port, or the switch has run out of filter resources.

ARP security

It is also possible to enable DHCP snooping ARP security. If enabled this will ensure that ARP packets received on non-trusted ports are only permitted if they originate from an IP address that has been allocated by DHCP.

► To enable DHCP snooping ARP security:

```
enable dhcpsnooping arpsecurity
```

DHCP snooping filter show command

To see what addresses have been inserted into filters using DHCP snooping classifiers, use the command **show dhcpsnooping filter**:

```
Manager > show dhcpsnooping filter

DHCP Snooping ACL ( 150 entries )
ClassID      FlowID      Port      EntryID      IP Address/Port/Mac
-----
60161        0           16        3            10.11.67.50/16/00-03-47-6b-a5-7a
61161        0           16        3            10.11.67.50/16/00-03-47-6b-a5-7a
62161        0           16        3            10.11.67.50/16/00-03-47-6b-a5-7a
...
```

List of terms:

The **FlowID** refers to the associated QoS FlowGroup.

The **EntryID** refers to the associated entry in the DHCP snooping database.

The **ClassID** refers to the dynamically created classifier entry.

Resource considerations

Because of the potential for classifier replication, you need to be cautious about running out of classifier resource. Some resource calculations are provided below.

When configuring DHCP classifiers it is possible to run out of classifier resource, especially when using QoS and hardware filter classifiers as well.

When DHCP snooping is enabled on an AT-8600, AT-8800, AT-8700XL, Rapier or Rapier i series switch, it will reserve only one blocking rule for each port (unlike on AT-9900 and x900 series switches). Each block of eight ports, starting from ports 1 to 8, share 127 available entries in the filter resource. Eight entries are immediately used by blocking rules and so the actual number of available leases is 119 over eight ports.

Because 119 entries must be shared between eight ports, the **average** maximum number of leases per port is 14. However, port 1 could be given a maximum of 100 leases, port 2 given

a maximum of 13 leases and ports 3 to 8 given 1 lease each. After that, no port could have its leases increased because the filter resource is completely used up.

Note: On Allied Telesis switches, IGMP snooping and MLD snooping are enabled by default, which occupy 2 filter entries. To dedicate 119 entries to DHCP snooping, IGMP and MLD snooping would need to be disabled with **disable igmpsnoping** and **disable mldsnoping**. Disabling these services is not desirable if multicasting is used in the network.

If other hardware filters are used, they will eat into the filter resource and so your maximum leases (and also your QoS classifiers) would be reduced.

Example on a Rapier 24i

- ▶ If leases are 2 on ports 1 and 2 but 5 on ports 3 to 8, then the number of filter resources used is:

$$(2 \text{ entries} * 2 \text{ ports}) + (5 \text{ entries} * 6 \text{ ports}) = 34 \text{ entries}$$

- ▶ If ARP security is enabled, add 1:

$$(2 \text{ entries} * 2 \text{ ports}) + (5 \text{ entries} * 6 \text{ ports}) + 1 = 35 \text{ entries}$$

- ▶ So, the number of available filter resources left for other hardware filters, QoS classifiers or more leases is:

$$(119 \text{ maximum entries}) - (34 \text{ used}) = 85 \text{ entries}$$

- ▶ or if ARP security is enabled, is:

$$(119 \text{ maximum entries}) - (35 \text{ used}) = 84 \text{ entries}$$

Configuration examples

This section contains the following examples:

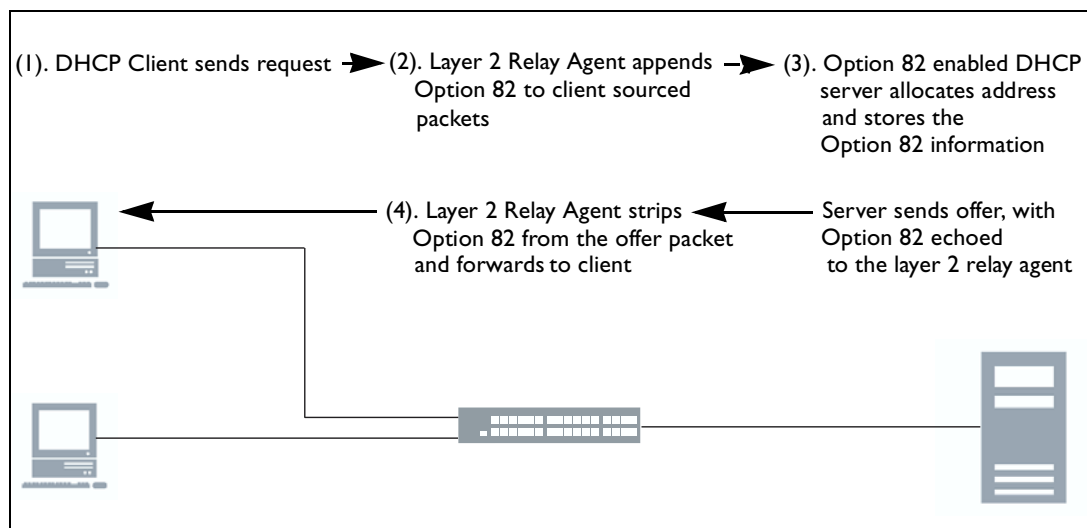
- "Configuring the switch for DHCP snooping, filtering and Option 82, when it is acting as a layer 2 switch" on page 14
- "Configuring the switch for DHCP snooping, filtering, and Option 82, when it is acting as a layer 3 BOOTP Relay Agent" on page 17

Configuring the switch for DHCP snooping, filtering and Option 82, when it is acting as a layer 2 switch

In a layer 2 switching environment, a switch configured with Option 82 snooping will snoop any client-originated DHCP packets and insert Option 82 information into it before forwarding the packet(s) to the DHCP server. In this sense it is a layer 2 relay agent; the packet source and destination addresses are not altered.

DHCP servers that are configured to recognise the relay agent information option (Option 82) may use the information to keep a log of switches and port numbers that IP addresses have been allocated to, and may also use the information for various address assignment policies.

The DHCP server echoes the option back verbatim to the relay agent in server-to-client replies, and the relay agent strips the option before forwarding the reply to the client. This process is shown in the following figure.



► Configure a private VLAN for customers:

```
create vlan="Customers" vid=48 private
```

A private VLAN provides security so customers will not be able to directly connect to or detect each other.

► Add the tagged uplink ports to the VLAN:

```
add vlan="48" port=24 frame=tagged uplink
```

► Add the untagged ports for the customers:

```
add vlan="48" port=1-23
```

This is a layer 2 solution. The IP protocol does not need to be configured.

► Enable DHCP snooping and Option 82 support:

```
enable dhcpsnooping  
enable dhcpsnooping option82
```

It is also possible to enable DHCP snooping ARP security. If enabled, this will ensure that ARP packets received on non-trusted ports are only permitted if they originate from an IP address that has been allocated and snooped by DHCP (**enable dhcpsnooping arpsecurity**).

► Define the DHCP snooping trusted ports:

```
set dhcpsnooping port=24 trusted=yes
```

These ports can receive Option 82 information, and the switch will permit them to send Option 82.

► Define the maximum number of DHCP leases permitted on each port:

```
set dhcpsnooping port=1-23 maxlease=1
```

► Define the string that will be used in the subscriber-ID suboption portion of the Option 82 inserted into DHCP packets:

```
set dhcpsnooping port=1 subscriberid="Ground Floor Room 1"
```

► Create a set of QoS classifiers:

```
create classifier=50 tcpdport=20
create classifier=51 tcpdport=21
create classifier=52 tcpdport=23
create classifier=53 ethformat=ethii prot=0800
```

Classifiers will be applied in QoS to allow prioritisation or traffic shaping. The above example classifies FTP and telnet.

Note: These switches do filtering by default. You do not need to write a rule to drop the traffic that doesn't have a current binding in the DHCP database.

► Define the upstream QoS flow groups:

```
create qos flow=50 priority=7
create qos flow=52 priority=5
create qos flow=53 priority=3
add qos flow=50 classifier=50
add qos flow=50 classifier=51
add qos flow=52 classifier=52
add qos flow=53 classifier=53
```

► Create a traffic class for all upstream flow groups:

```
create qos trafficclass=1
add qos trafficclass=1 flow=50
add qos trafficclass=1 flow=52
add qos trafficclass=1 flow=53
```

► Apply the QoS policy to the downstream ingress ports (customer-facing edge ports):

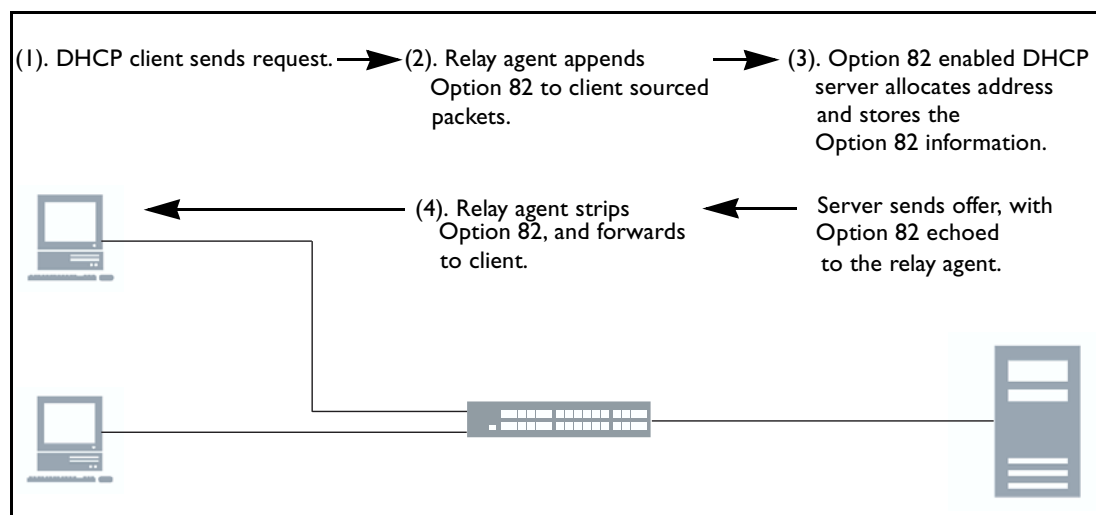
```
create qos policy=1
add qos policy=1 trafficclass=1
set qos port=1-23 policy=1
```

This can be used to control the egress queues that all upstream traffic is sent to. Note that the higher value egress queues have higher priority, so FTP traffic has priority over Telnet.

Configuring the switch for DHCP snooping, filtering, and Option 82, when it is acting as a layer 3 BOOTP Relay Agent

In a layer 3 routing environment, the switch takes on a role of BOOTP Relay Agent, with support for DHCP Option 82. The relay agent inserts the information mentioned above when forwarding client-originated DHCP packets to a DHCP server. DHCP servers that are configured to recognise the relay agent information option may use the information to keep a log of switches and port numbers that IP addresses have been allocated to, and may also use this information for various address assignment policies.

The DHCP server echoes the option back to the relay agent in server-to-client replies, and the relay agent strips the option before forwarding the reply to the client (RFC 3046). This process is shown in the following figure.



► Configure two VLANs for layer 3 access to the DHCP server:

```
create vlan="Customers" vid=48
create vlan="Network" vid=50
```

Here the DHCP Server is on VLAN 50, while the DHCP clients are on VLAN 48.

► Add ports to the VLANs:

```
add vlan="48" port=1-24
add vlan="50" port=25
```

► Configure the switch's IP:

```
enable ip
add ip int=vlan48 ip=10.11.67.254 mask=255.255.255.0
add ip int=vlan50 ip=10.50.1.254 mask=255.255.255.0
add ip rou=0.0.0.0 mask=0.0.0.0 int=vlan50 next=10.50.1.1
```

► For layer 3 support, enable the BOOTP Relay:

```
enable bootp relay
add bootp relay=10.50.1.100
```

Here the DHCP server is set to 10.50.1.100.

► Enable DHCP snooping and Option 82 support:

```
enable dhcpsnooping
enable dhcpsnooping option82
```

Note: It is also possible to enable DHCP snooping ARP security. If enabled this will ensure that ARP packets received on un-trusted ports are only permitted if they originate from an IP address that has been allocated and snooped by DHCP (**enable dhcpsnooping arpsecurity**).

► Define the DHCP snooping trusted port:

```
set dhcpsnooping port=25 trusted=yes
```

This port is open for generating and receiving Option 82 information. By default, the other ports are non-trusted.

► Define the maximum number of DHCP leases permitted on each port:

```
set dhcpsnooping port=1-24 maxlease=1
```

► Define the string that will be used in the subscriber-ID suboption portion of the Option 82 inserted into DHCP packets:

```
set dhcpsnooping port=1 subscriberid="Ground Floor Room 1"
```

► Create a set of QoS classifiers:

```
create classifier=50 tcpdport=20
create classifier=51 tcpdport=21
create classifier=52 tcpdport=23
create classifier=53 ethformat=ethii prot=0800
```

Classifiers will be applied in QoS to allow prioritisation or traffic shaping. The above example classifies FTP and telnet.

Note: These switches do filtering by default. You do not need to write a rule to drop the traffic that doesn't have a current binding in the DHCP database.

► Define the upstream QoS flow groups:

```
create qos flow=50 priority=7
create qos flow=52 priority=5
create qos flow=53 priority=3
add qos flow=50 classifier=50
add qos flow=50 classifier=51
add qos flow=52 classifier=52
add qos flow=53 classifier=53
```

► Create a traffic class for all upstream flow groups:

```
create qos trafficclass=1
add qos trafficclass=1 flow=50
add qos trafficclass=1 flow=52
add qos trafficclass=1 flow=53
```

► Apply the QoS policy to the downstream ingress ports (customer-facing edge ports):

```
create qos policy=1
add qos policy=1 trafficclass=1
set qos port=1-23 policy=1
```

This can be used to control the egress queues that all upstream traffic is sent to. Note that the higher value egress queues have higher priority, so FTP traffic has priority over Telnet.

Troubleshooting

Use the command **enable dhcp snooping debug=all** to get the most verbose level of debugging available. In the following sections, all debugging comes from that command.

Let's look at how you can use debugging to investigate some common problem scenarios.

No trusted ports configured

In the following output, you can see that a DHCP request has arrived at the switch on port 1. The switch does not forward this on to any other port.

```

DHCPSN_Process: [0b4333cc] DHCP Snooping pkt for VLAN 1 from port 1
DHCPSN_Process: [0b4333cc] Type: REQUEST
DHCPSN_Process: [0b4333cc] On DHCP Snooping non-trusted port
DHCPSN_Process: [0b4333cc] DHCP Snoop forwarding pkt at L2 for VLAN 1 InPort 1
DHCPSN_Process: [0b4333cc] L2 Dest MAC is broadcast
DHCPSN_Process: [0b4333cc] Type: REQUEST, L2 forward to trusted ports
DHCPSN_Process: [0b4333cc] Forward ports (except 1)
DHCPSN_Process: [0b4333cc] Tagged:None
DHCPSN_Process: [0b4333cc] Untagged:None

```

The reason for this behaviour is because there are no trusted ports configured. Your DHCP server must be attached to a trusted port.

When a trusted port is configured, the debug shows a more complete conversation, as the following output shows.

```

Manager > set dhcp snooping port=48 trusted=yes

Info (1137260): DHCP Snooping port(s) 48 updated successfully.

Manager >
DHCPSN_Process: [0b43a58c] DHCP Snooping pkt for VLAN 1 from port 1
DHCPSN_Process: [0b43a58c] Type: REQUEST
DHCPSN_Process: [0b43a58c] On DHCP Snooping non-trusted port
DHCPSN_Process: [0b43a58c] DHCP Snoop forwarding pkt at L2 for VLAN 1 InPort 1
DHCPSN_Process: [0b43a58c] L2 Dest MAC is broadcast
DHCPSN_Process: [0b43a58c] Type: REQUEST, L2 forward to trusted ports
DHCPSN_Process: [0b43a58c] Forward ports (except 1)
DHCPSN_Process: [0b43a58c] Tagged:None
DHCPSN_Process: [0b43a58c] Untagged:48
DHCPSN_Process: [0b43adac] DHCP Snooping pkt for VLAN 1 from port 48
DHCPSN_Process: [0b43adac] Type: REPLY
DHCPSN_Process: [0b43adac] On DHCP Snooping trusted port
DHCPSN_Process: [0b43adac] Lookup result for CHAddr 00-06-5b-31-14-af: Port 1
DHCPSN_Process: [0b43adac] DHCP Snoop forwarding pkt at L2 for VLAN 1 InPort 48
DHCPSN_Process: [0b43adac] L2 Dest MAC is broadcast
DHCPSN_Process: [0b43adac] Type: REPLY
DHCPSN_Process: [0b43adac] L2 forward using client port 1
DHCPSN_Process: [0b43adac] Forward ports (except 48)
DHCPSN_Process: [0b43adac] Tagged:None
DHCPSN_Process: [0b43adac] Untagged:1

```

The DHCP client continually sends requests instead of a discover

This happens when the client is renewing its lease or, for whatever reason, believes that should be issued a specific address. If the client does not receive either an ACK or NACK (from a DHCP server) then the client will continue to request the address.

A NACK should cause the client to send a discover packet instead of a request. Hence, if NACK is not received, the client (depending on its DHCP software) may continue to request an address and never send a discover.

Maximum number of leases is exceeded

By default, there is one lease per switch port. If there is already an entry for a port in the DHCP snooping database (in the current valid entries), then the next request on that port from a different MAC address will see the DHCP server ACK discarded:

```
DHCPSN_Process: [0b47d60c] DHCP Snooping pkt for VLAN 1 from port 3
DHCPSN_Process: [0b47d60c] Type: REQUEST
DHCPSN_Process: [0b47d60c] On DHCP Snooping non-trusted port
DHCPSN_Process: [0b47d60c] DHCP Snoop forwarding pkt at L2 for VLAN 1 InPort 3
DHCPSN_Process: [0b47d60c] L2 Dest MAC is broadcast
DHCPSN_Process: [0b47d60c] Type: REQUEST, L2 forward to trusted ports
DHCPSN_Process: [0b47d60c] Forward ports (except 3)
DHCPSN_Process: [0b47d60c]   Tagged:None
DHCPSN_Process: [0b47d60c]   Untagged:48
DHCPSN_Process: [0b47de2c] DHCP Snooping pkt for VLAN 1 from port 48
DHCPSN_Process: [0b47de2c] Type: REPLY
DHCPSN_Process: [0b47de2c] On DHCP Snooping trusted port
DHCPSN_Process: [0b47de2c] Lookup result for CHAddr 00-00-00-00-00-01: Port 3
DHCPSN_Process: [0b47de2c] DHCP Snoop forwarding pkt at L2 for VLAN 1 InPort 48
DHCPSN_Process: [0b47de2c] L2 Dest MAC is unicast
DHCPSN_Process: [0b47de2c] Using chaddr lookup result for dest port(s)
DHCPSN_Process: [0b47de2c] L2 forward packet directly to port 3
DHCPSN_Process: [0b47de2c] Forward ports (except 48)
DHCPSN_Process: [0b47de2c]   Tagged:None
DHCPSN_Process: [0b47de2c]   Untagged:3
DHCPSN_Process: [0b47e64c] DHCP Snooping pkt for VLAN 1 from port 3
DHCPSN_Process: [0b47e64c] Type: REQUEST
DHCPSN_Process: [0b47e64c] On DHCP Snooping non-trusted port
DHCPSN_Process: [0b47e64c] DHCP Snoop forwarding pkt at L2 for VLAN 1 InPort 3
DHCPSN_Process: [0b47e64c] L2 Dest MAC is broadcast
DHCPSN_Process: [0b47e64c] Type: REQUEST, L2 forward to trusted ports
DHCPSN_Process: [0b47e64c] Forward ports (except 3)
DHCPSN_Process: [0b47e64c]   Tagged:None
DHCPSN_Process: [0b47e64c]   Untagged:48
DHCPSN_Process: [0b47ee6c] DHCP Snooping pkt for VLAN 1 from port 48
DHCPSN_Process: [0b47ee6c] Type: REPLY
DHCPSN_Process: [0b47ee6c] On DHCP Snooping trusted port
DHCPSN_Process: [0b47ee6c] Lookup result for CHAddr 00-00-00-00-00-01: Port 3
DHCPSN_Process: [0b47ee6c] DHCP ACK Found...
DHCPSN_DB: Updating entryId 7. Flags 00000010
DHCPSN_DB: Couldn't update: Listener error or will exceed MAXLEASES on port 3 (Current/
MAX 1/1)
DHCPSN_Process: [0b47ee6c] Error adding entry to DB
DHCPSN_Process: [0b47ee6c] Discard packet, DHCP ACK not forwarded
```

Increasing the port's maximum leases will permit multiple clients per port.

```
Manager > set dhcp snooping port=3 maxleases=2
```

```
Info (1137260): DHCP Snooping port(s) 3 updated successfully.
```

Switch is dropping ARPs

If you have DHCP snooping in ARP security mode, then unknown clients on untrusted ports will not be able to ARP.

```
DHCPSN_ARP: [0193a9ec] ARP Received on untrusted port 24 VLAN 1
DHCPSN_ARP: [0193a9ec] ARP Discarded, sender not found in DHCP Snoop DB
```

Known clients on untrusted ports *will be* able to ARP.

```
DHCPSN_ARP: [01a6f5ec] ARP Received on untrusted port 1 VLAN 1
DHCPSN_ARP: [01a6f5ec] ARP to be forwarded, sender validated
DHCPSN_ARP: [01a6f5ec] Forwarding ARP at L2 for VLAN 1
DHCPSN_ARP: [01a6f5ec] Forward ports (except 1)
DHCPSN_ARP: [01a6f5ec] Tagged:None
DHCPSN_ARP: [01a6f5ec] Untagged:24
```

A client is known on an untrusted port if it has an IP/MAC entry in the DHCP snooping database (**show dhcp snooping database**). Your DHCP server must be on a trusted port.

```
Manager > set dhcp snooping port=24 trusted=yes
```

```
Info (1137260): DHCP Snooping port(s) 24 updated successfully.
```

```
Manager >
```

```
DHCPSN_ARP: [023a218c] ARP Received on trusted port 24 VLAN 1
DHCPSN_ARP: [023a218c] Forwarding ARP at L2 for VLAN 1
DHCPSN_ARP: [023a218c] Forward ports (except 24)
DHCPSN_ARP: [023a218c] Tagged:None
DHCPSN_ARP: [023a218c] Untagged:1
```

You cannot work around dropped ARPs from the DHCP server by statically binding the DHCP server's IP and MAC address to a port, instead of setting it as trusted. The switch *will not* send the DHCP server the DHCP request. The switch will not flood the DHCP request to any ports other than trusted ones. So although the switch will let the DHCP server send ARP requests, the DHCP server will not receive any DHCP requests.

```

Manager > add dhcp Snooping binding=00-50-FC-EE-F5-13 ip=172.16.1.1 int=vlan1 port=24
DHCPSN_DB: Creating new entry with entryId 3.
DHCPSN_DB: Notifying DB listener: CLASSIFR
DHCPSN_ACL: dhcpSnoopAclListener >> dbEntryPt=0x010caed4 flags=0x00000080
DHCPSN_ACL: dhcpSnoopAclBindingFindByEntryIndex >> finding binding entryId=3
DHCPSN_ACL: dhcpSnoopAclBindingFindGroup >> found 0 items
DHCPSN_ACL: dhcpSnoopAclBindingFindByEntryIndex >> finding binding entryId=3 it0
DHCPSN_ACL: dhcpSnoopAclBindingFindAllByPortNumber >> finding binding portNum=24
DHCPSN_ACL: dhcpSnoopAclBindingFindGroup >> found 0 items
DHCPSN_ACL: dhcpSnoopAclBindingFindAllByPortNumber >> finding binding portNum=20
DHCPSN_ACL: dhcpSnoopAclBindingCreate >> templateId=10001 flowId=0 port=24 num=3
DHCPSN_ACL: dhcpSnoopAclBindingCreate >> created child-3 bindings of templateId1
DHCPSN_ACL: dhcpSnoopAclBindingBinds >> bclassId=20003 portNum=24 entryId=3
DHCPSN_ACL: dhcpSnoopAclBindingBinds >> success, classifierId=20003 flowGroupId3
DHCPSN_ACL: dhcpSnoopAclListener >> NEW, returns=1
DHCPSN_DB: Change state for 00-50-fc-ee-f5-13, in NONE for event LISTENER_OK
DHCPSN_DB: Changed state for 00-50-fc-ee-f5-13, to FULL

```

Info (1137003): Operation successful.

```

Manager >
DHCPSN_ARP: [02680e6c] ARP Received on untrusted port 24 VLAN 1
DHCPSN_ARP: [02680e6c] ARP to be forwarded, sender validated
DHCPSN_ARP: [02680e6c] Forwarding ARP at L2 for VLAN 1
DHCPSN_ARP: [02680e6c] Forward ports (except 24)
DHCPSN_ARP: [02680e6c] Tagged:None
DHCPSN_ARP: [02680e6c] Untagged:1

```

```

Manager >
DHCPSN_Process: [026ef9ac] DHCP Snooping pkt for VLAN 1 from port 1
DHCPSN_Process: [026ef9ac] Type: REQUEST
DHCPSN_Process: [026ef9ac] On DHCP Snooping non-trusted port
DHCPSN_Process: [026ef9ac] DHCP Snoop forwarding pkt at L2 for VLAN 1 InPort 1
DHCPSN_Process: [026ef9ac] L2 Dest MAC is broadcast
DHCPSN_Process: [026ef9ac] Type: REQUEST, L2 forward to trusted ports
DHCPSN_Process: [026ef9ac] Forward ports (except 1)
DHCPSN_Process: [026ef9ac] Tagged:None
DHCPSN_Process: [026ef9ac] Untagged:None

```

Displaying log entries

The **show log** command is also very useful:

```

Manager > sh log

Date/Time    S Mod  Type  SType Message
-----
02 21:42:55 3 DHCP DHCPS ADD   Adding new entry [chaddr
                                00-11-22-33-44-15],
                                clientIP 2.2.2.2, vlan1, port3, serverIP
                                0.0.0.0, Expires N/A (static entry)
02 21:43:20 4 DHCP DHCPS FAIL  Error adding entry [chaddr
                                00-11-22-33-44-16].
                                Adding another entry will exceed the
                                configured MAXLEASES of 1 for port 3
02 21:43:20 4 CH   MSG   ERROR Static DHCP Snooping entry could not be
                                added.
                                Check log for details
02 21:43:56 3 DHCP DHCPS ADD   Adding new entry [chaddr
                                00-11-22-33-44-16],
                                clientIP 2.2.2.2, vlan1, port7, serverIP
                                0.0.0.0, Expires N/A (static entry)

```

Appendix 1: ISC DHCP server

One DHCP server that has been tested against DHCP snooping is ISC DHCP. This is free software with an option of a support contract. At the time of writing this document, ISC DHCP did not support the logging of RFC3993 sub-option 6. For convenience, here is a sample configuration (dhcpd.conf) for ISC DHCP.

This configuration lets you specify the IP that is given to each MAC address. You may easily write a range statement to assign to any client.

```
ddns-update-style ad-hoc;
option domain-name "test.yourdomain.com";
option domain-name-servers 172.16.1.253;
option broadcast-address 172.16.1.255;
option subnet-mask 255.255.255.0;
use-host-decl-names on;
subnet 172.16.1.0 netmask 255.255.255.0 {
    #filename "/vmlinuz ";
    default-lease-time 86400;
    option subnet-mask 255.255.255.0;
    option domain-name "test.yourdomain.com";
    option domain-name-servers 172.16.1.1;
    option routers 172.16.1.1;
    option broadcast-address 172.16.1.255;
    host linux {
        hardware ethernet 00:06:5b:31:14:af;
        fixed-address 172.16.1.100;
        filename "/vmlinuz ";
    }
    host test01 {
        hardware ethernet 00:00:00:00:00:01;
        fixed-address 172.16.1.201;
    }
    host test02 {
        hardware ethernet 00:00:00:00:00:02;
        fixed-address 172.16.1.202;
    }
    host test03 {
        hardware ethernet 00:00:00:00:00:03;
        fixed-address 172.16.1.203;
    }
    host RapierMAX {
        hardware ethernet 00:00:cd:11:b2:4c;
        fixed-address 172.16.1.123;
    }
}
```

The following configuration (thanks to www.thtech.net/article/10) will record Option 82 information in syslog. This part is ignored if no Option 82 information is passed on. The logfile location is configured in syslog.

```
if exists agent.circuit-id
{
  log ( info, concat( "NEW LEASE - IP: ", binary-to-ascii (10, 8, ".", leased-address),
    ", PORT: ", binary-to-ascii (10, 8, ":", suffix ( option agent.circuit-id, 2)),
    ", VLAN: ", binary-to-ascii(10, 16, "", substring( option agent.circuit-id, 2, 2)),
    ", SWITCH: ", binary-to-ascii(16, 8, ":", substring( option agent.remote-id, 2, 6))));

  log ( info, concat( "IP ", binary-to-ascii (10, 8, ".", leased-address),
    " raw option-82 info is CID: ", binary-to-ascii (10, 8, ".", option agent.circuit-id), "
    AID: ",
    binary-to-ascii(16, 8, ".", option agent.remote-id)));
```

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

© 2007 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. Allied Telesis is a trademark or registered trademark of Allied Telesis, Inc. in the United States and other countries. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.

C613-16086-00 REV B