

Configuring Advanced Threat Protection

Contents

Introduction	11-3
DHCP Snooping	11-4
Overview	11-5
Enabling DHCP Snooping	11-6
Enabling DHCP Snooping on VLANs	11-8
Configuring DHCP Snooping Trusted Ports	11-8
Configuring Authorized Server Addresses	11-9
Using DHCP Snooping with Option 82	11-10
Changing the Remote-id from a MAC to an IP Address	11-12
Disabling the MAC Address Check	11-12
The DHCP Binding Database	11-13
Operational Notes	11-14
Log Messages	11-15
Dynamic ARP Protection	11-17
Introduction	11-17
Enabling Dynamic ARP Protection	11-19
Configuring Trusted Ports	11-19
Adding an IP-to-MAC Binding to the DHCP Database	11-21
Configuring Additional Validation Checks on ARP Packets	11-22
Verifying the Configuration of Dynamic ARP Protection	11-22
Displaying ARP Packet Statistics	11-23
Monitoring Dynamic ARP Protection	11-24
Dynamic IP Lockdown	11-24
Protection Against IP Source Address Spoofing	11-25
Prerequisite: DHCP Snooping	11-25
Filtering IP and MAC Addresses Per-Port and Per-VLAN	11-26
Enabling Dynamic IP Lockdown	11-27

Operating Notes	11-27
Adding an IP-to-MAC Binding to the DHCP Binding Database	11-29
Potential Issues with Bindings	11-29
Adding a Static Binding	11-30
Verifying the Dynamic IP Lockdown Configuration	11-30
Displaying the Static Configuration of IP-to-MAC Bindings	11-31
Debugging Dynamic IP Lockdown	11-32
Differences Between Switch Platforms	11-33
Using the Instrumentation Monitor	11-35
Operating Notes	11-36
Configuring Instrumentation Monitor	11-37
Examples	11-38
Viewing the Current Instrumentation Monitor Configuration	11-39

Introduction

As your network expands to include an increasing number of mobile devices, continuous Internet access, and new classes of users (such as partners, temporary employees, and visitors), additional protection from attacks launched from both inside and outside your internal network is often necessary.

Advanced threat protection can detect port scans and hackers who try to access a port or the switch itself. The following software features provide advanced threat protection and are described in this chapter:

- DHCP snooping: Protects your network from common DHCP attacks, such as:
 - Address spoofing in which an invalid IP address or network gateway address is assigned by a rogue DHCP server.
 - Address exhaustion of available addresses in the network DHCP server, caused by repeated attacker access to the network and numerous IP address requests.
- Dynamic ARP protection: Protects your network from ARP cache poisoning as in the following cases:
 - An unauthorized device forges an illegitimate ARP response and network devices use the response to update their ARP caches.
 - A denial-of-service (DoS) attack from unsolicited ARP responses changes the network gateway IP address so that outgoing traffic is prevented from leaving the network and overwhelms network devices.
- Instrumentation monitor: Protects your network from a variety of other common attacks besides DHCP and ARP attacks, including:
 - Attempts at a port scan to expose a vulnerability in the switch, indicated by an excessive number of packets sent to closed TCP/UDP ports
 - Attempts to fill all IP address entries in the switch's forwarding table and cause legitimate traffic to be dropped, indicated by an increased number of learned IP destination addresses
 - Attempts to spread viruses, indicated by an increased number of ARP request packets

- Attempts to exhaust system resources so that sufficient resources are not available to transmit legitimate traffic, indicated by an unusually high use of specific system resources
- Attempts to attack the switch's CPU and introduce delay in system response time to new network events
- Attempts by hackers to access the switch, indicated by an excessive number of failed logins or port authentication failures
- Attempts to deny switch service by filling the forwarding table, indicated by an increased number of learned MAC addresses or a high number of MAC address moves from one port to another
- Attempts to exhaust available CPU resources, indicated by an increased number of learned MAC address events being discarded

DHCP Snooping

Command	Page
dhcp-snooping	page 11-6
authorized-server	page 11-9
database	page 11-13
option	page 11-10
trust	page 11-8
verify	page 11-12
vlan	page 11-8
show dhcp-snooping	page 11-6
show dhcp-snooping stats	page 11-7
dhcp-snooping binding	page 11-14
debug dhcp-snooping	page 11-14

Overview

You can use DHCP snooping to help avoid the Denial of Service attacks that result from unauthorized users adding a DHCP server to the network that then provides invalid configuration data to other DHCP clients on the network. DHCP snooping accomplishes this by allowing you to distinguish between trusted ports connected to a DHCP server or switch and untrusted ports connected to end-users. DHCP packets are forwarded between trusted ports without inspection. DHCP packets received on other switch ports are inspected before being forwarded. Packets from untrusted sources are dropped. Conditions for dropping packets are shown below.

Condition for Dropping a Packet	Packet Types
A packet from a DHCP server received on an untrusted port	DHCPOFFER, DHCPACK, DHCPNACK
If the switch is configured with a list of authorized DHCP server addresses and a packet is received from a DHCP server on a trusted port with a source IP address that is not in the list of authorized DHCP server addresses.	DHCPOFFER, DHCPACK, DHCPNACK
Unless configured to not perform this check, a DHCP packet received on an untrusted port where the DHCP client hardware address field does not match the source MAC address in the packet	N/A
Unless configured to not perform this check, a DHCP packet containing DHCP relay information (option 82) received from an untrusted port	N/A
A broadcast packet that has a MAC address in the DHCP binding database, but the port in the DHCP binding database is different from the port on which the packet is received	DHCPRELEASE, DHCPDECLINE

Enabling DHCP Snooping

DHCP snooping is enabled globally by entering this command:

```
ProCurve(config)# dhcp-snooping
```

Use the **no** form of the command to disable DHCP snooping.

Syntax: [no] dhcp-snooping [authorized-server | database | option | trust | verify | vlan]

authorized server: Enter the IP address of a trusted DHCP server. If no authorized servers are configured, all DHCP server addresses are considered valid.
Maximum: 20 authorized servers

database: To configure a location for the lease database, enter a URL in the format **tftp://ip-addr/ascii-string**. The maximum number of characters for the URL is 63.

option: Add relay information option (Option 82) to DHCP client packets that are being forwarded out trusted ports. The default is **yes**, add relay information.

trust: Configure trusted ports. Only server packets received on trusted ports are forwarded. Default: **untrusted**.

verify: Enables DHCP packet validation. The DHCP client hardware address field and the source MAC address must be the same for packets received on untrusted ports or the packet is dropped. Default: **Yes**

vlan: Enable DHCP snooping on a vlan. DHCP snooping must be enabled already. Default: **No**

To display the DHCP snooping configuration, enter this command:

```
ProCurve(config)# show dhcp-snooping
```

An example of the output is shown below.

```
ProCurve(config)# show dhcp-snooping
DHCP Snooping Information
  DHCP Snooping           : Yes
  Enabled Vlans           :
  Verify MAC              : Yes
  Option 82 untrusted policy : drop
  Option 82 Insertion     : Yes
  Option 82 remote-id     : mac
  Store lease database    : Not configured
  Port Trust
  -----
  B1      No
  B2      No
```

Figure 11-1. An Example of the DHCP Snooping Command Output

To display statistics about the DHCP snooping process, enter this command:

```
ProCurve(config)# show dhcp-snooping stats
```

An example of the output is shown below.

```
ProCurve(config)# show dhcp-snooping stats
```

Packet type	Action	Reason	Count
server	forward	from trusted port	8
client	forward	to trusted port	8
server	drop	received on untrusted port	2
server	drop	unauthorized server	0
client	drop	destination on untrusted port	0
client	drop	untrusted option 82 field	0
client	drop	bad DHCP release request	0
client	drop	failed verify MAC check	0

Figure 11-2. Example of Show DHCP Snooping Statistics

Enabling DHCP Snooping on VLANs

DHCP snooping on VLANs is disabled by default. To enable DHCP snooping on a VLAN or range of VLANs enter this command:

```
ProCurve(config)# dhcp-snooping vlan <vlan-id-range>
```

You can also use this command in the vlan context, in which case you cannot enter a range of VLANs for snooping.

Below is an example of DHCP snooping enabled on VLAN 4.

```
ProCurve(config)# dhcp-snooping vlan 4
ProCurve(config)# show dhcp-snooping

DHCP Snooping Information

DHCP Snooping           : Yes
Enabled Vlans           : 4
Verify MAC               : Yes
Option 82 untrusted policy : drop
Option 82 Insertion     : Yes
Option 82 remote-id     : mac
```

Figure 11-3. Example of DHCP Snooping on a VLAN

Configuring DHCP Snooping Trusted Ports

By default, all ports are untrusted. To configure a port or range of ports as trusted, enter this command:

```
ProCurve(config)# dhcp-snooping trust <port-list>
```

You can also use this command in the interface context, in which case you are not able to enter a list of ports.

```
ProCurve(config)# dhcp-snooping trust B1-B2
ProCurve(config)# show dhcp-snooping

DHCP Snooping Information

DHCP Snooping           : Yes
Enabled Vlans           : 4
Verify MAC               : Yes
Option 82 untrusted policy : drop
Option 82 Insertion     : Yes
Option 82 remote-id     : mac

Store lease database : Not configured

Port  Trust
-----
B1    Yes
B2    Yes
B3    No
```

Figure 11-4. Example of Setting Trusted Ports

DHCP server packets are forwarded only if received on a trusted port; DHCP server packets received on an untrusted port are dropped.

Use the **no** form of the command to remove the trusted configuration from a port.

Configuring Authorized Server Addresses

If authorized server addresses are configured, a packet from a DHCP server must be received on a trusted port AND have a source address in the authorized server list in order to be considered valid. If no authorized servers are configured, all servers are considered valid. You can configure a maximum of 20 authorized servers.

To configure a DHCP authorized server address, enter this command in the global configuration context:

```
ProCurve(config)# dhcp-snooping authorized-server
                    <ip-address>
```

```
ProCurve(config)# show dhcp-snooping

DHCP Snooping Information

DHCP Snooping           : Yes
Enabled Vlans           : 4
Verify MAC              : No
Option 82 untrusted policy : drop
Option 82 Insertion     : Yes
Option 82 remote-id     : subnet-ip

Authorized Servers
-----
111.222.3.4
```

Figure 11-5. Example of Authorized Servers for DHCP Snooping

Using DHCP Snooping with Option 82

DHCP adds Option 82 (relay information option) to DHCP request packets received on untrusted ports by default. (See “Configuring DHCP Relay” in the *Management and Configuration Guide* for more information on Option 82.)

When DHCP is enabled globally and also enabled on a VLAN, and the switch is acting as a DHCP relay, the settings for the DHCP relay Option 82 command are ignored when snooping is controlling Option 82 insertion. Option 82 inserted in this manner allows the association of the client’s lease with the correct port, even when another device is acting as a DHCP relay or when the server is on the same subnet as the client.

Note

DHCP snooping only overrides the Option 82 settings on a VLAN that has snooping enabled, not on VLANS without snooping enabled.

If DHCP snooping is enabled on a switch where an edge switch is also using DHCP snooping, it is desirable to have the packets forwarded so the DHCP bindings are learned. To configure the policy for DHCP packets from untrusted ports that already have Option 82 present, enter this command in the global configuration context.

Syntax: [no] dhcp-snooping option 82 [remote-id <mac | subnet-ip | mgmt-ip>]
[untrusted-policy <drop | keep | replace>]

Enables DHCP Option 82 insertion in the packet.

remote-id *Set the value used for the **remote-id** field of the relay information option.*

mac: *The switch mac address is used for the remote-id. This is the default.*

subnet-ip: *The IP address of the VLAN the packet was received on is used for the remote-id. If **subnet-ip** is specified but the value is not set, the MAC address is used.*

mgmt-ip: *The management VLAN IP address is used as the remote-id. If **mgmt-ip** is specified but the value is not set, the MAC address is used.*

untrusted-policy *Configures DHCP snooping behavior when forwarding a DHCP packet from an untrusted port that already contains DHCP relay information (Option 82). The default is **drop**.*

drop: *The packet is dropped.*

keep: *The packet is forwarded without replacing the option information.*

replace: *The existing option is replaced with a new Option 82 generated by the switch.*

Note

The default **drop** policy should remain in effect if there are any untrusted nodes, such as clients, directly connected to this switch.

Changing the Remote-id from a MAC to an IP Address

By default, DHCP snooping uses the MAC address of the switch as the remote-id in Option 82 additions. The IP address of the VLAN the packet was received on or the IP address of the management VLAN can be used instead by entering this command with the associated parameter:

```
ProCurve(config)# dhcp-snooping option 82 remote-id  
                <mac|subnet-ip|mgmt-ip>
```

```
ProCurve(config)# dhcp-snooping option 82 remote-id subnet-  
ip  
ProCurve(config)# show dhcp-snooping  
  
DHCP Snooping Information  
  
DHCP Snooping           : Yes  
Enabled Vlans           : 4  
Verify MAC              : Yes  
Option 82 untrusted policy : drop  
Option 82 Insertion     : Yes  
Option 82 remote-id     : subnet-ip
```

Figure 11-6. Example of DHCP Snooping Option 82 using the VLAN IP Address

Disabling the MAC Address Check

DHCP snooping drops DHCP packets received on untrusted ports when the check address (chaddr) field in the DHCP header does not match the source MAC address of the packet (default behavior). To disable this checking, use the **no** form of this command.

```
ProCurve(config)# dhcp-snooping verify mac
```

```
ProCurve(config)# dhcp-snooping verify mac
ProCurve(config)# show dhcp-snooping

DHCP Snooping Information

DHCP Snooping           : Yes
Enabled Vlans           : 4
Verify MAC              : yes
Option 82 untrusted policy : drop
Option 82 Insertion     : Yes
Option 82 remote-id     : subnet-ip
```

Figure 11-7. Example Showing the DHCP Snooping Verify MAC Setting

The DHCP Binding Database

DHCP snooping maintains a database of up to 8192 DHCP bindings on untrusted ports. Each binding consists of:

- Client MAC address
- Port number
- VLAN identifier
- Leased IP address
- Lease time

The switch can be configured to store the bindings at a specific URL so they will not be lost if the switch is rebooted. If the switch is rebooted, it will read its binding database from the specified location. To configure this location use this command.

Syntax: [no] dhcp-snooping database [file<tftp://<ip-address>/<ascii-string>>]
[delay<15-86400>][timeout<0-86400>]

- | | |
|----------------|---|
| file | <i>Must be in Uniform Resource Locator (URL) format — “tftp://ip-address/ascii-string”. The maximum filename length is 63 characters.</i> |
| delay | <i>Number of seconds to wait before writing to the database. Default = 300 seconds.</i> |
| timeout | <i>Number of seconds to wait for the database file transfer to finish before returning an error. A value of zero (0) means retry indefinitely. Default = 300 seconds.</i> |

A message is logged in the system event log if the DHCP binding database fails to update.

To display the contents of the DHCP snooping binding database, enter this command.

Syntax: show dhcp-snooping binding

```
ProCurve(config)# show dhcp-snooping binding
```

MacAddress	IP	VLAN	Interface	Time left
22.22.22.22.22.22	10.0.0.1	4	B2	1600

Figure 11-8. Example Showing DHCP Snooping Binding Database Contents

Note

If a lease database is configured, the switch drops all DHCP packets until the lease database is read. This only occurs when the switch reboots and is completed quickly. If the switch is unable to read the lease database from the tftp server, it waits until that operation times out and then begins forwarding DHCP packets.

Enabling Debug Logging

To enable debug logging for DHCP snooping, use this command.

Syntax: [no] debug dhcp-snooping [agent | event | packet]

agent *Displays DHCP snooping agent messages.*

event *Displays DHCP snooping event messages.*

packet *Displays DHCP snooping packet messages.*

Operational Notes

- DHCP is not configurable from the web management interface or menu interface.
- If packets are received at too high a rate, some may be dropped and need to be re-transmitted.

- ProCurve recommends running a time synchronization protocol such as SNTP in order to track lease times accurately.
- A remote server must be used to save lease information or there may be a loss of connectivity after a switch reboot.

Log Messages

Server <ip-address> packet received on untrusted port <port-number> dropped. Indicates a DHCP server on an untrusted port is attempting to transmit a packet. This event is recognized by the reception of a DHCP server packet on a port that is configured as untrusted.

Ceasing untrusted server logs for %s. More than one packet was received from a DHCP server on an untrusted port. To avoid filling the log file with repeated attempts, untrusted server drop packet events will not be logged for the specified <duration>.

Client packet destined to untrusted port <port-number> dropped. Indicates that the destination of a DHCP client unicast packet is on an untrusted port. This event is recognized when a client unicast packet is dropped because the destination address is out a port configured as untrusted.

Ceasing untrusted port destination logs for %s. More than one client unicast packet with an untrusted port destination was dropped. To avoid filling the log file with repeated attempts, untrusted port destination attempts will not be logged for the specified <duration>.

Unauthorized server <ip-address> detected on port <port-number>. Indicates that an unauthorized DHCP server is attempting to send packets. This event is recognized when a server packet is dropped because there are configured authorized servers and a server packet is received from a server that is not configured as an authorized server.

Ceasing unauthorized server logs for <duration>. More than one unauthorized server packet was dropped. To avoid filling the log file with repeated attempts, unauthorized server transmit attempts will not be logged for the specified <duration>.

Received untrusted relay information from client <mac-address> on port <port-number>. Indicates the reception on an untrusted port of a client packet containing a relay information option field. This event is recognized when a client packet containing a relay information option field is dropped because it was received on a port configured as untrusted.

Ceasing untrusted relay information logs for <duration>. More than one DHCP client packet received on an untrusted port with a relay information field was dropped. To avoid filling the log file with repeated attempts, untrusted relay information packets will not be logged for the specified <duration>.

Client address <mac-address> not equal to source MAC <mac-address> detected on port <port-number>. Indicates that a client packet source MAC address does not match the “chaddr” field. This event is recognized when the dhcp-snooping agent is enabled to filter DHCP client packets that do not have a matching “chaddr” field and source MAC address.

Ceasing MAC mismatch logs for <duration>. More than one DHCP client packet with a mismatched source MAC and chaddr field was dropped. To avoid filling the log file with repeated attempts, client address mismatch events will not be logged for the specified <duration>.

Attempt to release address <ip-address> leased to port <port-number> detected on port <port-number> dropped. Indicates an attempt by a client to release an address when a DHCPRELEASE or DHCPDECLINE packet is received on a port different from the port the address was leased to.

Ceasing bad release logs for %s. More than one bad DHCP client release packet was dropped. To avoid filling the log file with repeated bad release dropped packets, bad releases will not be logged for <duration>.

Lease table is full, DHCP lease was not added. The lease table is full and this lease will not be added to it.

Write database to remote file failed errno (error-num). An error occurred while writing the temporary file and sending it using tftp to the remote server.

DHCP packets being rate-limited. Too many DHCP packets are flowing through the switch and some are being dropped.

Snooping table is full. The DHCP binding table is full and subsequent bindings are being dropped.

Dynamic ARP Protection

Introduction

On the VLAN interfaces of a routing switch, dynamic ARP protection ensures that only valid ARP requests and responses are relayed or used to update the local ARP cache. ARP packets with invalid IP-to-MAC address bindings advertised in the source protocol address and source physical address fields are discarded. For more information about the ARP cache, refer to “ARP Cache Table” in the *Multicast and Routing Guide*.

ARP requests are ordinarily broadcast and received by all devices in a broadcast domain. Most ARP devices update their IP-to-MAC address entries each time they receive an ARP packet even if they did not request the information. This behavior makes an ARP cache vulnerable to attacks.

Because ARP allows a node to update its cache entries on other systems by broadcasting or unicasting a gratuitous ARP reply, an attacker can send his own IP-to-MAC address binding in the reply that causes all traffic destined for a VLAN node to be sent to the attacker's MAC address. As a result, the attacker can intercept traffic for other hosts in a classic "man-in-the-middle" attack. The attacker gains access to any traffic sent to the poisoned address and can capture passwords, e-mail, and VoIP calls or even modify traffic before resending it.

Another way in which the ARP cache of known IP addresses and associated MAC addresses can be poisoned is through unsolicited ARP responses. For example, an attacker can associate the IP address of the network gateway with the MAC address of a network node. In this way, all outgoing traffic is prevented from leaving the network because the node does not have access to outside networks. As a result, the node is overwhelmed by outgoing traffic destined to another network.

Dynamic ARP protection is designed to protect your network against ARP poisoning attacks in the following ways:

- Allows you to differentiate between trusted and untrusted ports.
- Intercepts all ARP requests and responses on untrusted ports before forwarding them.
- Verifies IP-to-MAC address bindings on untrusted ports with the information stored in the lease database maintained by DHCP snooping and user-configured static bindings (in non-DHCP environments):

- If a binding is valid, the switch updates its local ARP cache and forwards the packet.
- If a binding is invalid, the switch drops the packet, preventing other network devices from receiving the invalid IP-to-MAC information.

DHCP snooping intercepts and examines DHCP packets received on switch ports before forwarding the packets. DHCP packets are checked against a database of DHCP binding information. Each binding consists of a client MAC address, port number, VLAN identifier, leased IP address, and lease time. The DHCP binding database is used to validate packets by other security features on the switch. For more information, refer to “DHCP Snooping” in the *Access Security Guide*.

If you have already enabled DHCP snooping on a switch, you may also want to add static IP-to-MAC address bindings to the DHCP snooping database so that ARP packets from devices that have been assigned static IP addresses are also verified.

- Supports additional checks to verify source MAC address, destination MAC address, and IP address.

ARP packets that contain invalid IP addresses or MAC addresses in their body that do not match the addresses in the Ethernet header are dropped.

When dynamic ARP protection is enabled, only ARP request and reply packets with valid IP-to-MAC address bindings in their packet header are relayed and used to update the ARP cache.

Dynamic ARP protection is implemented in the following ways on a switch:

- You can configure dynamic ARP protection only from the CLI; you cannot configure this feature from the web or menu interfaces.
- Line rate—Dynamic ARP protection copies ARP packets to the switch CPU, evaluates the packets, and then re-forwards them through the switch software. During this process, if ARP packets are received at too high a line rate, some ARP packets may be dropped and will need to be retransmitted.
- The SNMP MIB, HP-ICF-ARP-PROTECT-MIB, is created to configure dynamic ARP protection and to report ARP packet-forwarding status and counters.

Enabling Dynamic ARP Protection

To enable dynamic ARP protection for VLAN traffic on a routing switch, enter the **arp-protect vlan** command at the global configuration level.

Syntax: [no] arp-protect vlan [*vlan-range*]

vlan-range *Specifies a VLAN ID or a range of VLAN IDs from one to 4094; for example, 1–200.*

An example of the **arp-protect vlan** command is shown here:

```
ProCurve(config)# arp-protect vlan 1-101
```

Configuring Trusted Ports

In a similar way to DHCP snooping, dynamic ARP protection allows you to configure VLAN interfaces in two categories: trusted and untrusted ports. ARP packets received on trusted ports are forwarded without validation.

By default, all ports on a switch are untrusted. If a VLAN interface is untrusted:

- The switch intercepts all ARP requests and responses on the port.
- Each intercepted packet is checked to see if its IP-to-MAC binding is valid. If a binding is invalid, the switch drops the packet.

You must configure trusted ports carefully. For example, in the topology in Figure 11-9, Switch B may not see the leased IP address that Host 1 receives from the DHCP server. If the port on Switch B that is connected to Switch A is untrusted and if Switch B has dynamic ARP protection enabled, it will see ARP packets from Host 1 as invalid, resulting in a loss of connectivity.

On the other hand, if Switch A does not support dynamic ARP protection and you configure the port on Switch B connected to Switch A as trusted, Switch B opens itself to possible ARP poisoning from hosts attached to Switch A.

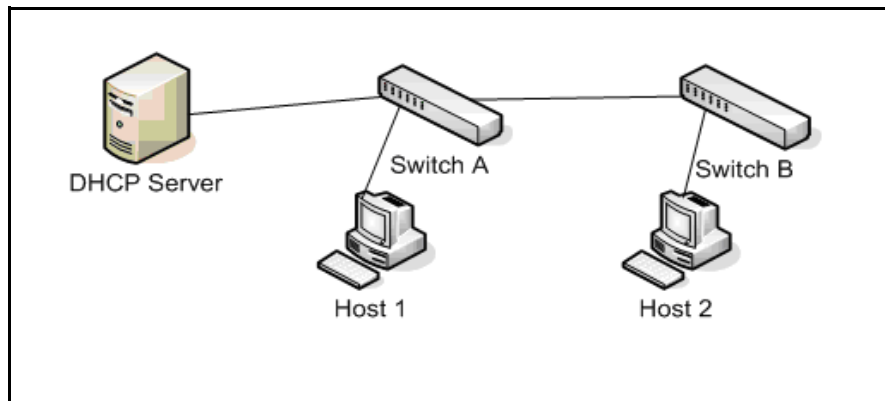


Figure 11-9. Configuring Trusted Ports for Dynamic ARP Protection

Take into account the following configuration guidelines when you use dynamic ARP protection in your network:

- You should configure ports connected to other switches in the network as trusted ports. In this way, all network switches can exchange ARP packets and update their ARP caches with valid information.
- Switches that do not support dynamic ARP protection should be separated by a router in their own Layer 2 domain. Because ARP packets do not cross Layer 2 domains, the unprotected switches cannot unknowingly accept ARP packets from an attacker and forward them to protected switches through trusted ports.

To configure one or more Ethernet interfaces that handle VLAN traffic as trusted ports, enter the **arp-protect trust** command at the global configuration level. The switch does not check ARP requests and responses received on a trusted port.

Syntax: [no] arp-protect trust <port-list>

port-list Specifies a port number or a range of port numbers. Separate individual port numbers or ranges of port numbers with a comma; for example: **c1-c3, c6**.

An example of the **arp-protect trust** command is shown here:

```
ProCurve(config)# arp-protect trust b1-b4, d1
```

Adding an IP-to-MAC Binding to the DHCP Database

A routing switch maintains a DHCP binding database, which is used for DHCP and ARP packet validation. Both the DHCP snooping and DHCP Option 82 insertion features maintain the lease database by learning the IP-to-MAC bindings on untrusted ports. Each binding consists of the client MAC address, port number, VLAN identifier, leased IP address, and lease time.

If your network does not use DHCP or if some network devices have fixed, user-configured IP addresses, you can enter static IP-to-MAC address bindings in the DHCP binding database. The switch uses manually configured static bindings for DHCP snooping and dynamic ARP protection.

To add the static configuration of an IP-to-MAC binding for a port to the database, enter the **ip source-binding** command at the global configuration level.

Syntax: [no] ip source-binding <mac-address> vlan <vlan-id> <ip-address>
interface <port-number>

mac-address Specifies a MAC address to bind with a VLAN and IP address on the specified port in the DHCP binding database.

vlan <vlan-id> Specifies a VLAN ID number to bind with the specified MAC and IP addresses on the specified port in the DHCP binding database.

ip-address Specifies an IP address to bind with a VLAN and MAC address on the specified port in the DHCP binding database.

interface <port-number> Specifies the port number on which the IP-to-MAC address and VLAN binding is configured in the DHCP binding database.

An example of the **ip source-binding** command is shown here:

```
ProCurve(config)# ip source-binding 0030c1-7f49c0  
interface vlan 100 10.10.20.1 interface A4
```

Note

Note that the **ip source-binding** command is the same command used by the Dynamic IP Lockdown feature to configure static bindings. The Dynamic ARP Protection and Dynamic IP Lockdown features share a common list of source IP-to-MAC bindings.

Configuring Additional Validation Checks on ARP Packets

Dynamic ARP protection can be configured to perform additional validation checks on ARP packets. By default, no additional checks are performed. To configure additional validation checks, enter the **arp-protect validate** command at the global configuration level.

Syntax: [no] arp-protect validate <[src-mac] | [dst-mac] | [ip]>

- src-mac** *(Optional) Drops any ARP request or response packet in which the source MAC address in the Ethernet header does not match the sender MAC address in the body of the ARP packet.*
- dst-mac** *(Optional) Drops any unicast ARP response packet in which the destination MAC address in the Ethernet header does not match the target MAC address in the body of the ARP packet.*
- ip** *(Optional) Drops any ARP packet in which the sender IP address is invalid. Drops any ARP response packet in which the target IP address is invalid. Invalid IP addresses include: 0.0.0.0, 255.255.255.255, all IP multicast addresses, and all Class E IP addresses.*

You can configure one or more of the validation checks. The following example of the **arp-protect validate** command shows how to configure the validation checks for source MAC address and destination MAC address:

```
ProCurve(config)# arp-protect validate src-mac dst-mac
```

Verifying the Configuration of Dynamic ARP Protection

To display the current configuration of dynamic ARP protection, including the additional validation checks and the trusted ports that are configured, enter the **show arp-protect** command:

```
ProCurve(config)# show arp-protect

ARP Protection Information

Enabled Vlans   : 1-4094
Validate       : dst-mac, src-mac

Port   Trust
-----
B1     Yes
B2     Yes
B3     No
B4     No
B5     No
```

Figure 11-1. The show arp-protect Command

Displaying ARP Packet Statistics

To display statistics about forwarded ARP packets, dropped ARP packets, MAC validation failure, and IP validation failures, enter the **show arp-protect statistics** command:

```
ProCurve(config)# show arp-protect statistics

Status and Counters - ARP Protection Counters for VLAN 1

Forwarded pkts   : 10      Bad source mac      : 2
Bad bindings     : 1       Bad destination mac: 1
Malformed pkts  : 0       Bad IP address      : 0

Status and Counters - ARP Protection Counters for VLAN 2

Forwarded pkts   : 1       Bad source mac      : 1
Bad bindings     : 1       Bad destination mac: 1
Malformed pkts  : 1       Bad IP address      : 1
```

Figure 11-2. Show arp-protect statistics Command

Monitoring Dynamic ARP Protection

When dynamic ARP protection is enabled, you can monitor and troubleshoot the validation of ARP packets with the **debug arp-protect** command. Use this command when you want to debug the following conditions:

- The switch is dropping valid ARP packets that should be allowed.
- The switch is allowing invalid ARP packets that should be dropped.

```
ProCurve(config)# debug arp-protect

1. ARP request is valid
"DARPP: Allow ARP request 000000-000001,10.0.0.1 for 10.0.0.2 port A1,
vlan "

2. ARP request detected with an invalid binding
"DARPP: Deny ARP request 000000-000003,10.0.0.1 port A1, vlan 1"

3. ARP response with a valid binding
"DARPP: Allow ARP reply 000000-000002,10.0.0.2 port A2, vlan 1"

4. ARP response detected with an invalid binding
"DARPP: Deny ARP reply 000000-000003,10.0.0.2 port A2, vlan 1"
```

Figure 11-3. Example of debug arp-protect Command

Dynamic IP Lockdown

The Dynamic IP Lockdown feature is used to prevent IP source address spoofing on a per-port and per-VLAN basis. When dynamic IP lockdown is enabled, IP packets in VLAN traffic received on a port are forwarded only if they contain a known source IP address and MAC address binding for the port. The IP-to-MAC address binding can either be statically configured or learned by the DHCP Snooping feature.

Protection Against IP Source Address Spoofing

Many network attacks occur when an attacker injects packets with forged IP source addresses into the network. Also, some network services use the IP source address as a component in their authentication schemes. For example, the BSD “r” protocols (rlogin, rcp, rsh) rely on the IP source address for packet authentication. SNMPv1 and SNMPv2c also frequently use authorized IP address lists to limit management access. An attacker that is able to send traffic that appears to originate from an authorized IP source address may gain access to network services for which he is not authorized.

Dynamic IP lockdown provides protection against IP source address spoofing by means of IP-level port security. IP packets received on a port enabled for dynamic IP lockdown are only forwarded if they contain a known IP source address and MAC address binding for the port.

Dynamic IP lockdown uses information collected in the DHCP Snooping lease database and through statically configured IP source bindings to create internal, per-port lists. The internal lists are dynamically created from known IP-to-MAC address bindings to filter VLAN traffic on both the source IP address and source MAC address.

Prerequisite: DHCP Snooping

Dynamic IP lockdown requires that you enable DHCP snooping as a prerequisite for its operation on ports and VLAN traffic:

- Dynamic IP lockdown only enables traffic for clients whose leased IP addresses are already stored in the lease database created by DHCP snooping or added through a static configuration of an IP-to-MAC binding.

Therefore, if you enable DHCP snooping after dynamic IP lockdown is enabled, clients with an existing DHCP-assigned address must either request a new leased IP address or renew their existing DHCP-assigned address. Otherwise, a client's leased IP address is not contained in the DHCP binding database. As a result, dynamic IP lockdown will not allow inbound traffic from the client.

- It is recommended that you enable DHCP snooping a week before you enable dynamic IP lockdown to allow the DHCP binding database to learn clients' leased IP addresses. You must also ensure that the lease time for the information in the DHCP binding database lasts more than a week.

Alternatively, you can configure a DHCP server to re-allocate IP addresses to DHCP clients. In this way, you repopulate the lease database with current IP-to-MAC bindings.

- The DHCP binding database allows VLANs enabled for DHCP snooping to be known on ports configured for dynamic IP lockdown. As new IP-to-MAC address and VLAN bindings are learned, a corresponding permit rule is dynamically created and applied to the port (preceding the final deny any vlan <VLAN_IDs> rule as shown in the example in Figure 11-4. These VLAN_IDs correspond to the subset of configured and enabled VLANS for which DHCP snooping has been configured.
- For dynamic IP lockdown to work, a port must be a member of at least one VLAN that has DHCP snooping enabled.
- Disabling DHCP snooping on a VLAN causes Dynamic IP bindings on Dynamic IP Lockdown-enabled ports in this VLAN to be removed. The port reverts back to switching traffic as usual.

Filtering IP and MAC Addresses Per-Port and Per-VLAN

This section contains an example that shows the following aspects of the Dynamic IP Lockdown feature:

- Internal Dynamic IP lockdown bindings dynamically applied on a per-port basis from information in the DHCP Snooping lease database and statically configured IP-to-MAC address bindings
- Packet filtering using source IP address, source MAC address, and source VLAN as criteria

In this example, the following DHCP leases have been learned by DHCP snooping on port 5. VLANs 2 and 5 are enabled for DHCP snooping.

Table 1. Sample DHCP Snooping Entries

IP Address	MAC Address	VLAN ID
10.0.8.5	001122-334455	2
10.0.8.7	001122-334477	2
10.0.10.3	001122-334433	5

The following example shows an IP-to-MAC address and VLAN binding that have been statically configured in the lease database on port 5.

IP Address	MAC Address	VLAN ID
10.0.10.1	001122-110011	5

Assuming that DHCP snooping is enabled and that port 5 is untrusted, dynamic IP lockdown applies the following dynamic VLAN filtering on port 5:

```
permit 10.0.8.5 001122-334455 vlan 2
permit 10.0.8.7 001122-334477 vlan 2
permit 10.0.10.3 001122-334433 vlan 5
permit 10.0.10.1 001122-110011 vlan 5
deny any vlan 1-10
permit any
```

Figure 11-4. Example of Internal Statements used by Dynamic IP Lockdown

Note that the **deny any** statement is applied only to VLANs for which DHCP snooping is enabled. The **permit any** statement is applied only to all other VLANs.

Enabling Dynamic IP Lockdown

To enable dynamic IP lockdown on all ports or specified ports, enter the **ip source-lockdown** command at the global configuration level. Use the **no** form of the command to disable dynamic IP lockdown.

Syntax: [no] ip source-lockdown <port-list>

Enables dynamic IP lockdown globally on all ports or on specified ports on the routing switch.

Operating Notes

- Dynamic IP lockdown is enabled at the port configuration level and applies to all bridged or routed IP packets entering the switch. The only IP packets that are exempt from dynamic IP lockdown are broadcast DHCP request packets, which are handled by DHCP snooping.
- DHCP snooping is a prerequisite for Dynamic IP Lockdown operation. The following restrictions apply:
 - DHCP snooping is required for dynamic IP lockdown to operate. To enable DHCP snooping, enter the **dhcp-snooping** command at the global configuration level.

- Dynamic IP lockdown only filters packets in VLANs that are enabled for DHCP snooping. In order for Dynamic IP lockdown to work on a port, the port must be configured for at least one VLAN that is enabled for DHCP snooping.

To enable DHCP snooping on a VLAN, enter the **dhcp-snooping vlan** [*vlan-id-range*] command at the global configuration level or the **dhcp-snooping** command at the VLAN configuration level.

- Dynamic IP lockdown is not supported on a trusted port. (However, note that the DHCP server must be connected to a trusted port when DHCP snooping is enabled.)

By default, all ports are untrusted. To remove the trusted configuration from a port, enter the **no dhcp-snooping trust** <*port-list*> command at the global configuration level.

For more information on how to configure and use DHCP snooping, see “DHCP Snooping” on page 11-4.

- After you enter the **ip source-lockdown** command (enabled globally with the desired ports entered in <*port-list*>), the dynamic IP lockdown feature remains disabled on a port if any of the following conditions exist:
 - If DHCP snooping has not been globally enabled on the switch.
 - If the port is not a member of at least one VLAN that is enabled for DHCP snooping.
 - If the port is configured as a trusted port for DHCP snooping.

Dynamic IP lockdown is activated on the port only after you make the following configuration changes:

- Enable DHCP snooping on the switch.
- Configure the port as a member of a VLAN that has DHCP snooping enabled.
- Remove the trusted-port configuration.
- You can configure dynamic IP lockdown only from the CLI; this feature cannot be configured from the web management or menu interface.
- If you enable dynamic IP lockdown on a port, you cannot add the port to a trunk.
- Dynamic IP lockdown must be removed from a trunk before the trunk is removed.

Adding an IP-to-MAC Binding to the DHCP Binding Database

A switch maintains a DHCP binding database, which is used for dynamic IP lockdown as well as for DHCP and ARP packet validation. The DHCP snooping feature maintains the lease database by learning the IP-to-MAC bindings of VLAN traffic on untrusted ports. Each binding consists of the client MAC address, port number, VLAN identifier, leased IP address, and lease time.

Dynamic IP lockdown supports a total of 4K static and dynamic bindings with up to 64 bindings per port. When DHCP snooping is enabled globally on a VLAN, dynamic bindings are learned when a client on the VLAN obtains an IP address from a DHCP server. Static bindings are created manually with the CLI or from a downloaded configuration file.

When dynamic IP lockdown is enabled globally or on ports the bindings associated with the ports are written to hardware. This occurs during these events:

- Switch initialization
- Hot swap
- A dynamic IP lockdown-enabled port is moved to a DHCP snooping-enabled VLAN
- DHCP snooping or dynamic IP lockdown characteristics are changed such that dynamic IP lockdown is enabled on the ports

Potential Issues with Bindings

- When dynamic IP lockdown is enabled, and a port or switch has the maximum number of bindings configured, the client DHCP request will be dropped and the client will not receive an IP address through DHCP.
- When dynamic IP lockdown is enabled and a port is configured with the maximum number of bindings, adding a static binding to the port will fail.
- When dynamic IP lockdown is enabled globally, the bindings for each port are written to hardware. If global dynamic IP lockdown is enabled and disabled several times, it is possible to run out of buffer space for additional bindings. The software will delay adding the bindings to hardware until resources are available.

Adding a Static Binding

To add the static configuration of an IP-to-MAC binding for a port to the lease database, enter the **ip source-binding** command at the global configuration level. Use the **no** form of the command to remove the IP-to-MAC binding from the database.

Syntax: [no] ip source-binding <vlan-id> <ip-address> <mac-address> <port-number>

<i>vlan-id</i>	<i>Specifies a valid VLAN ID number to bind with the specified MAC and IP addresses on the port in the DHCP binding database.</i>
<i>ip-address</i>	<i>Specifies a valid client IP address to bind with a VLAN and MAC address on the port in the DHCP binding database.</i>
<i>mac-address</i>	<i>Specifies a valid client MAC address to bind with a VLAN and IP address on the port in the DHCP binding database.</i>
<i>port-number</i>	<i>Specifies the port number on which the IP-to-MAC address and VLAN binding is configured in the DHCP binding database.</i>

Note

Note that the **ip source-binding** command is the same command used by the Dynamic ARP Protection feature to configure static bindings. The Dynamic ARP Protection and Dynamic IP Lockdown features share a common list of source IP-to-MAC address bindings.

Verifying the Dynamic IP Lockdown Configuration

To display the ports on which dynamic IP lockdown is configured, enter the **show ip source-lockdown status** command at the global configuration level.

Syntax: show ip source-lockdown status

An example of the **show ip source-lockdown status** command output is shown in Figure 11-5. Note that the operational status of all switch ports is displayed. This information indicates whether or not dynamic IP lockdown is supported on a port.

```
ProCurve(config)# show ip source-lockdown status
Dynamic IP Lockdown (DIPLD) Information

Global State: Enabled

      Port      Operational State
-----
A1      Active
A2      Not in DHCP Snooping vlan
A3      Disabled
A4      Disabled
A5      Trusted port, Not in DHCP Snooping vlan
. . . . .
```

Figure 11-5. Example of show ip source-lockdown status Command Output

Displaying the Static Configuration of IP-to-MAC Bindings

To display the static configurations of IP-to-MAC bindings stored in the DHCP lease database, enter the **show ip source-lockdown bindings** command.

Syntax: show ip source-lockdown bindings [*port-number*]

port-number (Optional) Specifies the port number on which source IP-to-MAC address and VLAN bindings are configured in the DHCP lease database.

An example of the **show ip source-lockdown bindings** command output is shown in Figure 11-6.

```
ProCurve(config)# show ip source-lockdown bindings

Dynamic IP Lockdown (DIPLD) Bindings

Mac Address      IP Address      VLAN    Port    Not in HW
-----
001122-334455   10.10.10.1     1111   X11
005544-332211   10.10.10.2     2222   Trk11   YES
. . . . .
```

Figure 11-6. Example of show ip source-lockdown bindings Command Output

In the **show ip source-lockdown bindings** command output, the “Not in HW” column specifies whether or not (YES or NO) a statically configured IP-to-MAC and VLAN binding on a specified port has been combined in the lease database maintained by the DHCP Snooping feature.

Debugging Dynamic IP Lockdown

To enable the debugging of packets dropped by dynamic IP lockdown, enter the **debug dynamic-ip-lockdown** command.

Syntax: debug dynamic-ip-lockdown

To send command output to the active CLI session, enter the **debug destination session** command.

Counters for denied packets are displayed in the **debug dynamic-ip-lockdown** command output. Packet counts are updated every five minutes. An example of the command output is shown in Figure 11-7.

When dynamic IP lockdown drops IP packets in VLAN traffic that do not contain a known source IP-to-MAC address binding for the port on which the packets are received, a message is entered in the event log.

```
ProCurve(config)# debug dynamic-ip-lockdown

DIPLD 01/01/90 00:01:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 1 packets
DIPLD 01/01/90 00:06:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 294 packets
DIPLD 01/01/90 00:11:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 300 packets
DIPLD 01/01/90 00:16:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 300 packets
DIPLD 01/01/90 00:21:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 299 packets
DIPLD 01/01/90 00:26:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 300 packets
DIPLD 01/01/90 00:31:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 300 packets
DIPLD 01/01/90 00:36:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 299 packets
DIPLD 01/01/90 00:41:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 300 packets
```

Figure 11-7. Example of debug dynamic-ip-lockdown Command Output

Differences Between Switch Platforms

There are some differences in the feature set and operation of Dynamic IP Lockdown, depending on the switch on which it is implemented. These are listed below.

- There is no restriction on GVRP on 3500/5400 switches. On 2600/2800/3400 switches, Dynamic IP Lockdown is not supported if GVRP is enabled on the switch.
- Dynamic IP Lockdown has the host limits shown in the table below. There is a DHCP snooping limit of 8,192 entries.

Configuring Advanced Threat Protection

Dynamic IP Lockdown

Switch	Number of Hosts	Comments
3500/5400	64 bindings per port Up to 4096 manual bindings per switch	This limit is shared with DHCP snooping because they both use the snooping database.
3400/2800	32 bindings per port; up to 512 manual bindings Up to 32 VLANs with DHCP snooping enabled	This is not guaranteed as the hardware resources are shared with QoS.
2610	8 bindings per port; up to 512 manual bindings Globally 118 to 125 hosts Up to 8 VLANs with DHCP snooping enabled	This is not guaranteed as the hardware resources are shared with IDM ACLs. The number of global bindings available is based on the number of DHCP snooping-enabled VLANs (1-8).
2600	8 bindings per port; up to 512 manual bindings Up to 8 VLANs with DHCP snooping enabled	This is not guaranteed as the hardware resources are shared with QoS.

- A source is considered “trusted” for all VLANs if it is seen on any VLAN without DHCP snooping enabled.
- On the ProCurve switch series 5400 and 3500, dynamic IP lockdown is supported on a port configured for statically configured port-based ACLs.

Using the Instrumentation Monitor

The instrumentation monitor can be used to detect anomalies caused by security attacks or other irregular operations on the switch. The following table shows the operating parameters that can be monitored at pre-determined intervals, and the possible security attacks that may trigger an alert:

Parameter Name	Description
pkts-to-closed-ports	The count of packets per minute sent to closed TCP/UDP ports. An excessive amount of packets could indicate a port scan, in which an attacker is attempting to expose a vulnerability in the switch.
arp-requests	The count of ARP requests processed per minute. A large amount of ARP request packets could indicate a host infected with a virus that is trying to spread itself.
ip-address-count	The number of destination IP addresses learned in the IP forwarding table. Some attacks fill the IP forwarding table causing legitimate traffic to be dropped.
system-resource-usage	The percentage of system resources in use. Some Denial-of-Service (DoS) attacks will cause excessive system resource usage, resulting in insufficient resources for legitimate traffic.
login-failures/min	The count of failed CLI login attempts or SNMP management authentication failures. This indicates an attempt has been made to manage the switch with an invalid login or password. Also, it might indicate a network management station has not been configured with the correct SNMP authentication parameters for the switch.
port-auth-failures/min	The count of times a client has been unsuccessful logging into the network
system-delay	The response time, in seconds, of the CPU to new network events such as BPDUs or packets for other network protocols. Some DoS attacks can cause the CPU to take too long to respond to new network events, which can lead to a breakdown of Spanning Tree or other features. A delay of several seconds indicates a problem.
mac-address-count	The number of MAC addresses learned in the forwarding table. Some attacks fill the forwarding table so that new conversations are flooded to all parts of the network.
mac-moves/min	The average number of MAC address moves from one port to another per minute. This usually indicates a network loop, but can also be caused by DoS attacks.
learn-discards/min	Number of MAC address learn events per minute discarded to help free CPU resources when busy.

Operating Notes

- To generate alerts for monitored events, you must enable the instrumentation monitoring log and/or SNMP trap. The threshold for each monitored parameter can be adjusted to minimize false alarms (see “Configuring Instrumentation Monitor” on page 11-37).
- When a parameter exceeds its threshold, an alert (event log message and/or SNMP trap) is generated to inform network administrators of this condition. The following example shows an event log message that occurs when the number of MAC addresses learned in the forwarding table exceeds the configured threshold:

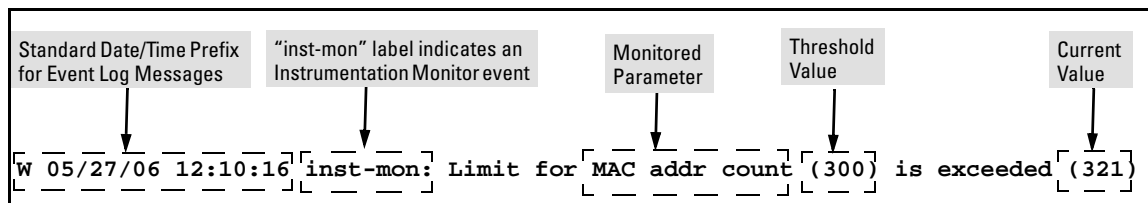


Figure 11-8. Example of Event Log Message generated by Instrumentation Monitor

- Alerts are automatically rate limited to prevent filling the log file with redundant information. The following is an example of alerts that occur when the device is continually subject to the same attack (too many MAC addresses in this instance):

```
W 01/01/90 00:05:00 inst-mon: Limit for MAC addr count (300) is exceeded (321)
W 01/01/90 00:10:00 inst-mon: Limit for MAC addr count (300) is exceeded (323)
W 01/01/90 00:15:00 inst-mon: Limit for MAC addr count (300) is exceeded (322)
W 01/01/90 00:20:00 inst-mon: Limit for MAC addr count (300) is exceeded (324)
W 01/01/90 00:20:00 inst-mon: Ceasing logs for MAC addr count for 15 minutes
```

Figure 11-9. Example of rate limiting when multiple messages are generated

In the preceding example, if a condition is reported 4 times (persists for more than 15 minutes) then alerts cease for 15 minutes. If after 15 minutes the condition still exists, the alerts cease for 30 minutes, then for 1 hour, 2 hours, 4 hours, 8 hours, and after that the persisting condition is reported once a day. As with other event log entries, these alerts can be sent to a syslog server.

- **Known Limitations:** The instrumentation monitor runs once every five minutes. The current implementation does not track information such as the port, MAC, and IP address from which an attack is received.

Configuring Instrumentation Monitor

The following commands and parameters are used to configure the operational thresholds that are monitored on the switch. By default, the instrumentation monitor is disabled.

Syntax: [no] instrumentation monitor [parameterName|all] [<low|med|high|limitValue>]

[log] : Enables/disables instrumentation monitoring log so that event log messages are generated every time there is an event which exceeds a configured threshold.

(Default threshold setting when instrumentation monitoring is enabled: **enabled**)

[all] : Enables/disables all counter types on the switch but does not enable/disable instrumentation monitor logging.

(Default threshold setting when enabled: **see parameter listings below**)

[arp-requests] : The number of arp requests that are processed each minute.

(Default threshold setting when enabled: **1000 (med)**)

[ip-address-count]: The number of destination IP addresses learned in the IP forwarding table.

(Default threshold setting when enabled: **1000 (med)**)

[learn-discards]: The number of MAC address learn events per minute discarded to help free CPU resources when busy.

(Default threshold setting when enabled: **100 (med)**)

[login-failures]: The count of failed CLI login attempts or SNMP management authentication failures per hour.

(Default threshold setting when enabled: **10 (med)**)

[mac-address-count] : The number of MAC addresses learned in the forwarding table. You must enter a specific value in order to enable this feature.

(Default threshold setting when enabled: **1000 (med)**)

[mac-moves] : The average number of MAC address moves per minute from one port to another.

(Default threshold setting when enabled: **100 (med)**)

[pkts-to-closed-ports] : The count of packets per minute sent to closed TCP/UDP ports.

(Default threshold setting when enabled: **10 (med)**)

[port-auth-failures] : The count of times per minute that a client has been unsuccessful logging into the network.

(Default threshold setting when enabled: **10 (med)**)

[system-resource-usage]: The percentage of system resources in use.

(Default threshold setting when enabled: **50 (med)**)

[system-delay] : The response time, in seconds, of the CPU to new network events such as BPDU packets or packets for other network protocols.

(Default threshold setting when enabled: **3 seconds (med)**)

[trap] : Enables or disables SNMP trap generation.

(Default setting when instrumentation monitoring is enabled: **disabled**)

To enable instrumentation monitor using the default parameters and thresholds, enter the general **instrumentation monitor** command. To adjust specific settings, enter the name of the parameter that you wish to modify, and revise the threshold limits as needed.

Examples

To turn on monitoring and event log messaging with the default medium values:

```
ProCurve(config)# instrumentation monitor
```

To turn off monitoring of the system delay parameter:

```
ProCurve(config)# no instrumentation monitor system-  
delay
```

To adjust the alert threshold for the MAC address count to the low value:

```
ProCurve(config)# instrumentation monitor mac-  
address-count low
```

To adjust the alert threshold for the MAC address count to a specific value:

```
ProCurve(config)# instrumentation monitor mac-  
address-count 767
```

To enable monitoring of learn discards with the default medium threshold value:

```
ProCurve(config)# instrumentation monitor learn-  
discards
```

To disable monitoring of learn discards:

```
ProCurve(config)# no instrumentation monitor learn-  
discards
```

To enable or disable SNMP trap generation:

```
ProCurve(config)# [no] instrumentation monitor trap
```

Viewing the Current Instrumentation Monitor Configuration

The **show instrumentation monitor configuration** command displays the configured thresholds for monitored parameters.

```
ProCurve# show instrumentation monitor configuration
```

PARAMETER	LIMIT
mac-address-count	1000 (med)
ip-address-count	1000 (med)
system-resource-usage	50 (med)
system-delay	5 (high)
mac-moves/min	100 (med)
learn-discards/min	100 (med)
ip-port-scans/min	10 (med)
arp-requests/min	100 (low)
login-failures/min	10 (med)
port-auth-failures/min	10 (med)

```
SNMP trap generation for alerts: enabled  
Instrumentation monitoring log : enabled
```

Figure 11-10. Viewing the Instrumentation Monitor Configuration

An alternate method of determining the current Instrumentation Monitor configuration is to use the **show run** command. However, the show run command output does not display the threshold values for each limit set.

Configuring Advanced Threat Protection
Using the Instrumentation Monitor