DHCP Snooping
Mini Primer on DHCP (RFC 2131 and 2132)

- Centralized administration of IP address config
- Superset of BootP Client/Server protocol
- Temporary allocation of IP address and options based on MAC, Client ID, or subnet (GIADDR)
- Transport: UDP, port 67 (server listens on this port) and 68 (client listens on this port)
- Lease renewal efforts occur at two intervals:
  - T1 – 1/2 of the lease has been used
  - T2 – 7/8 of the lease has been used
DHCP Address Acquisition

DHCP Discover: sent out as Layer2 broadcast
DHCP Offer: Server responds with a proposal of parameters
DHCP Request: the client broadcasts to the preferred server. An implicit decline to others.
DHCP ACK: the server assigns an IP address
DHCP NACK: the server rejects the request from the client
DHCP Release: the client returns the assigned address before lease expires
DHCP Decline: the client rejects the offered address

NOTE: The reply from server may contain not only the client's Layer3 address (IP Address) but also other important configuration parameters such as the subnet mask, default router and Domain Name System (DNS) server. The DHCP ACK contains the all necessary IP/Lease parameters (DNS server, WINS server, NetBIOS Node type, domain name, T1/T2 timers, Gateway, etc.).
DHCP Discover (client-to-server)

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol - Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>39:21:484968</td>
<td>171.69.80.2</td>
<td>171.69.81.42</td>
<td>DHCP DHCP Offer - Transaction 10 607ab0b20</td>
</tr>
<tr>
<td>39:21:484968</td>
<td>171.69.80.2</td>
<td>171.69.81.42</td>
<td>DHCP DHCP Offer - Transaction 10 607ab0b20</td>
</tr>
<tr>
<td>39:15:92337</td>
<td>0.0.0.1</td>
<td>255.255.255.255</td>
<td>DHCP DHCP Request - Transaction 10 607ab0b20</td>
</tr>
<tr>
<td>40:15:92337</td>
<td>171.69.80.2</td>
<td>171.69.81.48</td>
<td>DHCP DHCP Offer - Transaction 10 607ab0b20</td>
</tr>
<tr>
<td>41:15:92337</td>
<td>171.69.80.2</td>
<td>171.69.81.48</td>
<td>DHCP DHCP Offer - Transaction 10 607ab0b20</td>
</tr>
<tr>
<td>42:15:92337</td>
<td>171.69.80.2</td>
<td>171.69.81.48</td>
<td>DHCP DHCP Offer - Transaction 10 607ab0b20</td>
</tr>
</tbody>
</table>

This is the last IP Address I had. In this case it was a static IP address I assigned before I changed it over to "dynamic" to force the DHCP process.
DHCP Offer (server-to-client)

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>18:42:06.005</td>
<td>0.0.0.0</td>
<td>172.255.255.255</td>
<td>DHCP</td>
<td>DHCP Offer - Transaction ID 0x7da800</td>
</tr>
<tr>
<td>18:42:06.005</td>
<td>0.0.0.0</td>
<td>172.255.255.255</td>
<td>DHCP</td>
<td>DHCP Offer - Transaction ID 0x7da800</td>
</tr>
<tr>
<td>18:42:06.005</td>
<td>0.0.0.0</td>
<td>172.255.255.255</td>
<td>DHCP</td>
<td>DHCP Offer - Transaction ID 0x7da800</td>
</tr>
<tr>
<td>18:42:06.005</td>
<td>0.0.0.0</td>
<td>172.255.255.255</td>
<td>DHCP</td>
<td>DHCP Offer - Transaction ID 0x7da800</td>
</tr>
<tr>
<td>18:42:06.005</td>
<td>0.0.0.0</td>
<td>172.255.255.255</td>
<td>DHCP</td>
<td>DHCP Offer - Transaction ID 0x7da800</td>
</tr>
<tr>
<td>18:42:06.005</td>
<td>0.0.0.0</td>
<td>172.255.255.255</td>
<td>DHCP</td>
<td>DHCP Offer - Transaction ID 0x7da800</td>
</tr>
<tr>
<td>18:42:06.005</td>
<td>0.0.0.0</td>
<td>172.255.255.255</td>
<td>DHCP</td>
<td>DHCP Offer - Transaction ID 0x7da800</td>
</tr>
</tbody>
</table>

Time 36 (JSL bytes on wire, JSL bytes captured)


Internet protocol, src 172.69.68.2 (172.69.68.2), dst 172.69.68.4 (172.69.68.4)

User Datagram Protocol, src Port: bootps (67), dest Port: bootps (68)

bootp protocol

Message type: BOOTREPLY (2)

Hardware type: ethernet

Hardware address length: 6

Hops: 0

Transaction Id: 0x7da80020

seconds elapsed: 0

Bootp flags: 0x0000 (unicast)

Client IP address: 0.0.0.0 (0.0.0.0)

Your (client) IP address: 172.69.68.4 (172.69.68.4)

Next server IP address: 172.69.68.4 (172.69.68.4)

Relay agent IP address: 172.69.68.4 (172.69.68.4)

Client MAC address: Foxconn-na-6520r (00:02:65:65:65:65)

Server host name not given

Root File name: /dhcp/udpboot/udboot0

Magic cookie: 0x00

Option 53: DHCP Message Type = DHCP Offer

Option 54: Server Identifier = 172.69.10.69

Option 51: IP Address Lease Time = 2 days, 18 hours, 40 minutes, 35 seconds

Option 11: Subnet Mask = 255.255.255.0

Option 15: Domain Name = "cisco.com"

Option 31: Router = 172.69.68.1

Option 6: Domain Name Server

Option 44: Hostname over TCP/IP Name Server

Option 60: Vendor-Specific Option (vendor: 0118, 0201)

© 2000 Cisco Systems, Inc. All rights reserved.
DHCP Request (client-to-server)

<table>
<thead>
<tr>
<th>Seq</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>37</td>
<td>15:56:55</td>
<td>0.0.0.0</td>
<td>255.255.255.255</td>
<td>DHCP</td>
<td>DHCP DISCOVER - Transaction ID 0x75-da-b890</td>
</tr>
<tr>
<td>38</td>
<td>15:56:59</td>
<td>255.255.255.255</td>
<td>172.0.0.0</td>
<td>DHCP</td>
<td>DHCP OFFER - Transaction ID 0x75-da-b890</td>
</tr>
<tr>
<td>39</td>
<td>15:57:03</td>
<td>172.0.0.0</td>
<td>172.0.0.0</td>
<td>DHCP</td>
<td>DHCP ACK - Transaction ID 0x75-da-b890</td>
</tr>
<tr>
<td>40</td>
<td>15:57:03</td>
<td>0.0.0.0</td>
<td>172.0.0.0</td>
<td>DHCP</td>
<td>DHCP ACK - Transaction ID 0x75-da-b890</td>
</tr>
<tr>
<td>41</td>
<td>15:57:04</td>
<td>172.0.0.0</td>
<td>172.0.0.0</td>
<td>DHCP</td>
<td>DHCP ACK - Transaction ID 0x75-da-b890</td>
</tr>
<tr>
<td>42</td>
<td>15:58:10</td>
<td>172.0.0.0</td>
<td>172.0.0.0</td>
<td>DHCP</td>
<td>DHCP ACK - Transaction ID 0x75-da-b890</td>
</tr>
</tbody>
</table>

Frame 39 (578 bytes on wire, 378 bytes captured):

Ethernet II, Src: 00:11:ac:6c:6a:28 (00:11:ac:6c:6a:28), Dest: broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dest: 255.255.255.255 (255.255.255.255)
User datagram protocol, Src Port: bootpc (68), Dest Port: bootps (67)

BOOTP/BOOTPROTOCOL:
Message type: Boot Request (1)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x75-da-b890
Seconds elapsed: 0
Boots flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (Client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Server IP address: 0.0.0.0 (0.0.0.0)
Server host name not given
Boot file name not given
Magic cookie: (cm)

Option 53: DHCP Message Type = DHCP Request
Option 60: Client Identifier
Option 54: Requested IP Address = 172.0.0.43
Option 51: Server Identifier = 172.55.30.0
Option 52: Host Name = "kboegart-wxp64"
Option 54: File
Option 60: Vendor Class Identifier = "NSFT 5.0"
Option 55: Parameter Request List

© 2003, Cisco Systems, Inc. All rights reserved.
Duplicate packets??

- Why do you think my laptop was sent TWO DHCP Offers?

<table>
<thead>
<tr>
<th>Frame 40 (311 bytes on wire, 311 bytes captured)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Protocol, Src: 172.69.60.2, Dst: 172.69.60.2, Src: 172.69.60.43 (172.69.60.43)</td>
</tr>
<tr>
<td>User Datagram Protocol, Src Port: 68688 (67), Dst Port: 6780 (80)</td>
</tr>
</tbody>
</table>

Bootstrap Protocol

Message Type: Boot Reply (2)
Hardware Type: Ethernet
Hardware Address Length: 6
Hops: 0
Transaction ID: 0x746a8029
Seconds Elapsed: 0

Boostrap Flags: 0x0000 (unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (Client) IP address: 172.69.61.43 (172.69.61.43)
Next server IP address: 172.69.61.43 (172.69.61.43)
Relay agent IP address: 172.69.61.43 (172.69.61.43)
Client MAC address: 0019:071e:6a7a:80 (0019:071e:6a7a:80)
Server boot name not given
Bootstrap file name: /x86tc/udp1/bstrap/bstrap.0
Magic cookie: 0x01 (ok)
Option 31: DHCP Message Type = DHCP Offer
Option 34: Server Identifier = 172.69.60.69
Option 51: IP Address Lease Time = 2 days, 18 hours, 46 minutes, 31 seconds
Option 11: Subnet Mask = 255.255.254.0
Option 13: Domain Name = "CISCO"
Option 3: Router = 172.69.60.1

© 2009, Cisco Systems, Inc. All rights reserved.
### DHCP ACK (server-to-client)

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Protocol</th>
<th>Port</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.69.92.3</td>
<td>00:0c:29:00:00:00</td>
<td>DHCP</td>
<td>67</td>
<td>68</td>
</tr>
<tr>
<td>172.69.92.2</td>
<td>00:0c:29:00:00:00</td>
<td>DHCP</td>
<td>67</td>
<td>68</td>
</tr>
<tr>
<td>172.69.92.1</td>
<td>00:0c:29:00:00:00</td>
<td>DHCP</td>
<td>67</td>
<td>68</td>
</tr>
</tbody>
</table>

**DHCP ACK (server-to-client)**

Message Type: Boot Reply (2)
Hardware Type: Ethernet
Hardware Address Length: 6
Hops: 0
Transaction ID: 0x7da40e29
seconds elapsed: 0
BOOTP Flags: 0x0000 (or/prot)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (Client) IP address: 172.69.92.43 (172.69.92.43)
Next server IP address: 172.69.92.43 (172.69.92.43)
Relay agent IP address: 172.69.92.43 (172.69.92.43)
Client MAC address: 00:0c:29:00:00:00 (00:0c:29:00:00:00)
Server host name not given
BOOTP lease name: /x86pc/und1/tbootstrap/0
Magic cookie: 0x63

Option 54: DHCP Message Type - DHCP ACK
Option 55: DHCP Server Identifier - 172.69.92.69
Option 56: IP Address Lease Time - 2 days, 18 hours, 40 minutes, 33 seconds
Option 57: Subnet Mask - 255.255.254.0
Option 61: Domain Name - x86pc.com
Option 63: Router - 172.69.92.1
Option 64: Domain Name Server
Option 66: NametoIP Name Server
Option 67: DNS Update over TCP/UDP Name Server

© 2003, Cisco Systems, Inc. All rights reserved.
Several DHCP message types…

Client messages:
- Discover
- Request (4 kinds):
  - selecting
  - renew
  - rebinding
  - Init/Reboot
- Decline
- Release
- Inform

Server messages:
- Offer
- ACK
- NAK

Message: DHCPDISCOVER  Use: Client broadcast to locate available servers.
DHCPREQUEST  Server to client in response to DHCPDISCOVER with offer of configuration parameters.
DHCPACK  Server to client with configuration parameters, including committed network address.
DHCPNAK  Server to client indicating client’s notion of network address is incorrect (e.g., client has moved to new subnet) or client’s lease as expired
DHCPDECLINE  Client to server indicating network address is already in use. Example: self-ARP detects offered IP address is already in use.
DHCPRELEASE  Client to server relinquishing network address and cancelling remaining lease.
DHCP Message Format

Description of fields in a DHCP message

<table>
<thead>
<tr>
<th>FIELD</th>
<th>OCTETS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>op</td>
<td>1</td>
<td>Message op code / message type.</td>
</tr>
<tr>
<td>htype</td>
<td>1</td>
<td>Hardware address type, see ARP Numbers&quot; RFC; e.g., '1' = 10mb ethernet.</td>
</tr>
<tr>
<td>section in &quot;Assigned ethernet.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hlen</td>
<td>1</td>
<td>Hardware address length (e.g. '6' for 10mb ethernet).</td>
</tr>
<tr>
<td>hops</td>
<td>1</td>
<td>Client sets to zero, optionally used by relay agents when booting via a relay agent.</td>
</tr>
<tr>
<td>xid</td>
<td>4</td>
<td>Transaction ID, a random number chosen by the client, used by the client and server to associate messages and responses between a client and a server.</td>
</tr>
<tr>
<td>secs</td>
<td>2</td>
<td>Filled in by client, seconds elapsed since client began address acquisition or renewal process.</td>
</tr>
<tr>
<td>flags</td>
<td>2</td>
<td>Flags</td>
</tr>
<tr>
<td>ciaddr</td>
<td>4</td>
<td>Client IP address; only filled in if client is in BOUND, RENEW or REBINDING state and can respond to ARP requests.</td>
</tr>
<tr>
<td>yiaddr</td>
<td>4</td>
<td>'your' (client) IP address.</td>
</tr>
<tr>
<td>Siaddr</td>
<td>4</td>
<td>IP address of next server to use in bootstrap; returned in DHCPoffer, DHCPACK by server.</td>
</tr>
<tr>
<td>giaddr</td>
<td>4</td>
<td>Relay agent IP address, used in booting via a relay agent.</td>
</tr>
<tr>
<td>chaddr</td>
<td>16</td>
<td>Client hardware address.</td>
</tr>
<tr>
<td>sname</td>
<td>64</td>
<td>Optional server host name, null</td>
</tr>
</tbody>
</table>
DHCP Spoofing Attack

Who:
- Malicious user: pretend to be the network DHCP server
- Mis-configured user: find DHCP server incorrectly

Where:
- Commonly seen in high education, metro Ether

How:
- Attacker Intercepts Discovery Broadcast and Replies with Bogus Gateway and DNS Addresses

© 2006, Cisco Systems, Inc. All rights reserved.

• Add text
Do I Trust You?

DHCP Snooping relies on correct identification of Trusted and Untrusted ports.

**default = All Ports Untrusted**

Trust ONLY those ports for which you have direct control of the end-device:

- Routers
- Switches
- Servers

```
Router(config-if)# ip dhcp snooping trust
```
DHCP Attack Solution: DHCP Snooping

ICP Snooping – discarding attacker’s bogus DHCP offer messages by intercepting DHCP messages within a switch
Switch forwards DHCP requests from untrusted access ports only to Trusted ports.
All other types of DHCP traffic from untrusted access ports dropped.
If network DHCP server not local to the switch, trust the uplink port
Building a DHCP binding table containing client IP address, client MAC address, pc VLAN number...
Optional insertion and removal of DHCP option 82 data into/from DHCP messages
DoS attack on DHCP server is prevented by rate limiting DHCP packets per access port
DHCP Binding Table

Contains binding entries for local untrusted ports only

Includes both static entries and dynamic entries learned via DHCP gleaning

<table>
<thead>
<tr>
<th>Field</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>4 bytes</td>
</tr>
<tr>
<td>MAC Address</td>
<td>6 bytes</td>
</tr>
<tr>
<td>VLAN Id</td>
<td>2 bytes</td>
</tr>
<tr>
<td>Lease Timer</td>
<td>4 bytes</td>
</tr>
<tr>
<td>Port</td>
<td>4 bytes</td>
</tr>
<tr>
<td>Binding Type</td>
<td>4 bytes</td>
</tr>
</tbody>
</table>

© 2003, Cisco Systems, Inc. All rights reserved.
What is allowed to pass (client-to-server)?
What is allowed to pass (server-to-client)?
What is prevented (untrusted-to-untrusted)
What is prevented (Untrusted Server Packets).
What is prevented (Who do you think YOU are??)

DHCP Binding Database:
MAC - AA = port 3/3

DROPPED!!
DHCP Decline
DHCP Release

Untrusted port 3/3
Untrusted port 3/3
trusted

SRC MAC = BB AA

© 2003, Cisco Systems, Inc. All rights reserved.
What is prevented (No relay for YOU!!).

- Normal DHCP-Relay operation populates “giaddr” field in DHCP messages.
- This is not allowed if arriving on untrusted port.
DHCP Relay packet dropped!!

Aggregation Switch with DHCP Snooping enabled drops DHCP packet on untrusted port with non-zero giaddr field.

The Solution:

```
Cat4500(config)#int fast 3/25
Cat4500(config-if)#ip add 3.3.3.3
Cat4500(config-if)#ip dhcp snooping trust
Cat4500(config-if)#end
Cat4500#  
```
DHCP Snooping - Configuration

Ensure that DHCP Server and the Relay Agent (if it exists) are already fully functional before you configure DHCP Snooping.

```
# 2. Ensure that DHCP Snooping is enabled for the selected VLANs
C3750(config)#ip dhcp snooping
C3750(config)#ip dhcp snooping vlan 2-99
C3750(config)#interface gig 1/0/2
C3750(config-if)#ip dhcp snooping trust
C3750(config-if)#end
C3750#```

Configure this on ports leading to trusted DHCP Servers... or on uplink ports to Aggregation Switches.

© 2000, Cisco Systems, Inc. All rights reserved.
DHCP Snooping – Additional Config Options

Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ip dhcp snooping limit rate 100

Prevents DHCP DoS attacks that would overwhelm the DHCP Server.

- DHCP Snooping can also be configured on Private VLANs.
- Must configure only on the Primary VLAN...will be dynamically propagated to all Secondary VLANs.
- No way (currently) to have different DHCP Snooping configurations applied to Secondary VLANs all residing under the same Primary VLAN.
DHCP Snooping – Verification

```
Cat6500#show ip dhcp snooping
Snooping is enabled.
DHCP snooping is configured on following VLANs: 1-12
DHCP snooping is operational on following VLANs: 1-8, 10, 11
DHCP snooping is configured on the following L3 Interfaces:
  Insertion of option 82 is enabled
  Option 82 on untrusted port is not allowed
  Verification of hwaddr field is enabled
  Verification of giaddr field is enabled
  DHCP snooping trust/rate is configured on the following Interfaces:
  Interface                  Trusted  Rate limit (pps)
  FastEthernet3/7            yes      unlimited
```

```
Cat6500#show ip dhcp snooping binding
MacAddress    IpAddress    Lease(sec)  Type  VLAN Interface
01:12:34:56:78:90  1.1.1.1      215944    dhcp-snooping  1  FastEthernet0/1
Total number of bindings: 1
```

© 2009, Cisco Systems, Inc. All rights reserved.
DHCP Relay Agent

- Best practice is to store DHCP Binding Database externally to the switch.
  - If stored locally in flash/bootflash, database must be erased and re-written for every new entry.
  - CPU intensive…can lock up the switch.
  - If switch crashes or reloads, all entries / lease info lost and can kill the DHCP Snooping process.

- Feature to do this is called “DHCP Snooping Database Agent”.

  Can also use FTP, HTTP, and RCP

  `witch(Config)# ip dhcp snooping database tftp://192.168.1.1/Snoop-data.dh`  
  `witch(Config)# ip dhcp snooping database write-delay 15`  

  Specify the duration for which the transfer should be delayed after the binding database changes. The range is from 15 to 86400 seconds. The default is 300 seconds (5 minutes).
DHCP Relay Agent Caveat

From the Cat3750 Configuration Guide:

- “For network-based URLs (such as TFTP and FTP), you must create an empty file at the configured URL before the switch can write bindings to the binding file at that URL. See the documentation for your TFTP server to determine whether you must first create an empty file on the server; some TFTP servers cannot be configured this way.”

  Meaning – The switch cannot create this file from scratch. The server must already contain a 0-byte file with this name for this to work.

- What will you see if you DON’T have a 0-byte file to start with??

```
Cat3750# show ip dhcp snooping database
Agent URL : tftp://192.168.1.1/Snoop-data.dhcp
Agent Running : No
Relay Timer Expiry : Not Running
Alert Timer Expiry : Not Running
Last Succeeded Time : N/A
Last Failed Reason : No line expected in database.
Total Attempts : 5033
Successful Transfers : 0
Failed Transfers : 5033
Successful Reads : 0
Failed Reads : 1
Successful Writes : 0
Failed Writes : 0
```

© 2006, Cisco Systems, Inc. All rights reserved.
Restricting Allocated Addresses

Customer’s Challenge:
1. “How can I ensure that each switch is only allocated a maximum of “X” addresses from my DHCP Pool?”
2. “How can I ensure that port 2/1 on Switch-B is only allocated a maximum of “X” addresses from my DHCP Pool?”
3. “What if someone in Customer-C’s network is attempting a DHCP DoS attack (sending multiple DHCPDiscover/Request messages to completely exhaust the DHCP Address Pool)? How can I prevent that?”

The Solution: DHCP Option-82
a.k.a. DHCP Relay Agent Option (RFC 3046)

© 2006 Cisco Systems, Inc. All rights reserved.
1. Option-82 allows trusted access devices to insert this option into (and remove from) DHCP Packets.
2. This option gives descriptive information about the device/port that received the DHCP message.
DHCP Option-82

1. Switch adds “Remote-ID” and “Circuit-ID” sub-options into Option-82 data.
   - Remote-ID default is switch MAC address
   - Circuit-ID default is port identifier in the format “vlan-mod-port”

2. These fields are configurable to use ASCII strings if you prefer

   - `ip dhcp snooping vlan vlan information option format-type circuit-id string ASCII-string`

(Optional) Configure the circuit-ID suboption for the specified interface.

Specify the VLAN and port identifier, using a VLAN ID in the range of 1 to 4094. The default circuit ID is the port identifier, in the format `vlan-mod-port`.

You can configure the circuit ID to be a string of 3 to 63 ASCII characters (no spaces).
### Circuit-ID Suboption Frame Format

<table>
<thead>
<tr>
<th>Suboption Type</th>
<th>Circuit ID Length</th>
<th>Circuit ID Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 bit</td>
<td>1 byte</td>
<td>2 bytes</td>
</tr>
</tbody>
</table>

### Remote ID Suboption Frame Format

<table>
<thead>
<tr>
<th>Remote ID Suboption Type</th>
<th>Remote ID Length</th>
<th>Remote ID Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 bit</td>
<td>1 byte</td>
<td>4 bytes</td>
</tr>
</tbody>
</table>

---

**Circuit-ID information:**
- 0x1 = Suboption type specifying Circuit-ID
- 0x6 = Total Length of Circuit-ID field
- 0x0 = Circuit-ID Type
- 0x4 = Length of the Circuit-id (VLAN + Module + Port)
- 0x0 = First Byte of Circuit-ID (unused in this case since VLAN-1 will be contained in the second byte but this field would be a non-zero number if representing any VLAN above VLAN-255)

- 0x1 = VLAN-1
- 0x3 = Slot-3
- 0x6 = Port-6

**Remote-ID information immediately follows:**
- 0x2 = Suboption Type for Remote-ID
- 0x8 = Total Length (in bytes) of Remote-ID Suboption
- 0x0 = Remote-id Type
- 0x6 = Remote-id Length (Length of MAC address by default)

MAC Address = 00-13:5f-1d-7f-80 (taken from MAC Address of Interface VLAN-1)
DHCP Option-82 Caveats

1. DHCP Servers must be configured to recognize and respond in some way to DHCP Option-82 otherwise packets may be dropped.

2. Switches receiving DHCP messages containing Option-82 will DROP THEM if received on an untrusted interface!!

   • The solution for aggregation switches:
     
     Switch(config)# ip dhcp snooping information option
     
     Switch(config)# ip dhcp snooping information option allow-untrusted

© 2008, Cisco Systems, Inc. All rights reserved.
Dynamic ARP Inspection (DAI)
MIM Attack – Attacking another host

© 2003, Cisco Systems, Inc. All rights reserved.
MIM Attack – Attacking another host

Layer 3 Network

DHCP Server

ARP Cache

ARP Request

Router “R”

Host

Malicious Host “M”

© 2003, Cisco Systems, Inc. All rights reserved.
MIM Attack – Attacking another host

Layer 3 Network

DHCP Server

Router “R”

Malicious Host “M”

ARP Cache

ARP Cast

Host

© 2003, Cisco Systems, Inc. All rights reserved.
MIM Attack – Attacking another host

Layer 3 Network

DHCP Server

Router “R”

Host

User Traffic

Malicious Host “M”

© 2000, Cisco Systems, Inc. All rights reserved.
MIM Attack – Attacking another host

Layer 3 Network

DHCP Server

Router “R”

ARP Cache

ARP Cast

Host

Malicious Host “M”

Unsolicited ARP Response
MIM Attack – Attacking another host

Layer 3 Network

DHCP Server

ARP Cache

 ARP Cast

Router “R”

Host

User Traffic

Malicious Host “M”

© 2003, Cisco Systems, Inc. All rights reserved.
DOS Attack – Attacking the default gateway

Router “R”
L2 Network with PVLAN

Malicious Host “M”
DOS Attack – Attacking the default gateway

Layer 3 Network

ARP Cache

Router “R”
L2 Network with PVLAN

Host

Malicious Host “M”
DOS Attack – Attacking the default gateway

Layer 3 Network

ARP Cache
IP_A MAC_A
IP_B MAC_B

User Traffic

Router “R”
L2 Network with PVLAN

Host

Malicious Host “M”

© 2003, Cisco Systems, Inc. All rights reserved.
DOS Attack – Attacking the default gateway

Layer 3 Network

ARP Cache

Router “R”

L2 Network with PVLAN

DHCP Ser

Host

Malicious Host “M”

Unsolicited ARP Response

© 2003, Cisco Systems, Inc. All rights reserved.
DOS Attack – Attacking the default gateway

Layer 3 Network

DHCP Server

ARP Cache

User Traffic

Router “R”

L2 Network with PVLAN

Host

Malicious Host “M”
ARP Poisoning: Serious Business

- Avaya demonstrated a variation of ARP poisoning at their customer briefing center using Cisco gear
- After intercepting a network connection, packets containing G.711 voice data are collected and the phone conversation is recorded and then replayed
- Demonstrated live to Cisco senior executives in the Cisco network
- Tools are publicly available with GUI and bi-directional spoofs: Ettercap and Dsniff
- Easily taught in 5 minutes
- Neither the victim nor the default gateway is aware of the attack

© 2003, Cisco Systems, Inc. All rights reserved.
ARP Poisoning Attack Solution: Dynamic ARP Inspection

Dynamic ARP Inspection – discarding attacker’s gratuitous ARP packets in the switch, and logging the attempts for auditing

Bindings of client IP address, client MAC address, port, VLA number are built dynamically by DHCP snooping

Switch intercepts all ARP requests and replies on the untrusted access ports

Each intercepted packet is verified for valid IP-to-MAC bindings

A solution with no change to the end user or host configurations
Dynamic ARP Inspection (DAI) Overview

- When DHCP Snooping not applicable, static ARP ACLs can be configured instead.
- ARP ACLs always take priority over DHCP Snooping Table.
  - If an ARP ACL is configured to drop a packet, that ARP will be dropped even if there is a valid entry in the DHCP Snooping Table.
- Relies on same concepts of “Trusted” and “Untrusted” ports as DHCP Snooping.
  - Ports are untrusted by default
  - DAI does not verify any ARP Requests/Replies from Trusted interfaces.

© 2003, Cisco Systems, Inc. All rights reserved.
ARP Inspection Procedure

1. Trusted I/F?
   - Yes
   - No
     - Ethernet & IPv4
       - Yes
       - Match ARP ACL?
         - Yes
         - Action?
           - Permit
           - Deny
         - Match DHCP binding table?
           - Yes
           - Forward valid ARP packet
           - No
           - Drop & log invalid ARP packet
         - No
       - No
     - No
     - No
     - No
     - No
     - No
     - No
     - No
     - No
ARP Inspection Overview

- An ARP request/response packet is considered valid if it meets the following criteria:

  1) Mandatory: Sender <MAC, IP, VLAN> triplet is valid
  2) Optional: Sender MAC == Source MAC
  3) Optional (for ARP response):
     Target MAC == Destination MAC

ARP Packet Format

<table>
<thead>
<tr>
<th>Field</th>
<th>Source MAC Addr</th>
<th>Frame Type</th>
<th>H/W Type</th>
<th>Prot Type</th>
<th>H/W Size</th>
<th>Prot Size</th>
<th>Op Code</th>
<th>Sender MAC Addr</th>
<th>Sender IP Addr</th>
<th>Target MAC Addr</th>
<th>Target IP Addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Addr</td>
<td>0x0000</td>
<td>0x0806</td>
<td>ARP</td>
<td>6</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source Addr</td>
<td>0x0000</td>
<td>0x0800</td>
<td>(IPv4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H/W Type</td>
<td>0x01</td>
<td>Ethernet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2003, Cisco Systems, Inc. All rights reserved.
Basic DAI Configuration

- Two Design Methodologies:
  1. Configure DAI on every switch in the network.
     - Leave all edge ports as Untrusted
     - Trust all interfaces connected to networking devices (routers, switches, etc).
  2. Configure DAI on all Edge switches (assuming that hosts are only connected to Edge switches).

- Step-1: Configure and verify DHCP Snooping first!
- Step-2: Configure DAI:

```
Cat6500#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
Cat6500(config)#ip arp inspection vlan 1-12
Cat6500(config)#interface fastethernet3/25
Cat6500(config-if)#ip arp inspection trust
Cat6500(config-if)#end
```

© 2003, Cisco Systems, Inc. All rights reserved.
DAI in action! (1)

```
VLAN-1

6500

DAI-enabled Switch

VLAN-1

Fa0/0

1.1.1.1

DHCP-given address of 1.1.1.1

Admin Shut
```

<table>
<thead>
<tr>
<th>MacAddress</th>
<th>IPAddress</th>
<th>Lease (sec)</th>
<th>Type</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:11:06:18:4F:40</td>
<td>1.1.1.1</td>
<td>20839</td>
<td>dhcp-snooping</td>
<td>1</td>
<td>FastEthernet1/0</td>
</tr>
</tbody>
</table>

Total number of bindings: 1

```
Cisco# show ip arp inspection

Source Mac Validation : Disabled
Destination Mac Validation : Disabled
IP Address Validation : Disabled

Vlan     Configuration     Operation  ACL Match  Static ACL
--------     -----------     --------  ---------  -------
1           Enabled        Active
```

© 2003, Cisco Systems, Inc. All rights reserved.
DAI in action!! (2)

As soon as the router’s FastEthernet interface comes up it will perform a gratuitous ARP…let’s see what happens!!
DAI in action!! (3)

Gratuitous ARP from Router is dropped by DAI on switch.
DAI for non-DHCP hosts

Notice that in this example, the router has been given a valid, static address of 1.1.1.6 /24. But because it is connected to an untrusted port and does not participate in DHCP, nobody can ARP for it!
DAI for non-DHCP hosts (2)

The Solution: ARP Access-List

```
 Cisco# show run
 ip arp inspection vlan 1:12
 ip arp inspection filters test vlan 1
 arp access-list test
 permit response ip host 1.1.1.6 any mac host 0011:5e:00:33:40 any
```

---

**1.1.1.6**

Rate sequence to short.

```
rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

DHCP-given address of 1.1.1.1

---

```
Router# show int fast 0/0
FastEthernet0/0 is up, line protocol is up
Hardware is FastEth, address is 0011:5e00:3340
```

```
Router# show int fast 0/1
Interface FastEthernet0/1
 ip address 1.1.1.6 255.255.255.0
duplex auto speed auto
```

---

© 2003, Cisco Systems, Inc. All rights reserved.
ARP ACL Example

Configuring ARP ACL
(Config)#arp access-list arp_acl_1
(config-arp-nacl)# permit ip host 10.1.1.1 mac host 0000.0001.0002
(config-arp-nacl)# deny ip 10.1.1.0 0.0.0.255 mac any
(config-arp-nacl)# permit ip any mac any

"IP" will apply to both ARP requests and responses. Alternatively you can also specify "Request" or "Response".

Applying ARP ACL to a VLAN
(config)# ip arp inspection filter arp_acl_1 vlan 5
or...
(config)# ip arp inspection filter arp_acl_1 vlan 5 static

Without the "static" keyword DAI will continue to look for a matching entry in the DHCP Snooping Database if no matches the ACL.

With the "static" keyword DAI will use the implicit "deny all" if no match is found in the ACL...even if a corresponding match IS in the DHCP Snooping DB.
Rate-Limiting of ARP traffic

- ARP packets are rate-limited to prevent a denial-of-service attack on Untrusted interfaces.
- Default is 15 pps
- Trusted interfaces are not rate-limited
- (config-if)# ip arp inspection limit <x> to raise or lower this limit.
- Exceeding the limit causes the interface to be placed into Errdisable state.

Mar 20 16:36:50.183: %SU-EAI-4-PACKET_RATE_EXCEED: 16 packets received in 12 milliseconds on Fa0/7.
Mar 20 16:36:50.384: %SU-EAI-4-DHCP_SNOOPEDEVMT: 16 Invalid ARPs (Neg) on Fa0/7, via 1.1.1.1/0.0.0.0 to 1.1.1.0/255.255.255.0 via 1.1.1.0/255.255.255.0
Mar 20 16:36:50.384: %SU-EAI-4-DHCP_SNOOPEDEVMT: 16 Invalid ARPs (Neg) on Fa0/7, via 1.1.1.1/0.0.0.0 to 1.1.1.0/255.255.255.0 via 1.1.1.0/255.255.255.0

© 2003, Cisco Systems, Inc. All rights reserved.