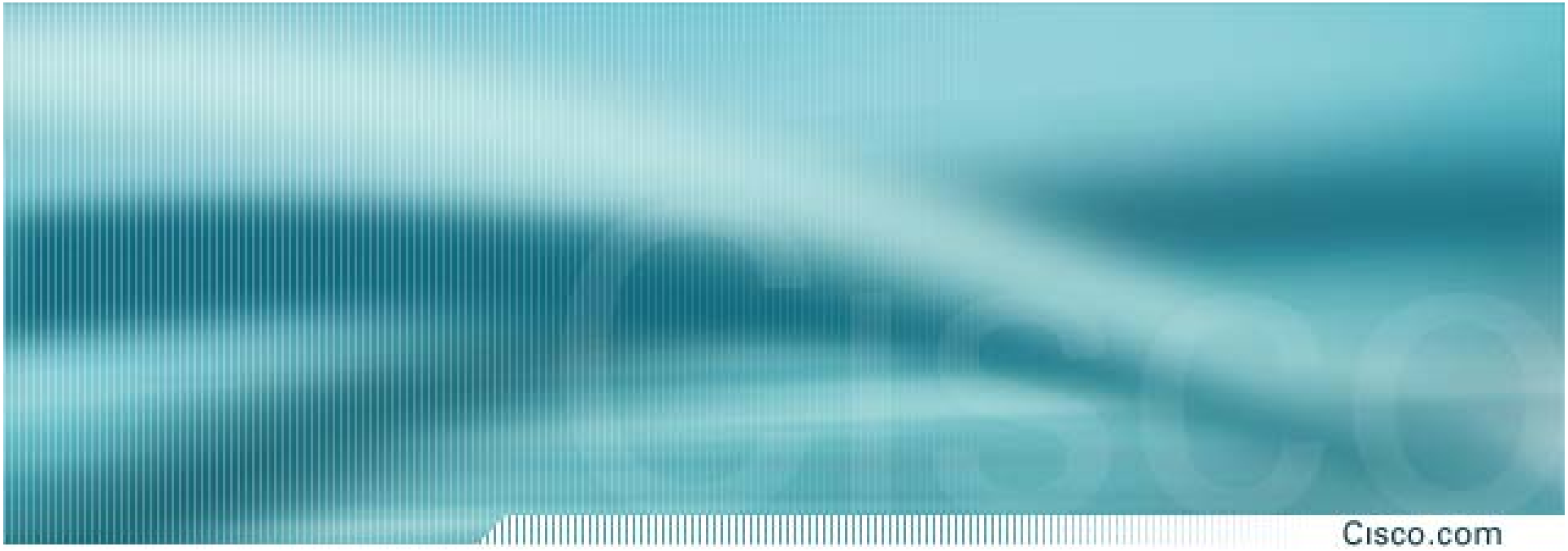
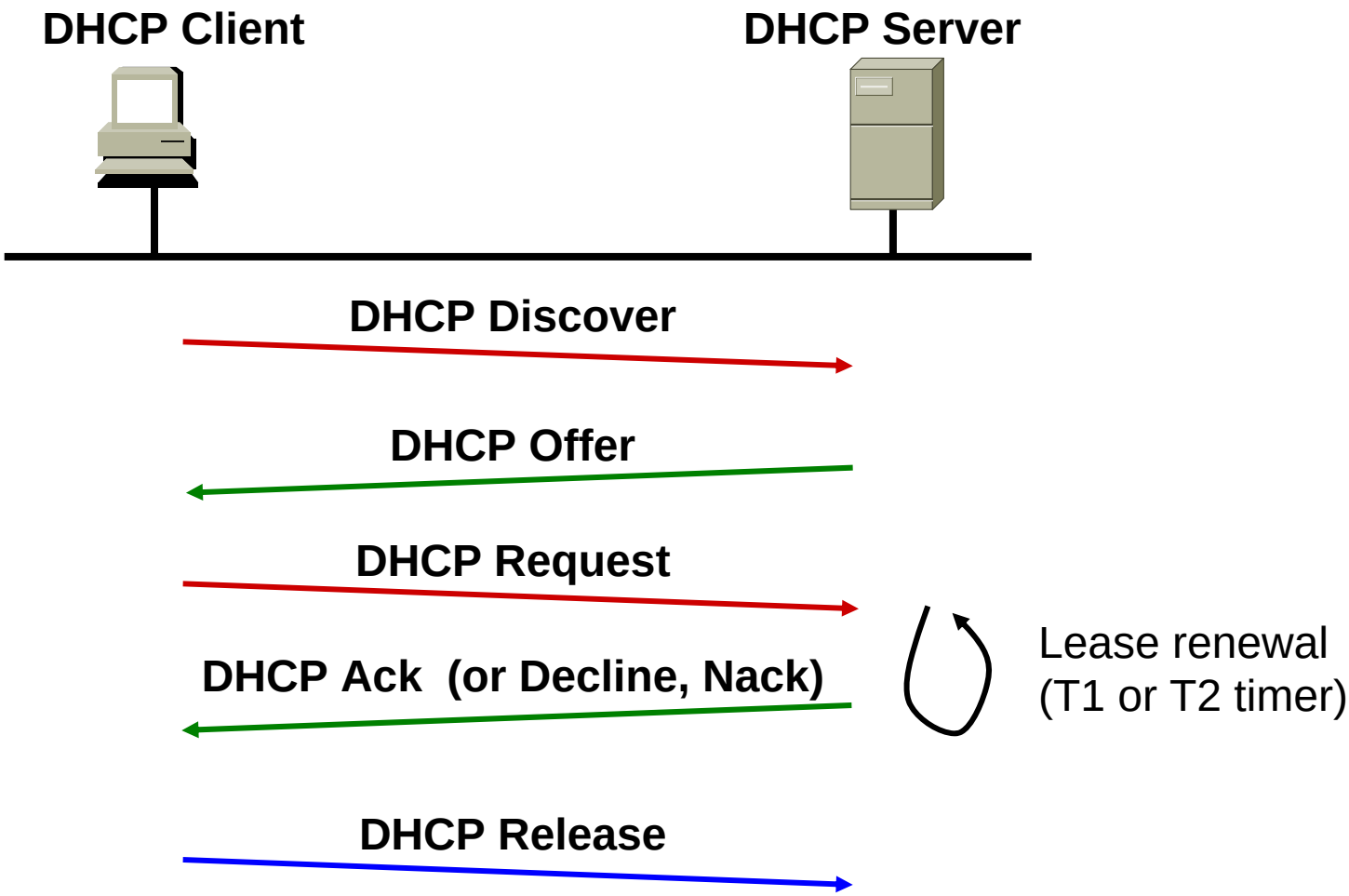


DHCP Snooping

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 (client-to-server)

No.	Time	Source	Destination	Protocol	Info
37	15.956730	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7dab8029
38	15.962968	171.69.80.3	171.69.81.43	DHCP	DHCP Offer - Transaction ID 0x7dab8029
39	15.963357	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7dab8029
40	15.968051	171.69.80.2	171.69.81.43	DHCP	DHCP Offer - Transaction ID 0x7dab8029
41	15.973204	171.69.80.2	171.69.81.43	DHCP	DHCP ACK - Transaction ID 0x7dab8029
42	15.981081	171.69.80.3	171.69.81.43	DHCP	DHCP ACK - Transaction ID 0x7dab8029

```
⊞ Frame 37 (342 bytes on wire, 342 bytes captured)
⊞ Ethernet II, Src: Foxconn_ea:6a:d8 (00:01:6c:ea:6a:d8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x7dab8029
    Seconds elapsed: 0
  ⊞ Bootp 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)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Foxconn_ea:6a:d8 (00:01:6c:ea:6a:d8)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Discover
    Option 116: DHCP Auto-Configuration (1 bytes)
  ⊞ Option 61: Client identifier
    Option 50: Requested IP Address = 1.1.1.1
    Option 12: Host Name = "kbogart-wxp04"
    Option 60: Vendor class identifier = "MSFT 5.0"
  ⊞ Option 55: Parameter Request List
    End Option
```

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)

No.	Time	Source	Destination	Protocol	Info
37	15.956730	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7dab8029
38	15.962968	171.69.80.3	171.69.81.43	DHCP	DHCP Offer - Transaction ID 0x7dab8029
39	15.963357	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7dab8029
40	15.968051	171.69.80.2	171.69.81.43	DHCP	DHCP Offer - Transaction ID 0x7dab8029
41	15.973204	171.69.80.2	171.69.81.43	DHCP	DHCP ACK - Transaction ID 0x7dab8029
42	15.981081	171.69.80.3	171.69.81.43	DHCP	DHCP ACK - Transaction ID 0x7dab8029

```
⊞ Frame 38 (351 bytes on wire, 351 bytes captured)
⊞ Ethernet II, Src: 00:19:07:ba:7d:c0 (00:19:07:ba:7d:c0), Dst: Foxconn_ea:6a:d8 (00:01:6c:ea:6a:d8)
⊞ Internet Protocol, Src: 171.69.80.3 (171.69.80.3), Dst: 171.69.81.43 (171.69.81.43)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x7dab8029
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 171.69.81.43 (171.69.81.43)
    Next server IP address: 171.71.179.41 (171.71.179.41)
    Relay agent IP address: 171.69.80.3 (171.69.80.3)
    Client MAC address: Foxconn_ea:6a:d8 (00:01:6c:ea:6a:d8)
    Server host name not given
    Boot file name: /x86pc/undi/bstrap/bstrap.0
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Offer
    Option 54: Server Identifier = 171.68.10.69
    Option 51: IP Address Lease Time = 2 days, 18 hours, 40 minutes, 35 seconds
    Option 1: Subnet Mask = 255.255.254.0
    Option 15: Domain Name = "cisco.com"
    Option 3: Router = 171.69.80.1
  ⊞ Option 6: Domain Name Server
  ⊞ Option 44: NetBIOS over TCP/IP Name Server
```

DHCP Request (client-to-server)

No.	Time	Source	Destination	Protocol	Info
37	15.956730	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7dab8029
38	15.962968	171.69.80.3	171.69.81.43	DHCP	DHCP Offer - Transaction ID 0x7dab8029
39	15.963357	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7dab8029
40	15.968051	171.69.80.2	171.69.81.43	DHCP	DHCP Offer - Transaction ID 0x7dab8029
41	15.973204	171.69.80.2	171.69.81.43	DHCP	DHCP ACK - Transaction ID 0x7dab8029
42	15.981081	171.69.80.3	171.69.81.43	DHCP	DHCP ACK - Transaction ID 0x7dab8029

```
⊞ Frame 39 (378 bytes on wire, 378 bytes captured)
⊞ Ethernet II, Src: Foxconn_ea:6a:d8 (00:01:6c:ea:6a:d8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x7dab8029
    Seconds elapsed: 0
  ⊞ Bootp 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)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Foxconn_ea:6a:d8 (00:01:6c:ea:6a:d8)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Request
  ⊞ Option 61: Client identifier
    Option 50: Requested IP Address = 171.69.81.43
    Option 54: Server Identifier = 171.68.10.69
    Option 12: Host Name = "kbogart-wxp04"
  ⊞ Option 81: FQDN
    Option 60: Vendor class identifier = "MSFT 5.0"
  ⊞ Option 55: Parameter Request List
    End Option
```

Duplicate packets??

Cisco.com

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

37	15.956730	0.0.0.0	255.255.255.255	DHCP	DHCP Discover	- Transaction ID 0x7dab8029
38	15.962968	171.69.80.3	171.69.81.43	DHCP	DHCP Offer	- Transaction ID 0x7dab8029
39	15.963357	0.0.0.0	255.255.255.255	DHCP	DHCP Request	- Transaction ID 0x7dab8029
40	15.968051	171.69.80.2	171.69.81.43	DHCP	DHCP Offer	- Transaction ID 0x7dab8029
41	15.973204	171.69.80.2	171.69.81.43	DHCP	DHCP ACK	- Transaction ID 0x7dab8029
42	15.981081	171.69.80.3	171.69.81.43	DHCP	DHCP ACK	- Transaction ID 0x7dab8029

```
⊞ Frame 40 (351 bytes on wire, 351 bytes captured)
⊞ Ethernet II, Src: 00:19:07:ea:7a:80 (00:19:07:ea:7a:80), Dst: Foxconn_ea:6a:d8 (00:01:6c:ea:6a:d8)
⊞ Internet Protocol, Src: 171.69.80.2 (171.69.80.2), Dst: 171.69.81.43 (171.69.81.43)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x7dab8029
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 171.69.81.43 (171.69.81.43)
    Next server IP address: 171.71.179.41 (171.71.179.41)
    Relay agent IP address: 171.69.80.2 (171.69.80.2)
    Client MAC address: Foxconn_ea:6a:d8 (00:01:6c:ea:6a:d8)
    Server host name not given
    Boot file name: /x86pc/undi/bstrap/bstrap.0
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Offer
    Option 54: Server Identifier = 171.68.10.69
    Option 51: IP Address Lease Time = 2 days, 18 hours, 40 minutes, 35 seconds
    Option 1: Subnet Mask = 255.255.254.0
    Option 15: Domain Name = "cisco.com"
    Option 3: Router = 171.69.80.1
```

DHCP ACK (server-to-client)

37	15.956730	0.0.0.0	255.255.255.255	DHCP	DHCP Discover	- Transaction ID 0x7dab8029
38	15.962968	171.69.80.3	171.69.81.43	DHCP	DHCP Offer	- Transaction ID 0x7dab8029
39	15.963357	0.0.0.0	255.255.255.255	DHCP	DHCP Request	- Transaction ID 0x7dab8029
40	15.968051	171.69.80.2	171.69.81.43	DHCP	DHCP Offer	- Transaction ID 0x7dab8029
41	15.973204	171.69.80.2	171.69.81.43	DHCP	DHCP ACK	- Transaction ID 0x7dab8029
42	15.981081	171.69.80.3	171.69.81.43	DHCP	DHCP ACK	- Transaction ID 0x7dab8029

```
⊞ Frame 41 (351 bytes on wire, 351 bytes captured)
⊞ Ethernet II, Src: 00:19:07:ea:7a:80 (00:19:07:ea:7a:80), Dst: Foxconn_ea:6a:d8 (00:01:6c:ea:6a:d8)
⊞ Internet Protocol, Src: 171.69.80.2 (171.69.80.2), Dst: 171.69.81.43 (171.69.81.43)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x7dab8029
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 171.69.81.43 (171.69.81.43)
    Next server IP address: 171.71.179.41 (171.71.179.41)
    Relay agent IP address: 171.69.80.2 (171.69.80.2)
    Client MAC address: Foxconn_ea:6a:d8 (00:01:6c:ea:6a:d8)
    Server host name not given
    Boot file name: /x86pc/undi/bstrap/bstrap.0
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP ACK
    Option 54: Server Identifier = 171.68.10.69
    Option 51: IP Address Lease Time = 2 days, 18 hours, 40 minutes, 35 seconds
    Option 1: Subnet Mask = 255.255.254.0
    Option 15: Domain Name = "cisco.com"
    Option 3: Router = 171.69.80.1
  ⊞ Option 6: Domain Name Server
  ⊞ Option 44: NetBIOS over TCP/IP Name Server
```

Several DHCP message types….

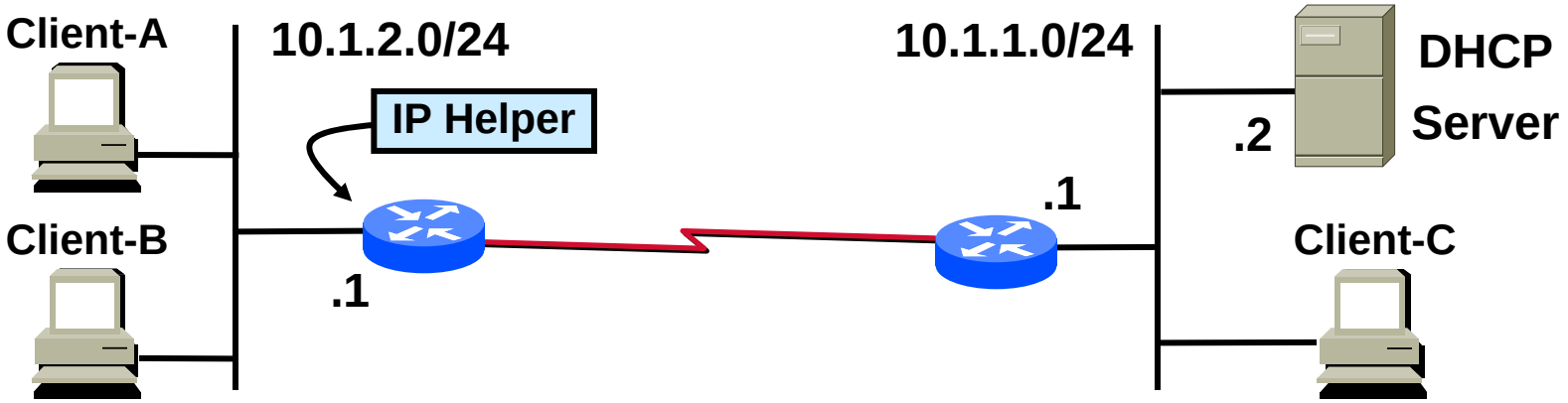
Client messages:

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

Server messages:

- Offer
- ACK
- NAK

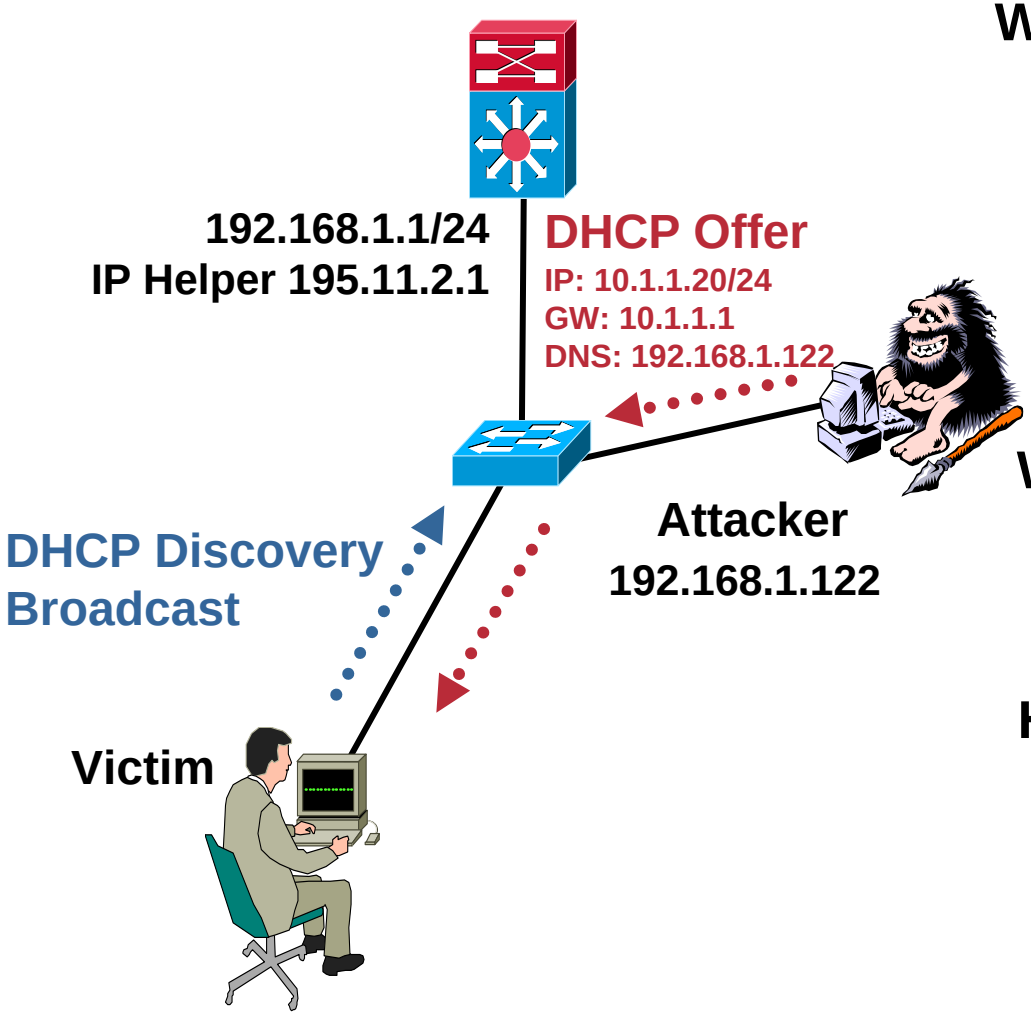
DHCP Message Format



0	16		32
OP Code (1)	HTYPE (1)	HLEN (1)	HOPS (1)
TRANSACTION ID (4)			
SECONDS (2)		UNUSED (2)	
CLIENT IP ADDRESS (4)			
YOUR IP ADDRESS (4)			
SERVER IP ADDRESS (4)			
GATEWAY IP ADDRESS (GiADDR) (4)			
SERVER HOST NAME (64)			
BOOT FILE NAME (128)			
VENDOR-SPECIFIC OPTIONS (312)			

The GIADDR is "stuffed" with IP address by IP Helper feature to ID subnet of client

DHCP Spoofing Attack



Who:

- Malicious user: pretend to be the network DHCP server
- Mis-configured user: fire up DHCP server incorrectly

Where:

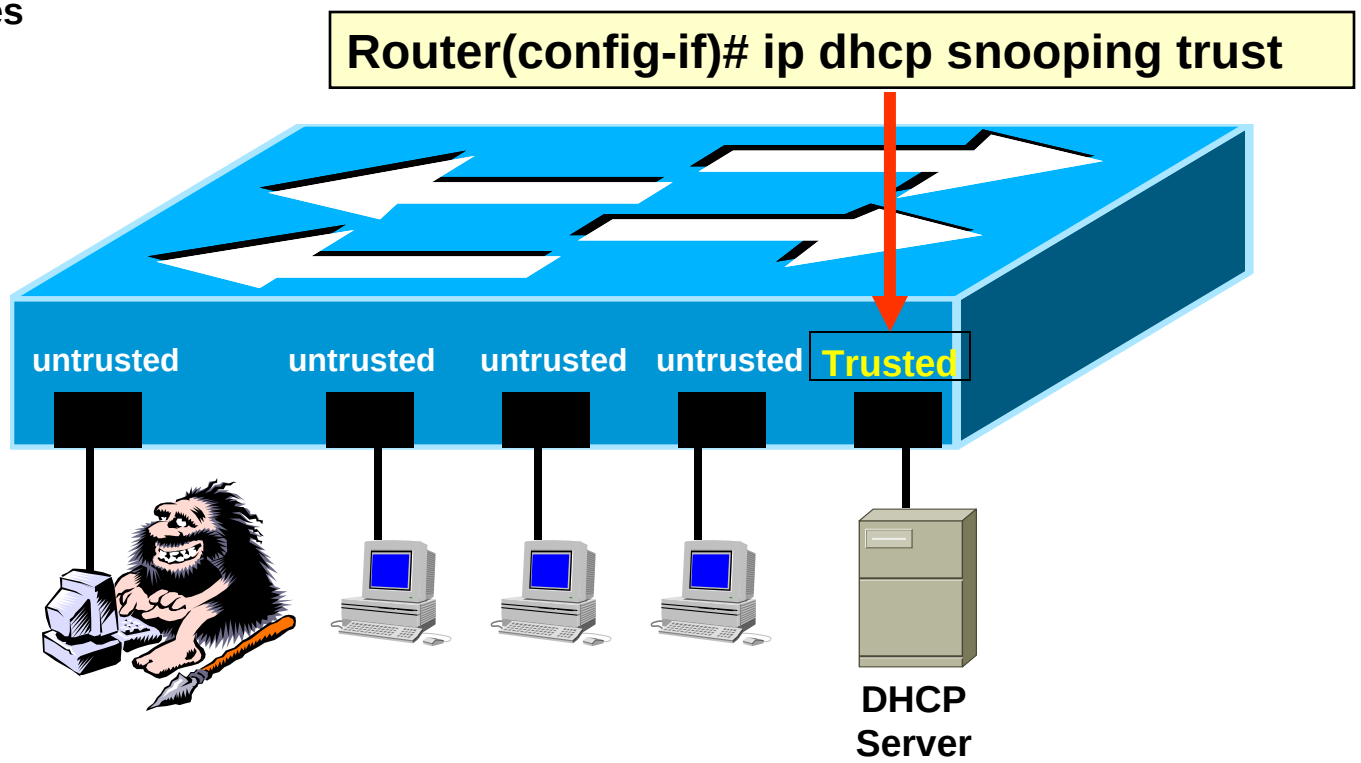
- Commonly seen in higher education, metro Ethernet

How:

- Attacker Intercepts Discovery Broadcast and Replies With Bogus Gateway and DNS Addresses

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, ie:
  - ✓Routers
  - ✓Switches
  - ✓Servers

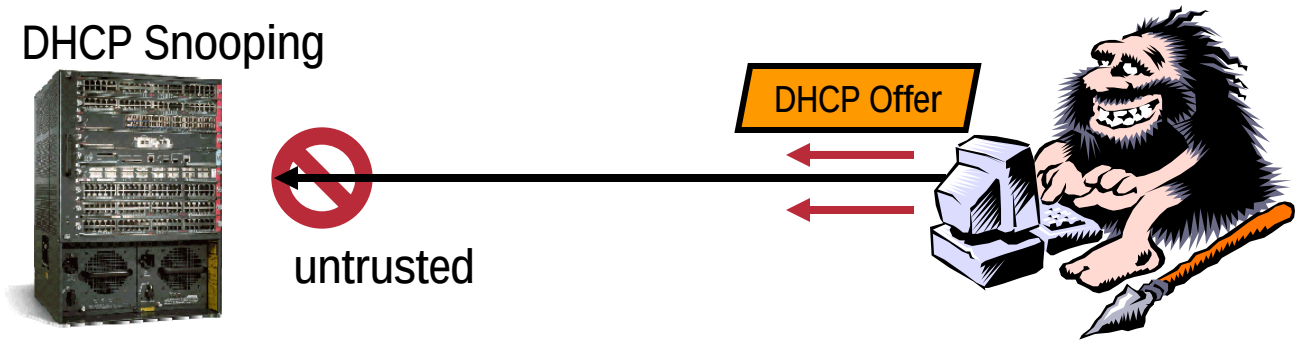


DHCP Attack Solution: DHCP Snooping

Cisco.com

DHCP 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, port, 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**

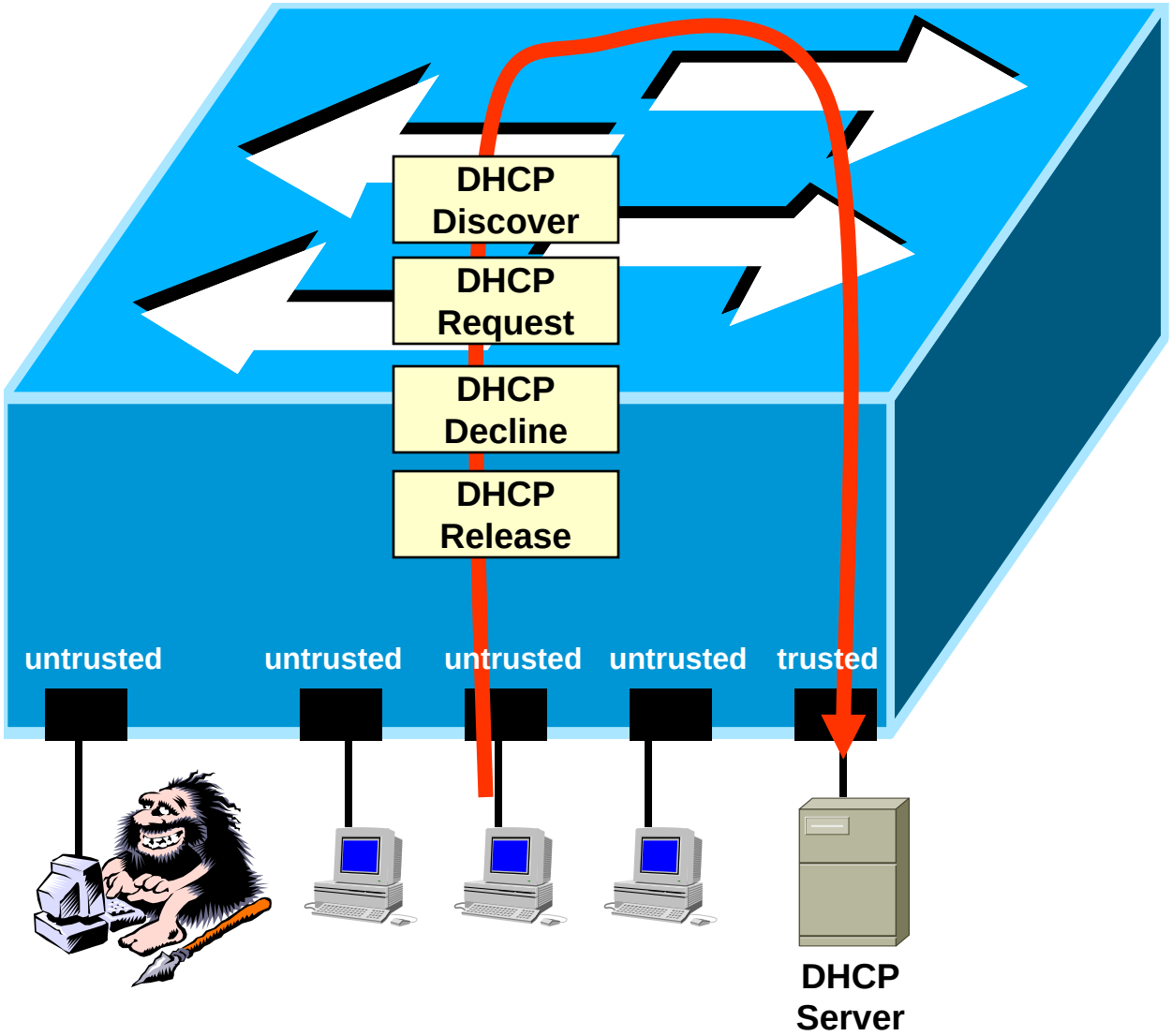


DHCP Binding Table

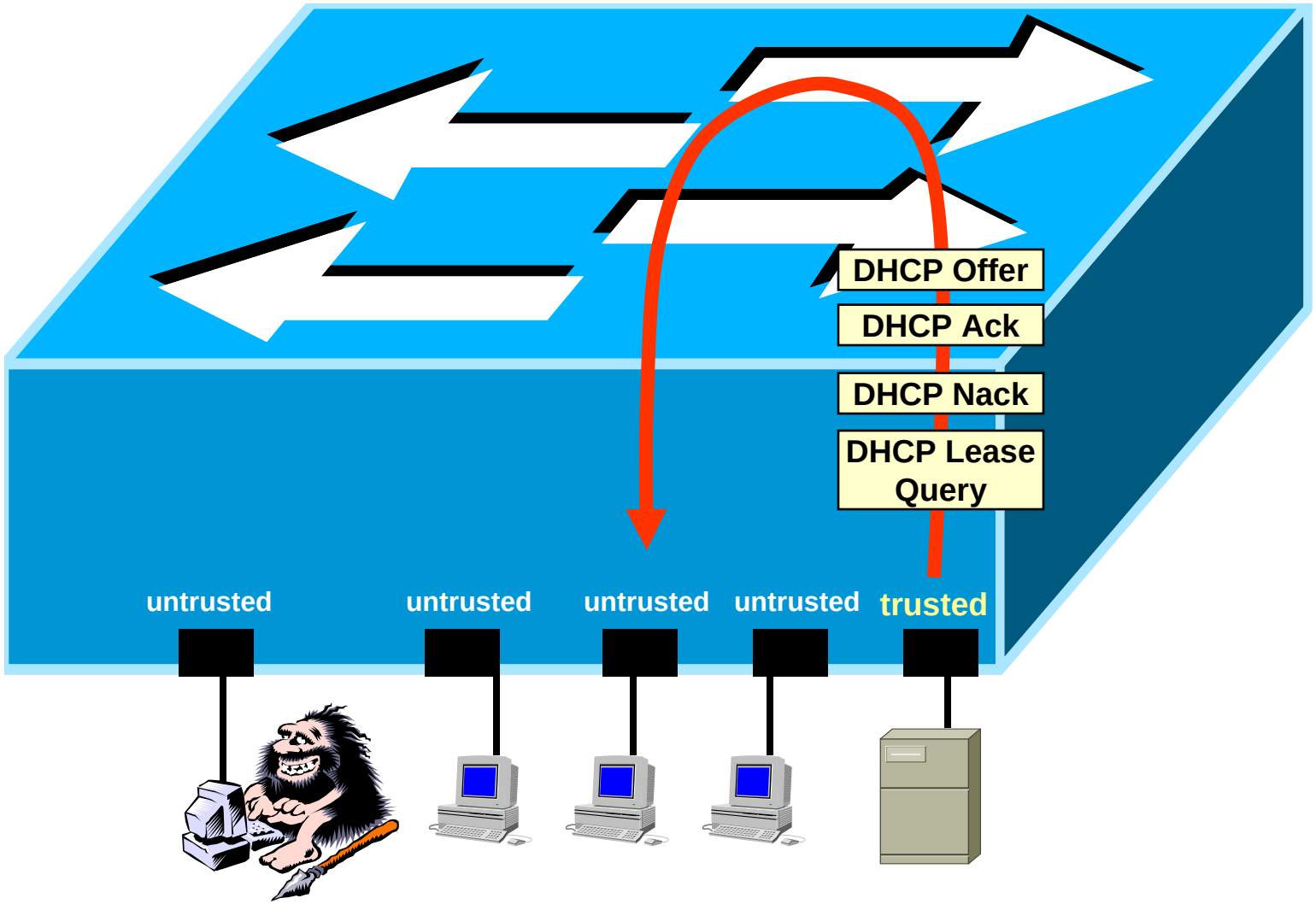
- **Contains binding entries for local untrusted ports only**
- **Includes both static entries and dynamic entries learned via DHCP gleaning**

4 bytes	**IP Address**
6 bytes	**MAC Address**
2 bytes	**VLAN Id**
4 bytes	**Lease Timer**
4 bytes	**Port**
4 bytes	**Binding Type**

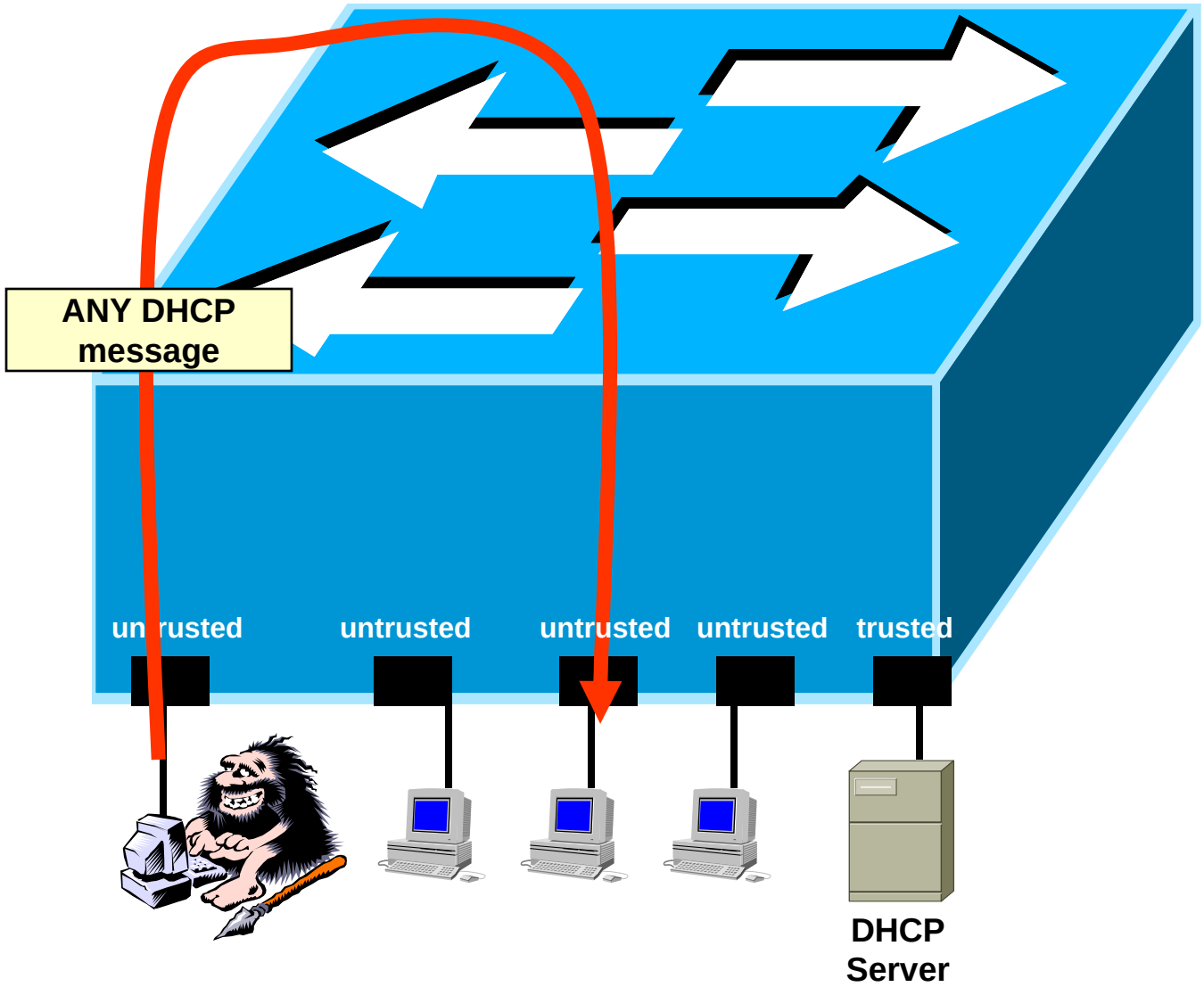
What is allowed to pass (client-to-server)?



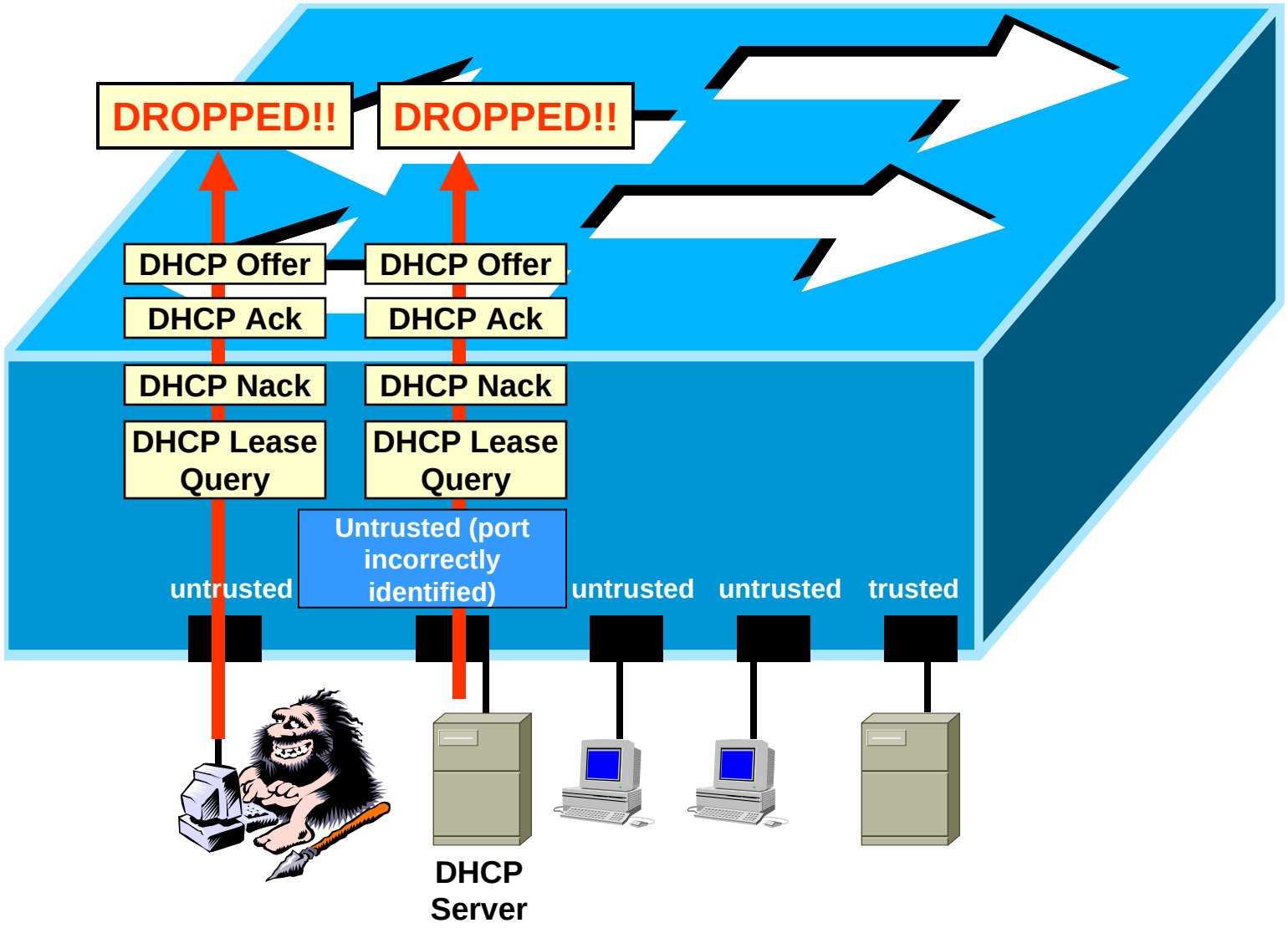
What is allowed to pass (server-to-client)?



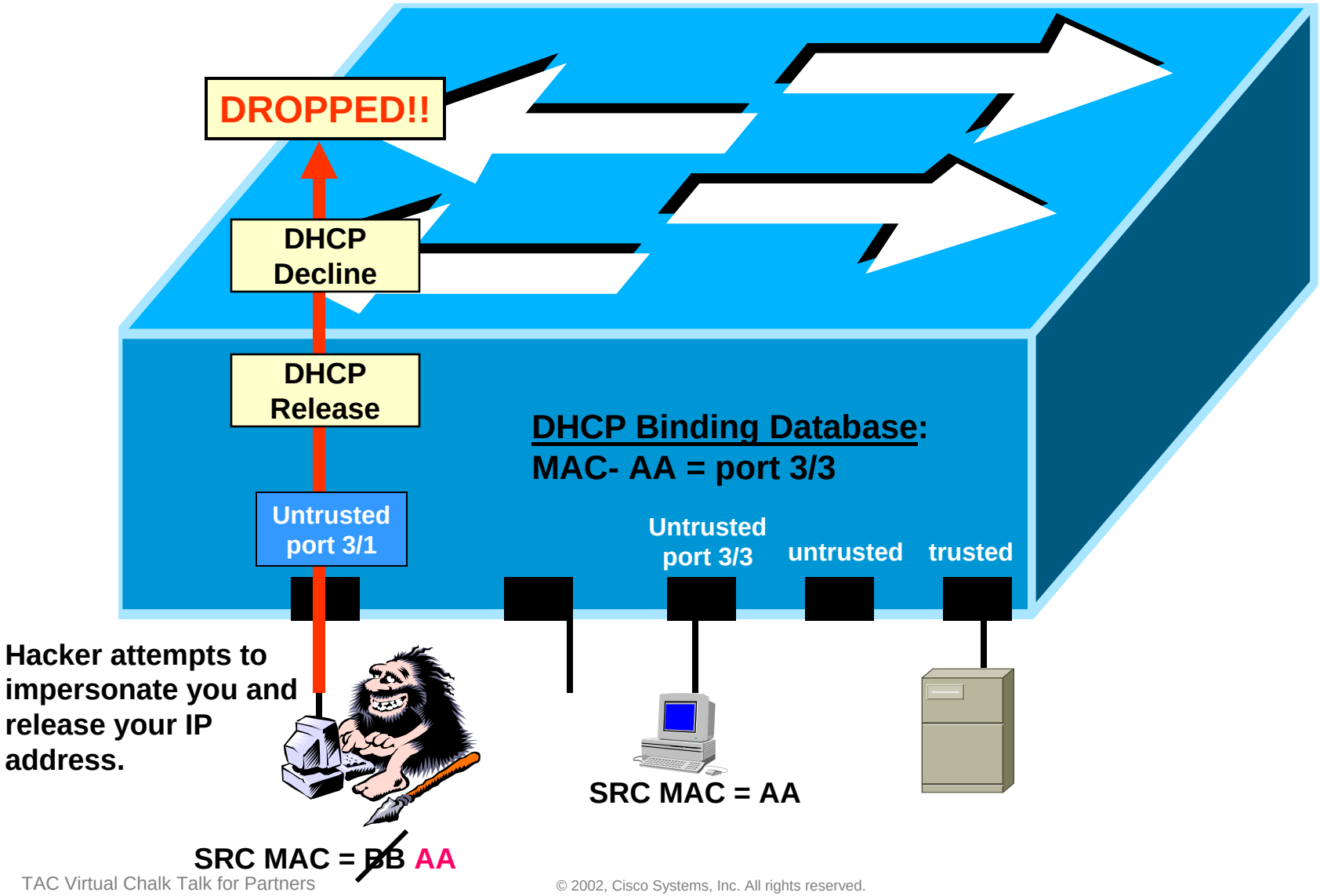
What is prevented (untrusted-to-untrusted).



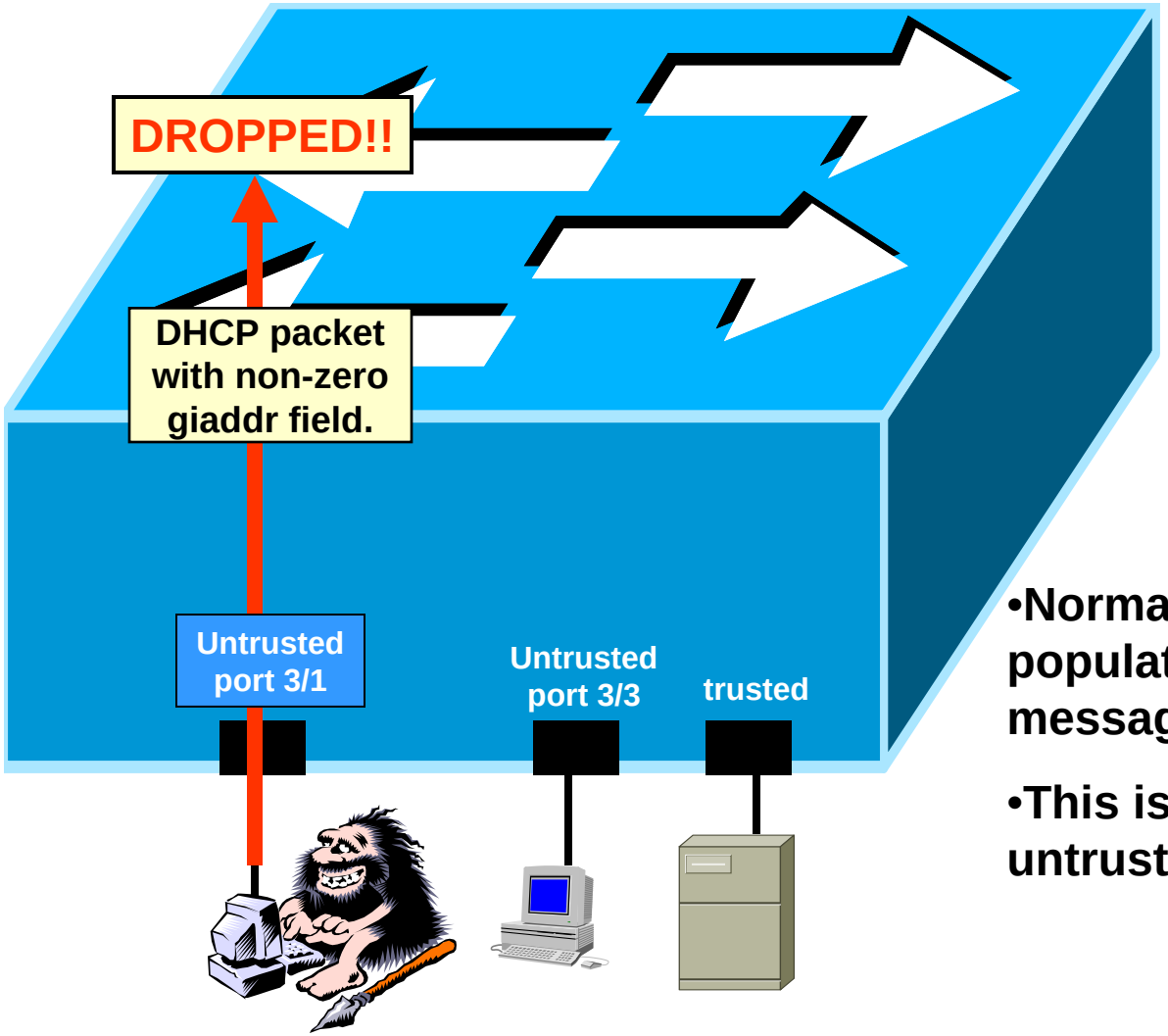
What is prevented (Untrusted Server Packets).



What is prevented (Who do you think YOU are??).

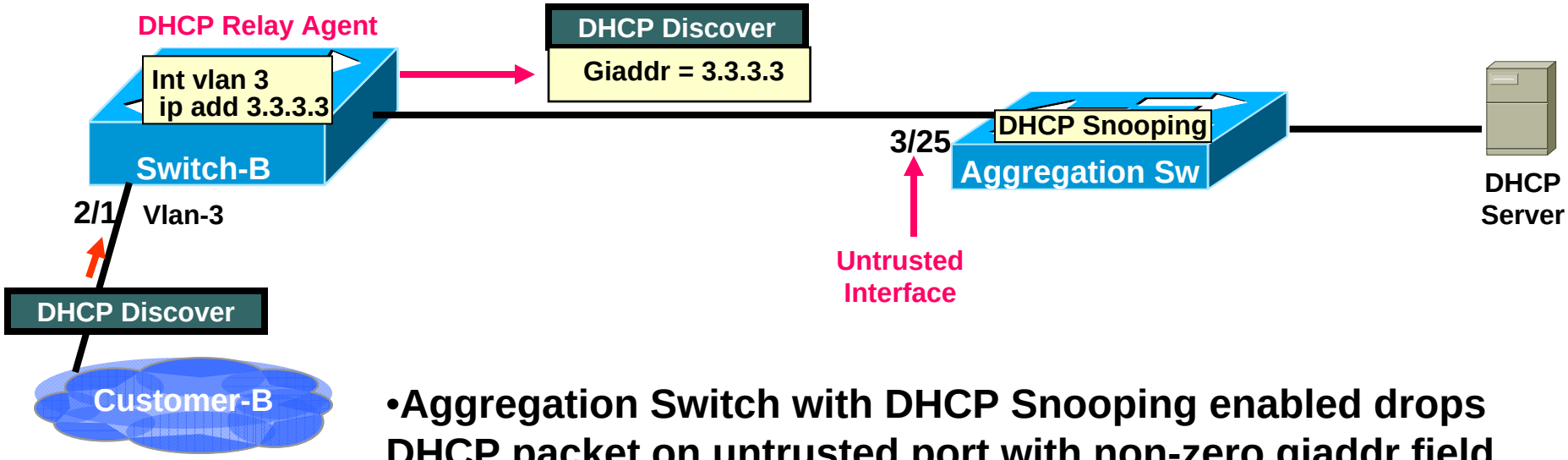


What is prevented (No relay for YOU!!).



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

DHCP Relay packet dropped!!



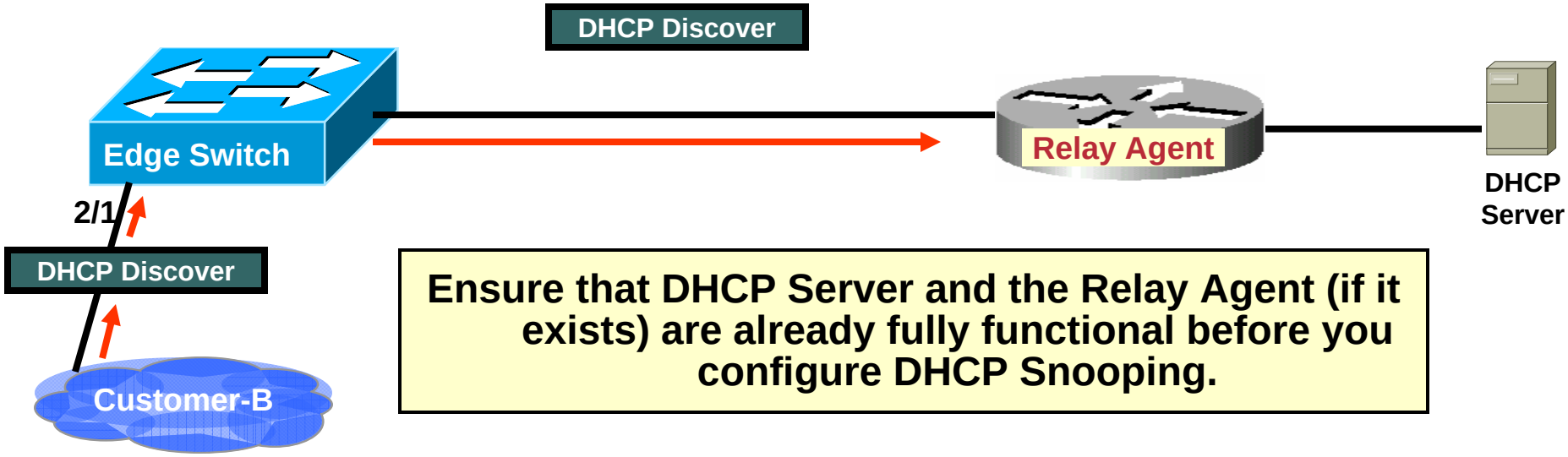
- Aggregation Switch with DHCP Snooping enabled drops DHCP packet on untrusted port with non-zero giaddr field.

```
Mar 20 12:06:03: %DHCP_SNOOPING-5-DHCP_SNOOPING_NONZERO_GIADDR: DHCP_SNOOPING drop
message with non-zero giaddr or option82 value on untrusted port, message type: DHC
PDISCOVER, MAC sa: 0013.5f1d.7f80
```

The Solution:

```
Cat4500(config)#int fast 3/25
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.

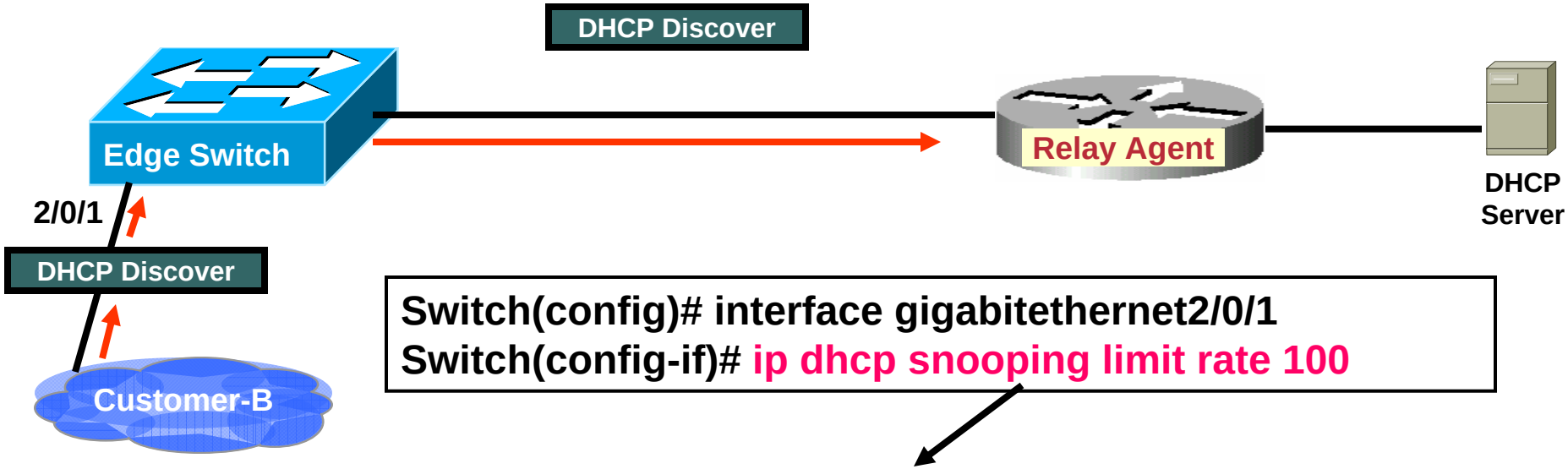
```
Cat3750(config)#
Cat3750(config)#
Cat3750(config)#ip dhcp snooping
Cat3750(config)#ip dhcp snooping vlan 2-8
Cat3750(config)#interface gig 1/0/2
Cat3750(config-if)#no ip dhcp snooping trust
Cat3750(config-if)#ip dhcp snooping trust
Cat3750(config-if)#end
Cat3750#
```

Enables DHCP Snooping only for these VLANs

Default setting

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

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

Cisco.com

```
Cat6500#sho ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1-12
DHCP snooping is operational on following VLANs:
1-8,10,12
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#
```

Untrusted interfaces don't display.

```
Cat6500#sho ip dhcp snooping bind
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -------------------
00:11:5C:16:4F:60   1.1.1.1          215944      dhcp-snooping   1     FastEthernet3/6
Total number of bindings: 1

Cat6500#
```

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

```
Switch(Config)# ip dhcp snooping database tftp://192.168.1.1/Snoop-data.dhcp
Switch(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 GOTCHAS (1)

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
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeded Time : None
Last Failed Time : 18:56:49 DST Mon Sep 18 2006
Last Failed Reason : New line expected in database.

Total Attempts       :     9285   Startup Failures :     9284
Successful Transfers :        0   Failed Transfers :     9285
Successful Reads     :        0   Failed Reads     :        1
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
```

DHCP Relay Agent GOTCHAS (2)

Cisco.com

From the Cat3750 Configuration Guide:

- **"To ensure that the lease time in the database is accurate, we recommend that you enable and configure NTP."**

The REAL STORY: NTP (Network Time Protocol) is MANDATORY! Agent won't work without it!!

- **What will you see if you DON'T have NTP running??**

```
*Jul 27 23:08:20: Safe write timer expired.
*Jul 27 23:08:20: Trying to open url in safe write mode..
*Jul 27 23:08:20: Safe write mode failed.  Restarting timer.
```

From Case# 601706547: "Safe read write mode is a special mode which tries to open the file mentioned in the database URL in the read-only format and only if it exists tries to write to it as in try to update it. If the file does not exist , it tries to create the file. And from the debug messages (the explanation of debug messages are not documented on CCO) , what I can see is safe mode is just simply failing to access the file.

- **A sniffer trace from the customer showed that the switch wasn't sending ANYTHING to the database server (which contradicted the explanation above because it wasn't even trying to read the file).**
- **Turned out that the NTP server had failed, which caused this problem.**

I need an NTP Server??!!

Cisco.com

- **If the customer doesn't normally use NTP (but it's required for the Database Agent) simply configure the NTP Server on another networking device.**

NTP Client (DHCP Snooping Switch)

```
Cat6500#sh run
Building configuration...

service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
clock timezone PST -8
clock summer-time PDT recurring
clock calendar-valid
!
interface Vlan1
 ip address 1.1.1.12 255.255.255.0
 ip helper-address 12.12.12.6
!
ntp logging
ntp clock-period 17179871  --> This is inserted by default, no need to modify
ntp source Vlan1
ntp update-calendar
ntp server 1.1.1.10
!
end
```

NTP Server (Any IOS Router/Switch with IP connectivity to the NTP Client)

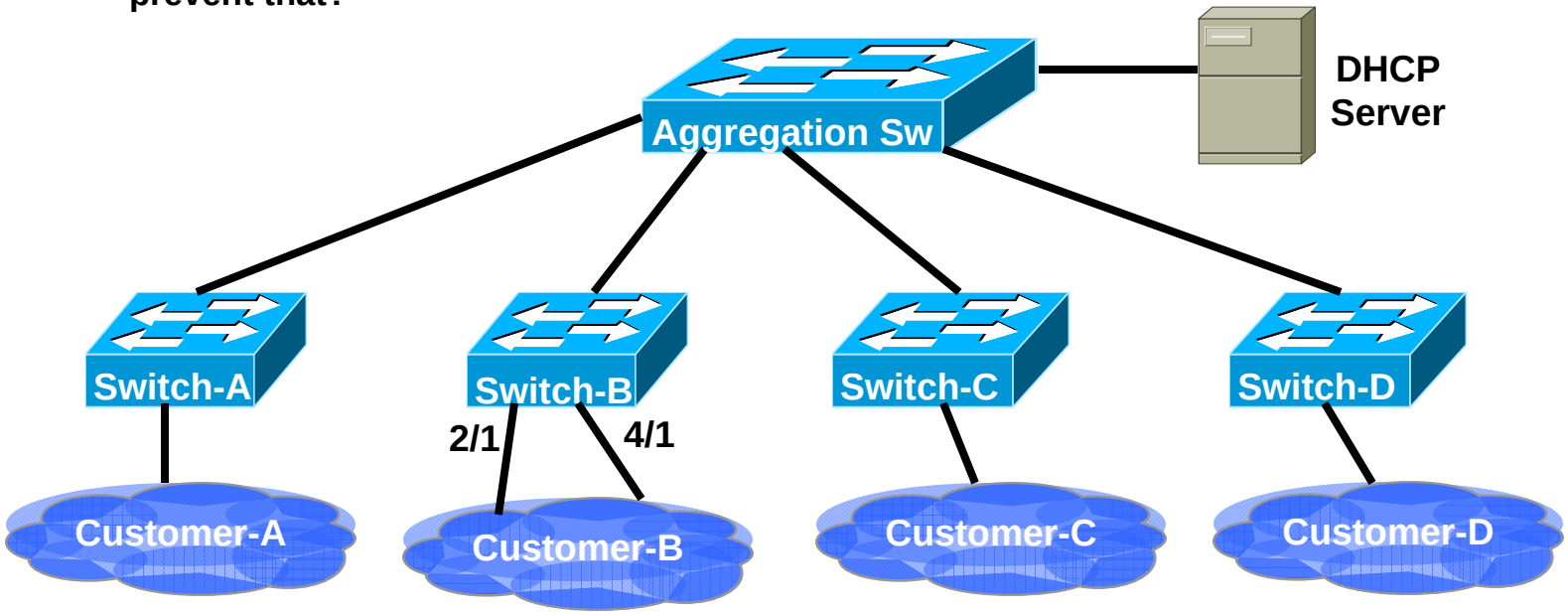
```
Cat4500#sh run
Building configuration...

service timestamps debug uptime
service timestamps log datetime
!
hostname Cat4500
!
interface Vlan1
 ip address 1.1.1.10 255.255.255.0
!
ntp source Vlan1
ntp master 1
ntp update-calendar
ntp peer 1.1.1.12 source Vlan1
end

Cat4500#clock set 19:01:30 19 March 2008 --> Don't forget to set the clock!!
```

Restricting Allocated Addresses

Cisco.com

Customer's Challenge:

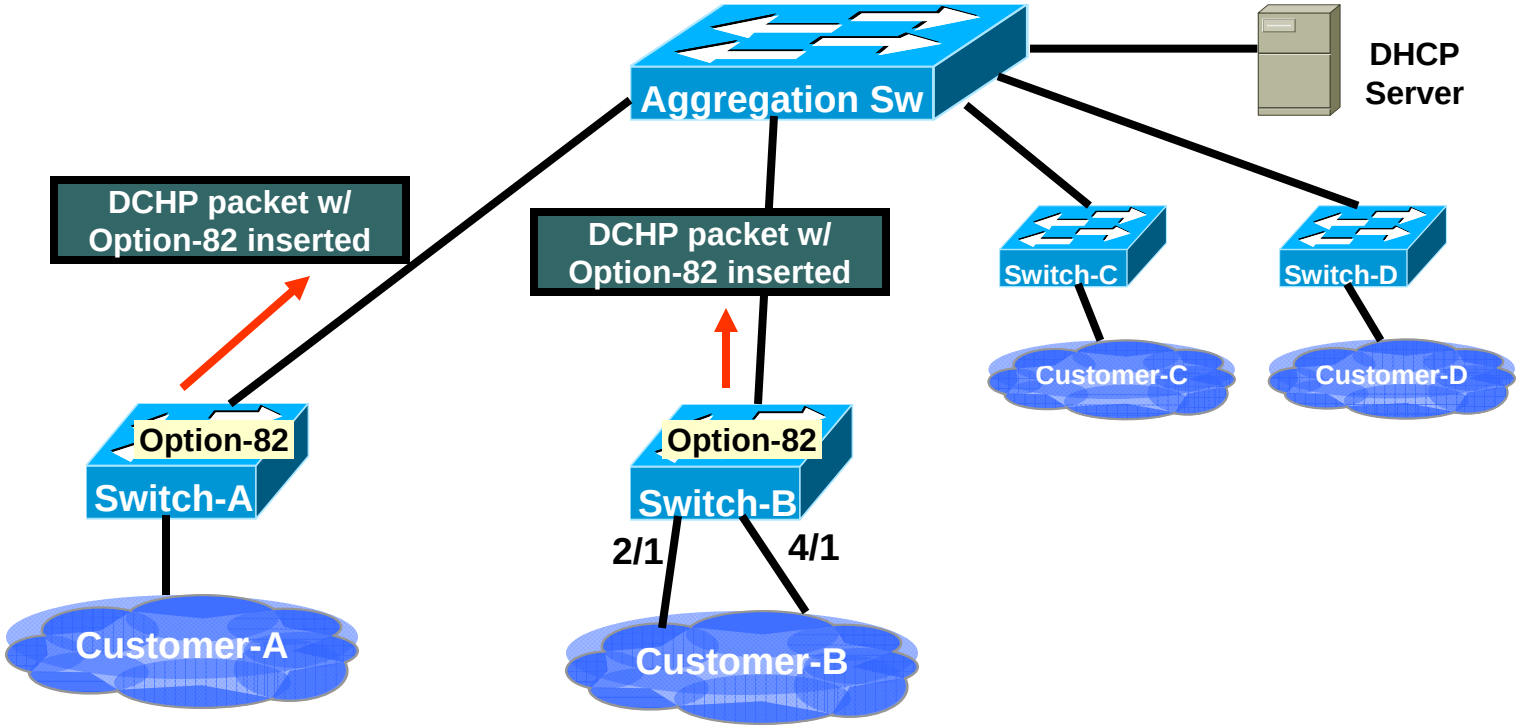
1. **"How can I ensure that each switch is only allocated a maximum of "X" addresses from my DHCP Pool?"**
2. **"How can I ensure that port 2/1 on Switch-B is only allocated a maximum of "X" addresses from my DHCP Pool?"**
3. **"What if someone in Customer-C's network is attempting a DHCP DoS attack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



The Solution: DHCP Option-82

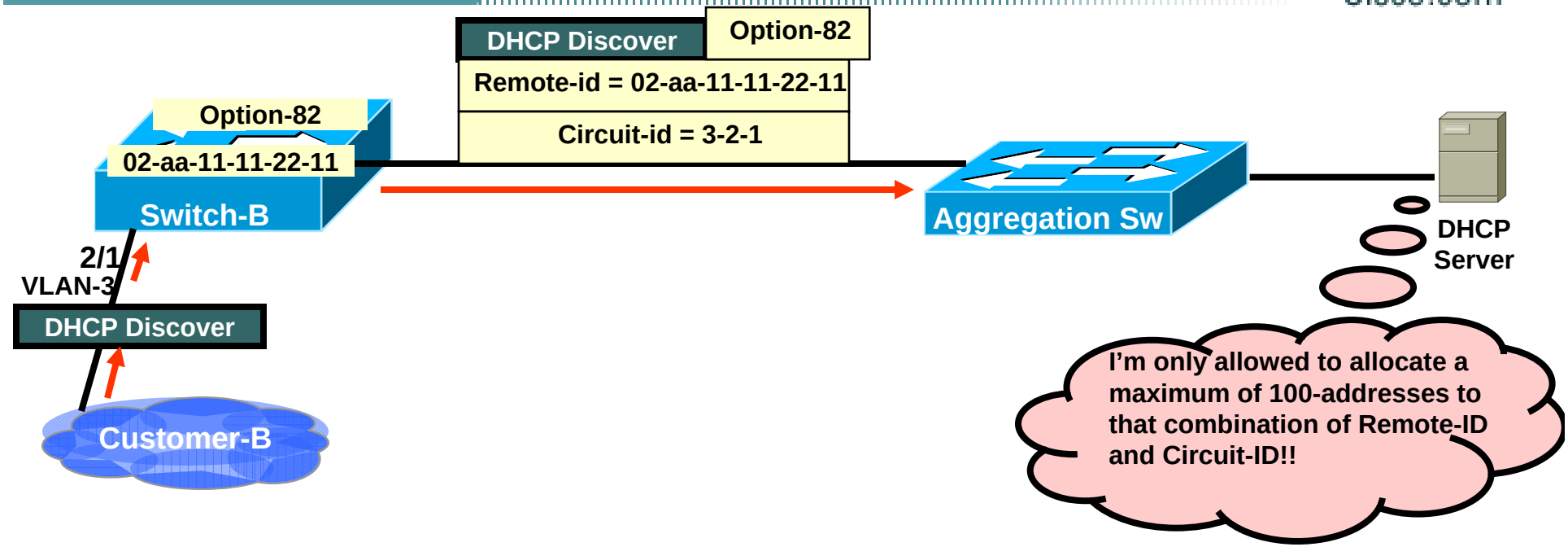
a.k.a. DHCP Relay Agent Option (RFC 3046)

DHCP Option-82



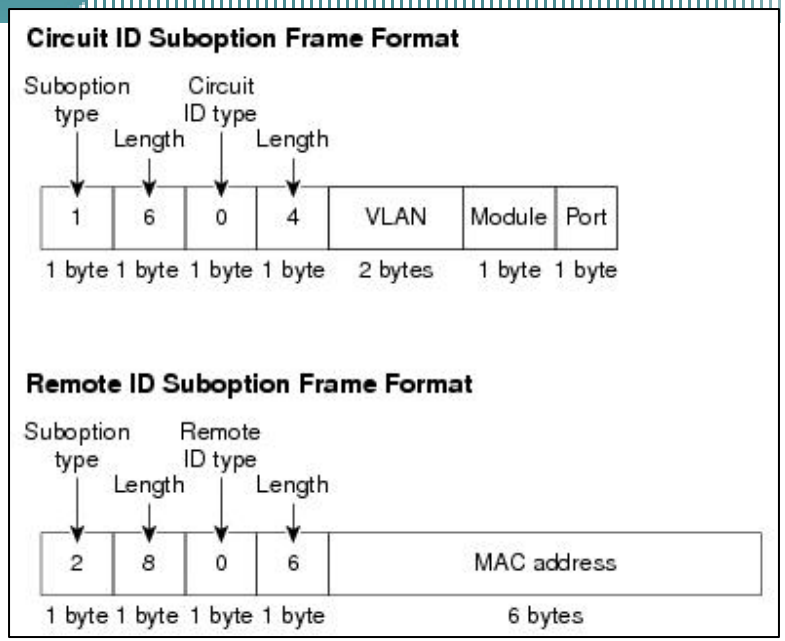
1. Option-82 allows trusted access devices to insert this option into (and remove from) DHCP Packets.
2. This option gives descriptive information about the device/port that received the DHCP message.

DHCP Option-82



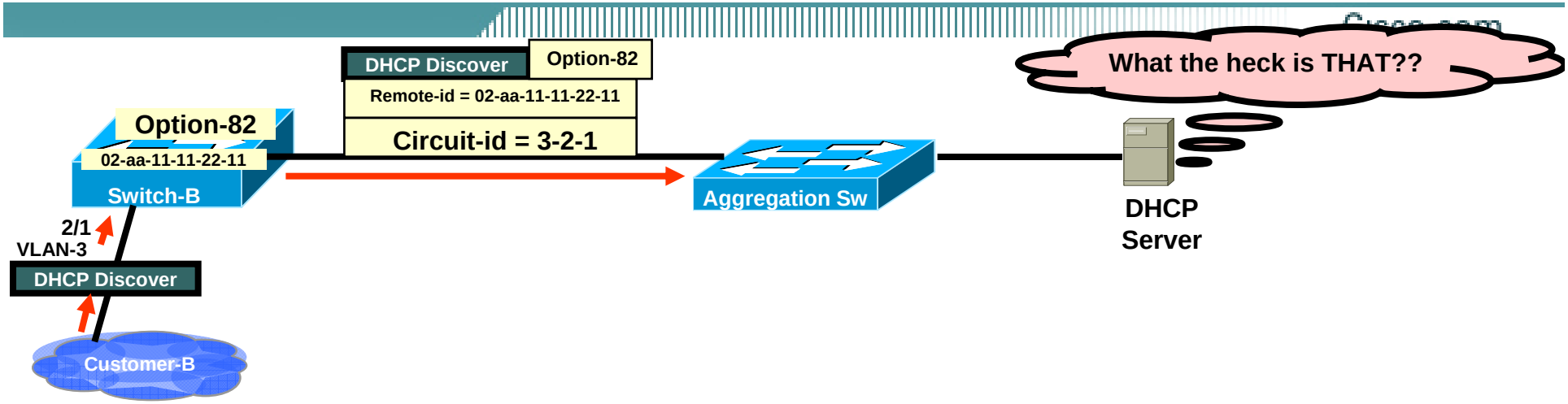
1. Switch adds "Remote-ID" and "Circuit-ID" sub-options into Option-82 data.
   - Remote-ID default is switch MAC address
   - Circuit-ID default is port identifier in the format "vlan-mod-port"
2. These fields are configurable to use ASCII strings if you prefer

DHCP Option-82 – Technical Details




```
Cat6500# Debug ip dhcp snooping packet
Cat6500#
Mar 19 12:33:49.023: dhcp_snooping_draco2_new_dhcp_pak: input idb: Vlan1, vlan 1
Mar 19 12:33:49.023: dhcp_snooping_draco2_new_dhcp_pak:slot = 3, port = 6
Mar 19 12:33:49.023: dhcp_snooping_draco2_new_dhcp_pak:ingress DHCP packet, fixed idb = FastEthern
et3/6
Mar 19 12:33:49.023: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet3/6
)
Mar 19 12:33:49.023: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input int
erface: Fa3/6, MAC da: ffff.ffff.ffff, MAC sa: 0011.5c16.4f60, IP da: 255.255.255.255, IP sa: 0.0.
0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP
chaddr: 0011.5c16.4f60
Mar 19 12:33:49.023: DHCP_SNOOPING: add relay information option.
Mar 19 12:33:49.023: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port format
Mar 19 12:33:49.023: DHCP_SNOOPING: binary dump of relay info option, length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x0 0x1 0x3 0x6 0x2 0x8 0x0 0x6 0x0 0x13 0x5F 0x1D 0x7F 0x80
```

DHCP Option-82 Caveats

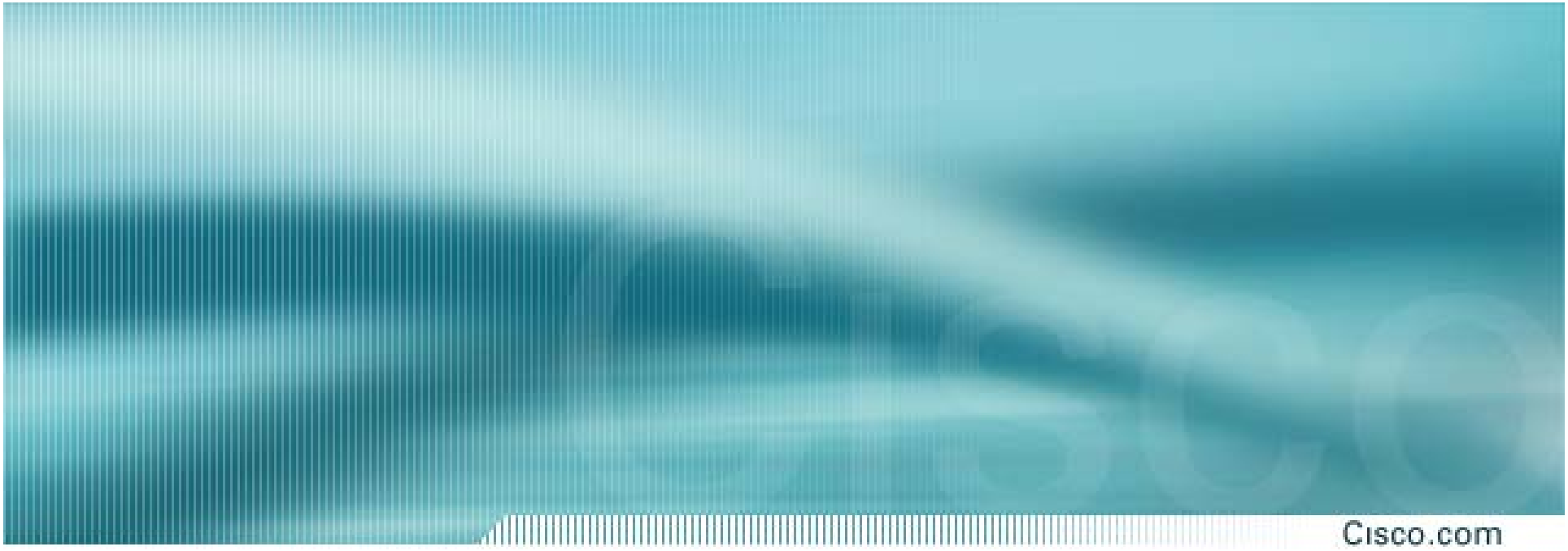


1. DHCP Servers must be configured to recognize and respond in some way to DHCP Option-82 otherwise packets may be dropped.
2. Switches receiving DHCP messages containing Option-82 will DROP THEM if received on an untrusted interface!!
   - The solution for aggregation switches:

     Switch(config)# ip dhcp snooping information option

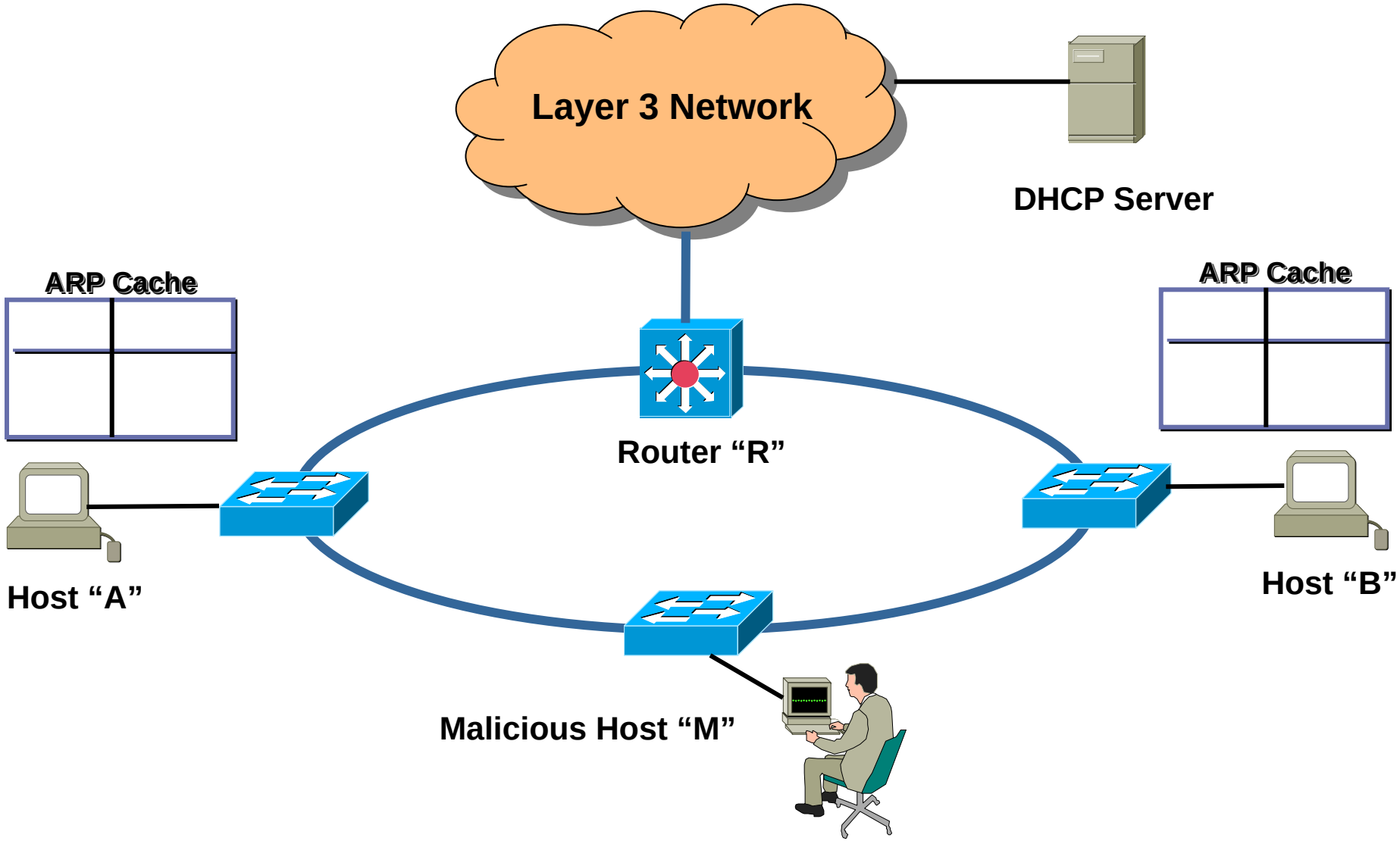
     Switch(config)# ip dhcp snooping information option allow-untrusted

This is the DEFAULT setting. Remove it if unsupported by the DHCP Server.

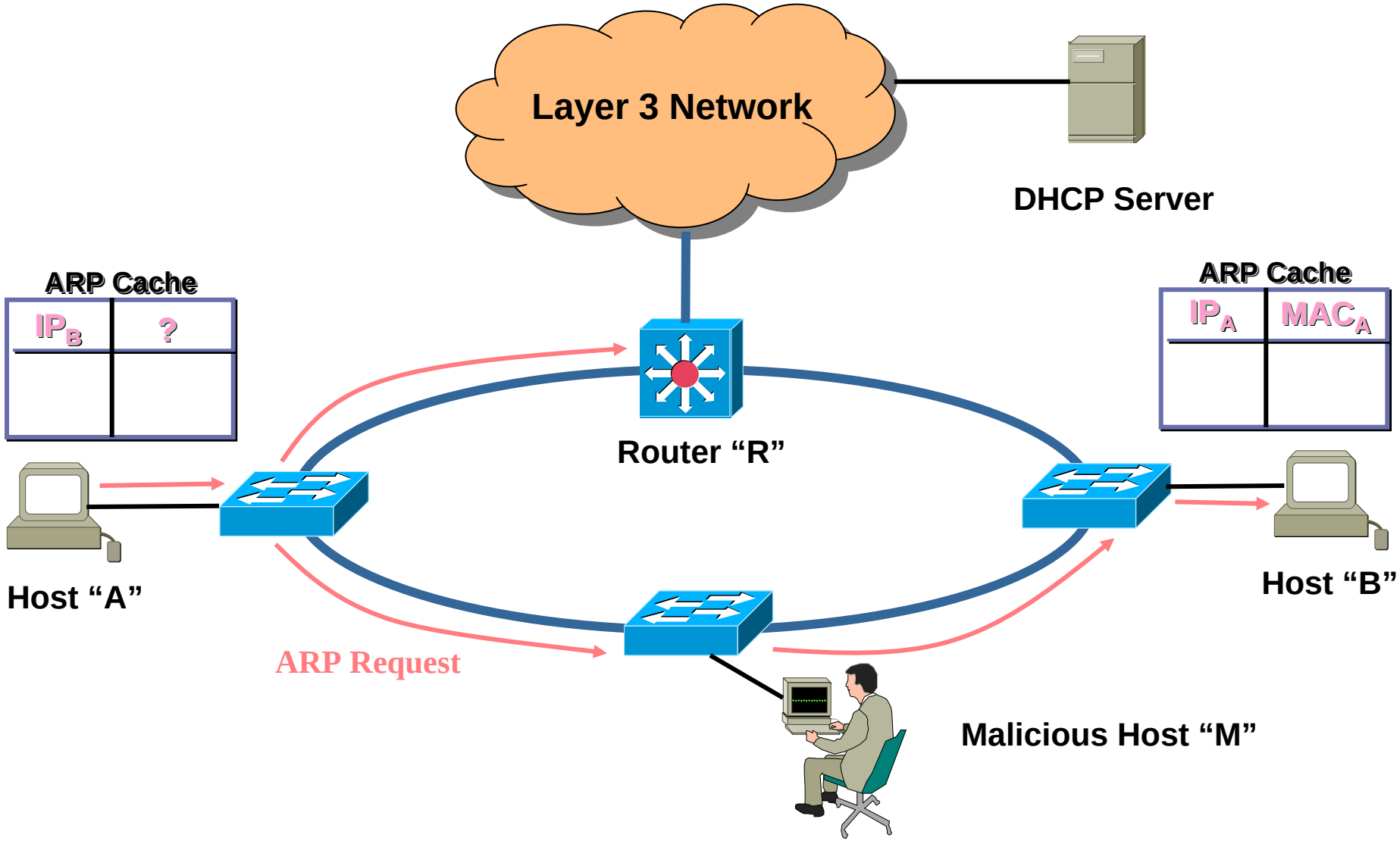


Dynamic ARP Inspection (DAI)

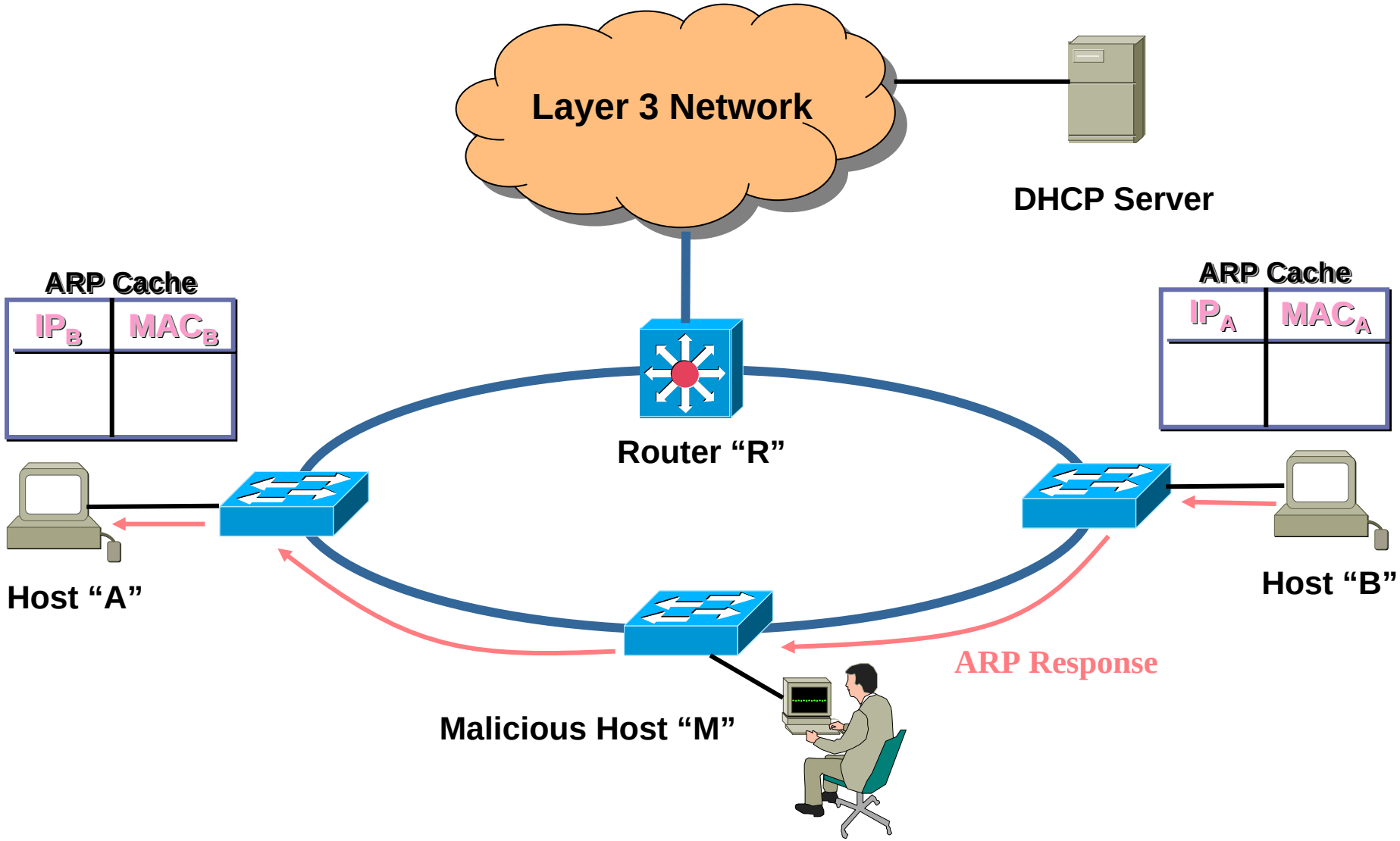
MIM Attack – Attacking another host



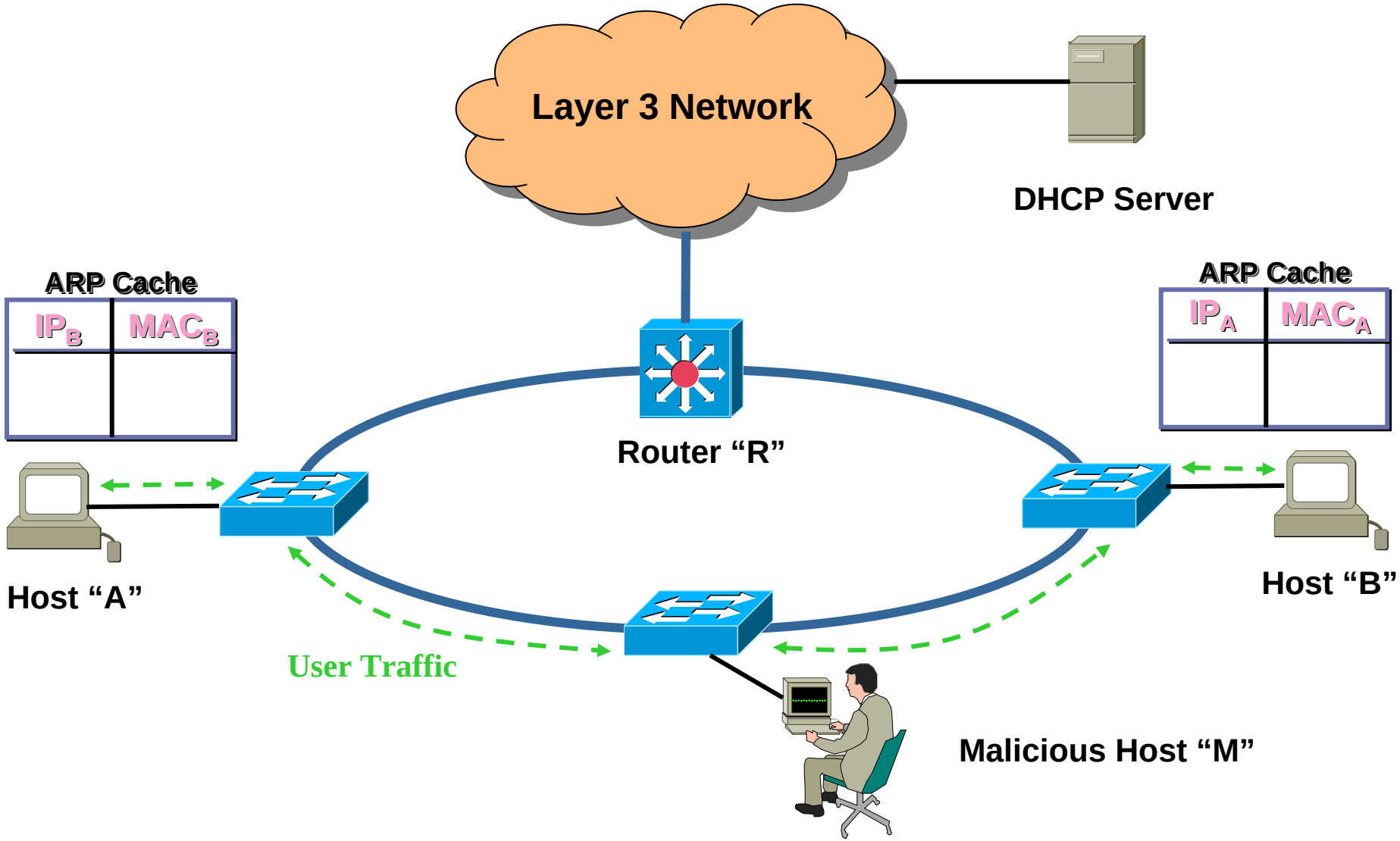
MIM Attack – Attacking another host



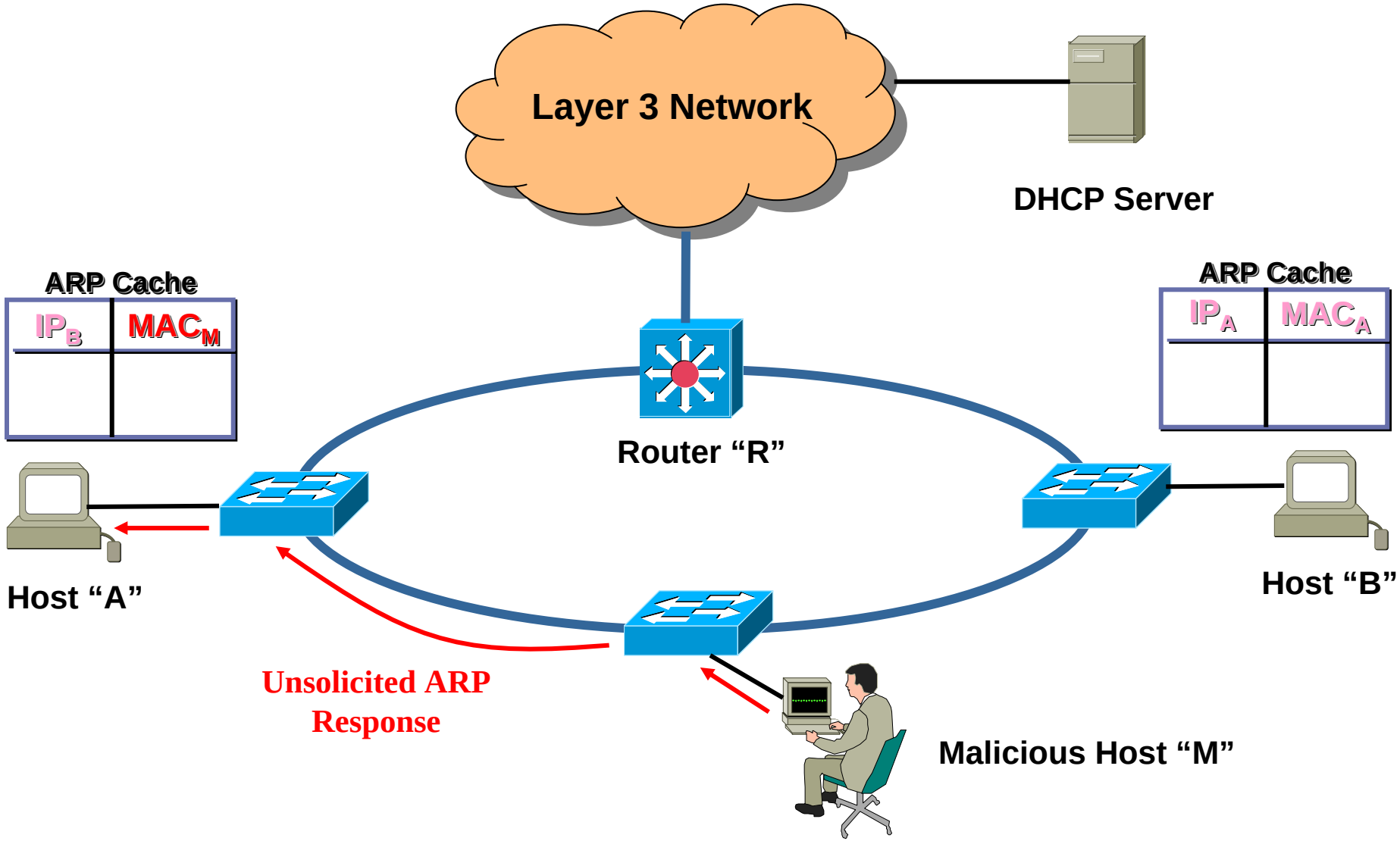
MIM Attack – Attacking another host



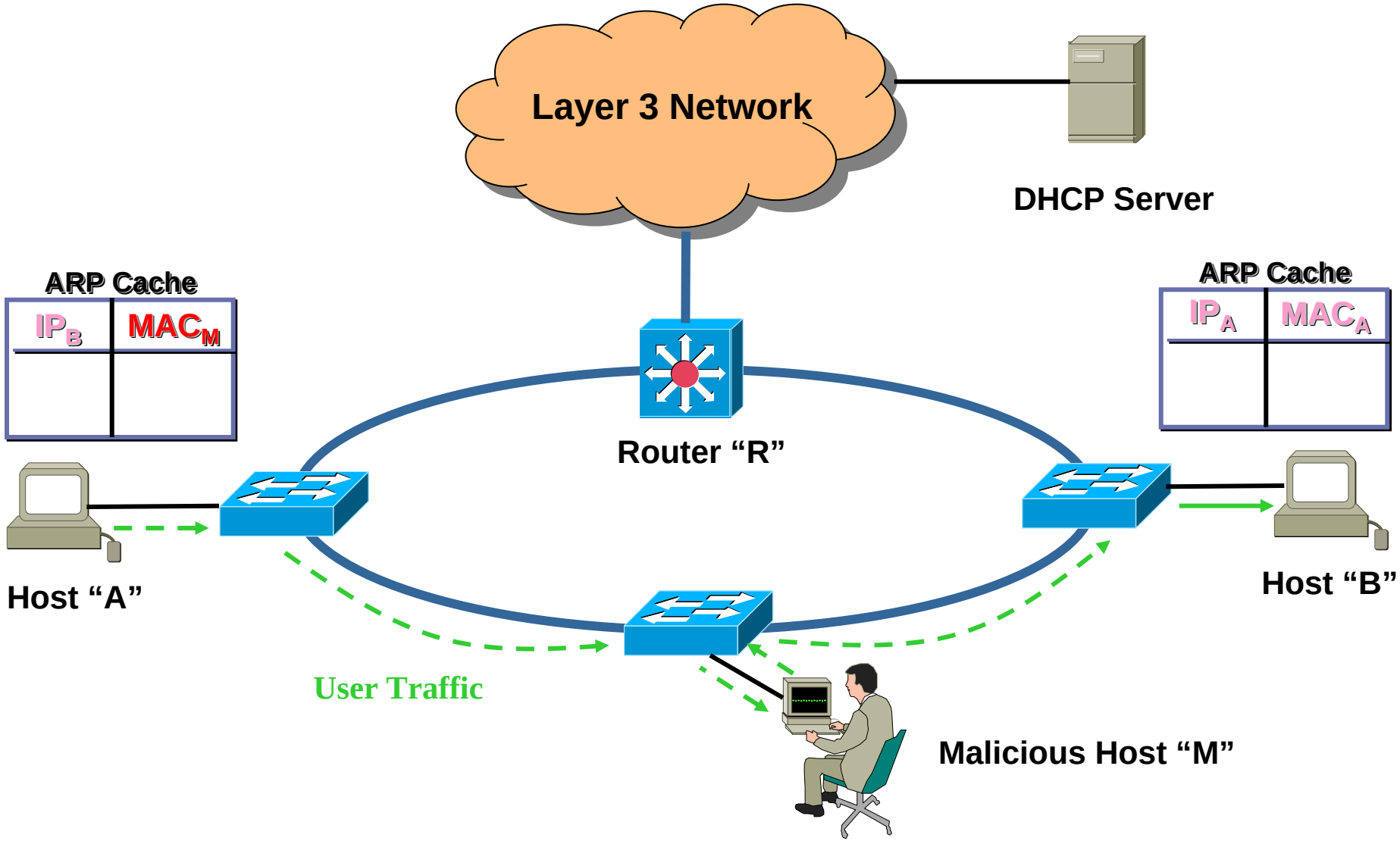
MIM Attack – Attacking another host



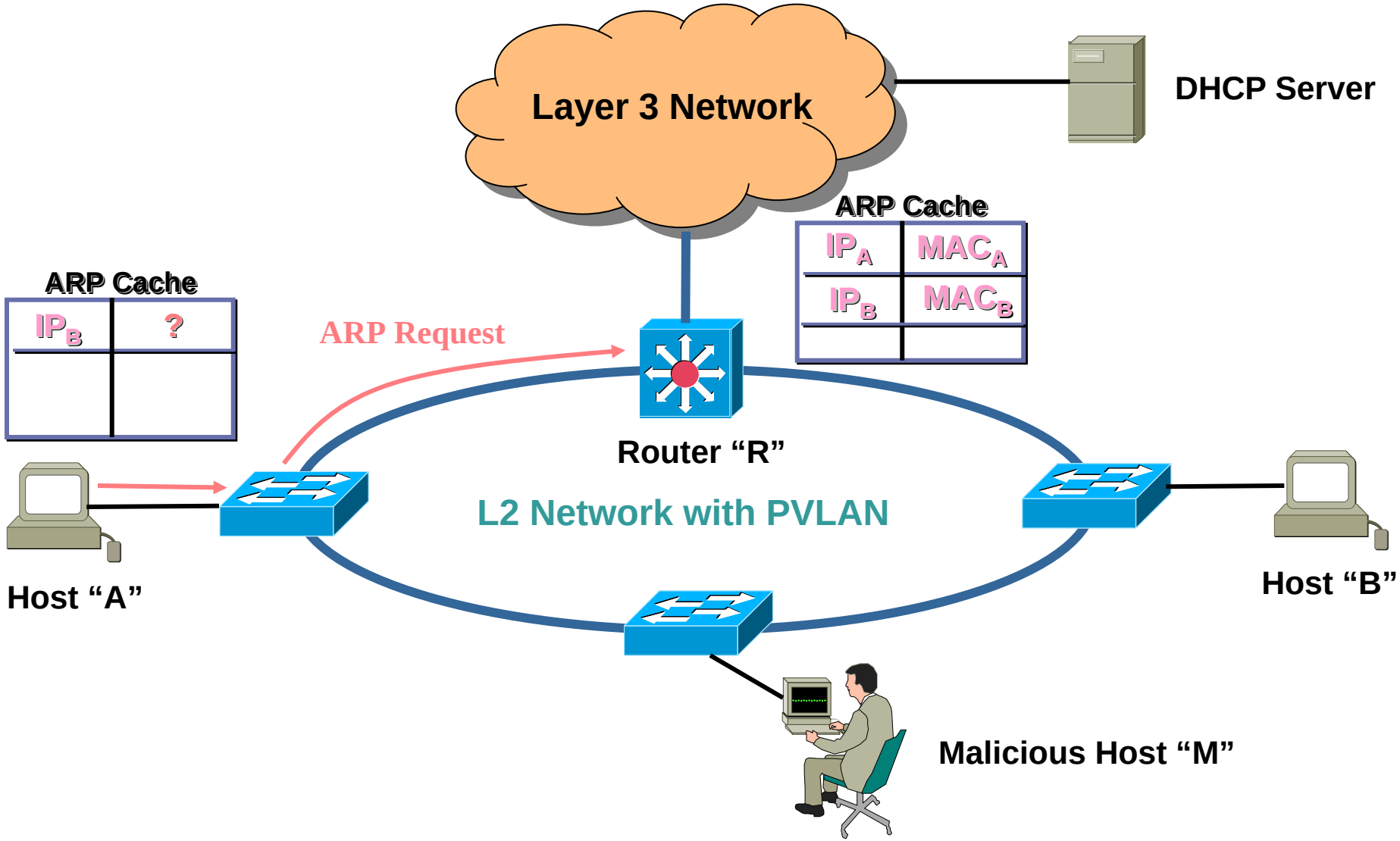
MIM Attack – Attacking another host



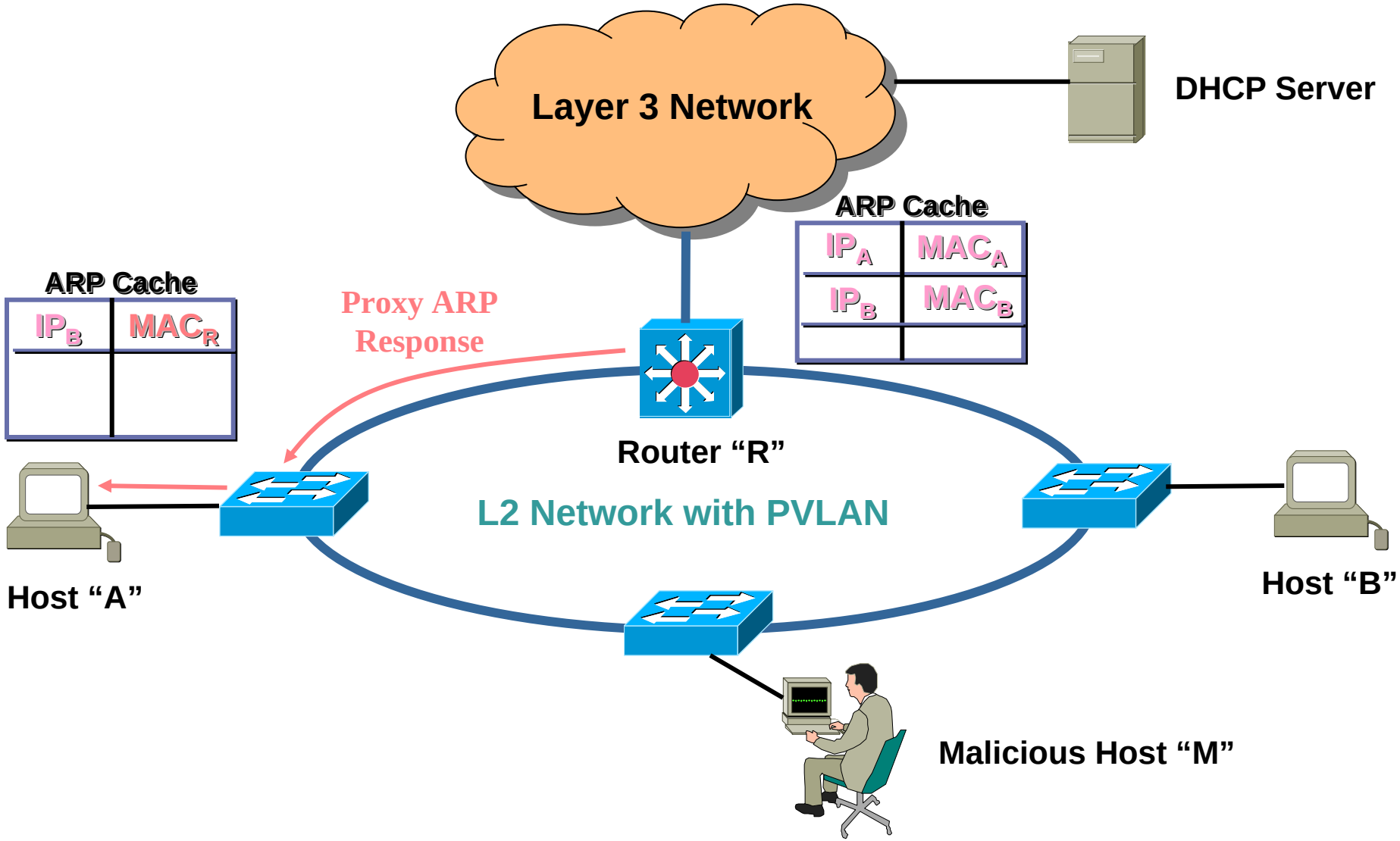
MIM Attack – Attacking another host



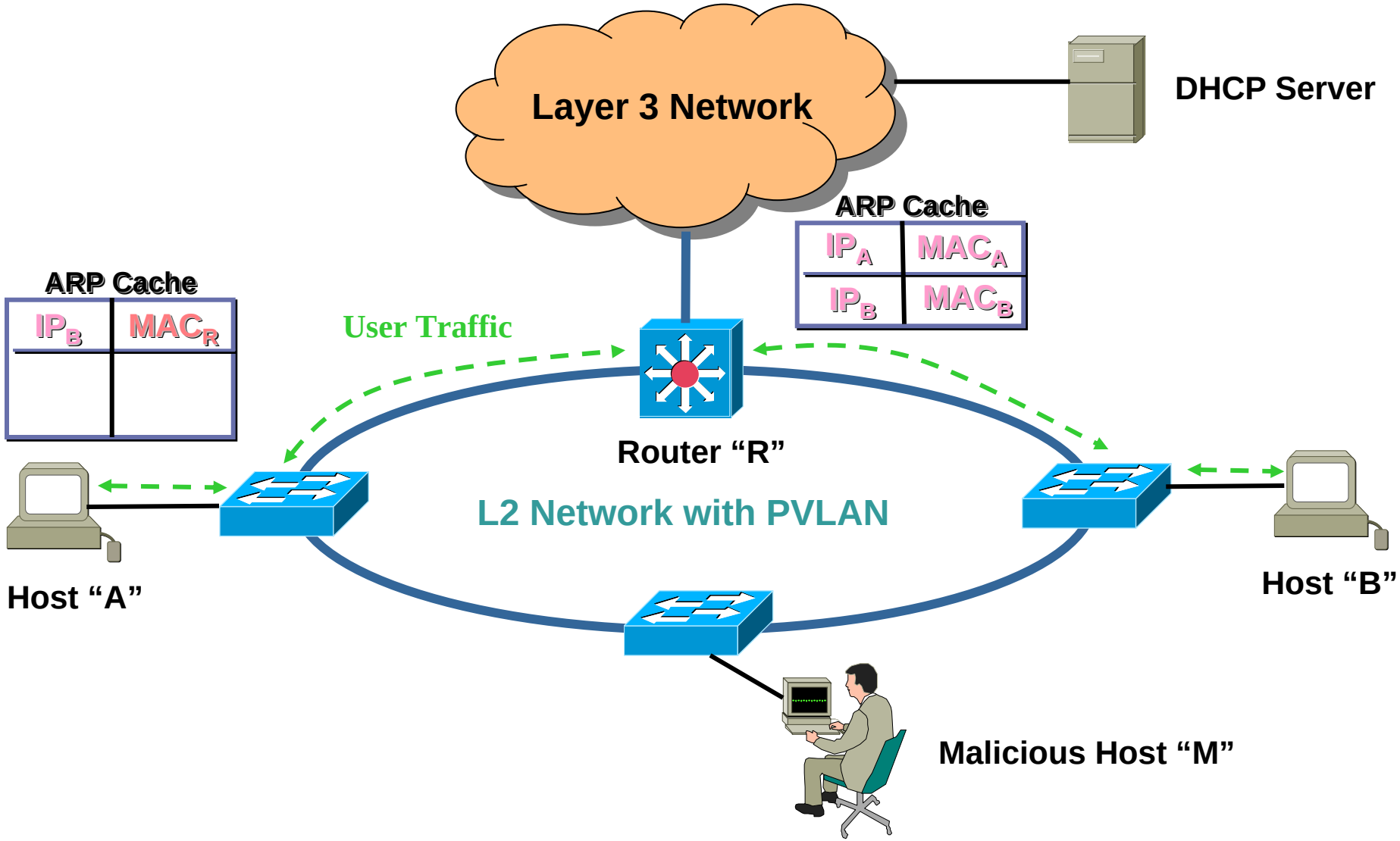
DOS Attack – Attacking the default gateway



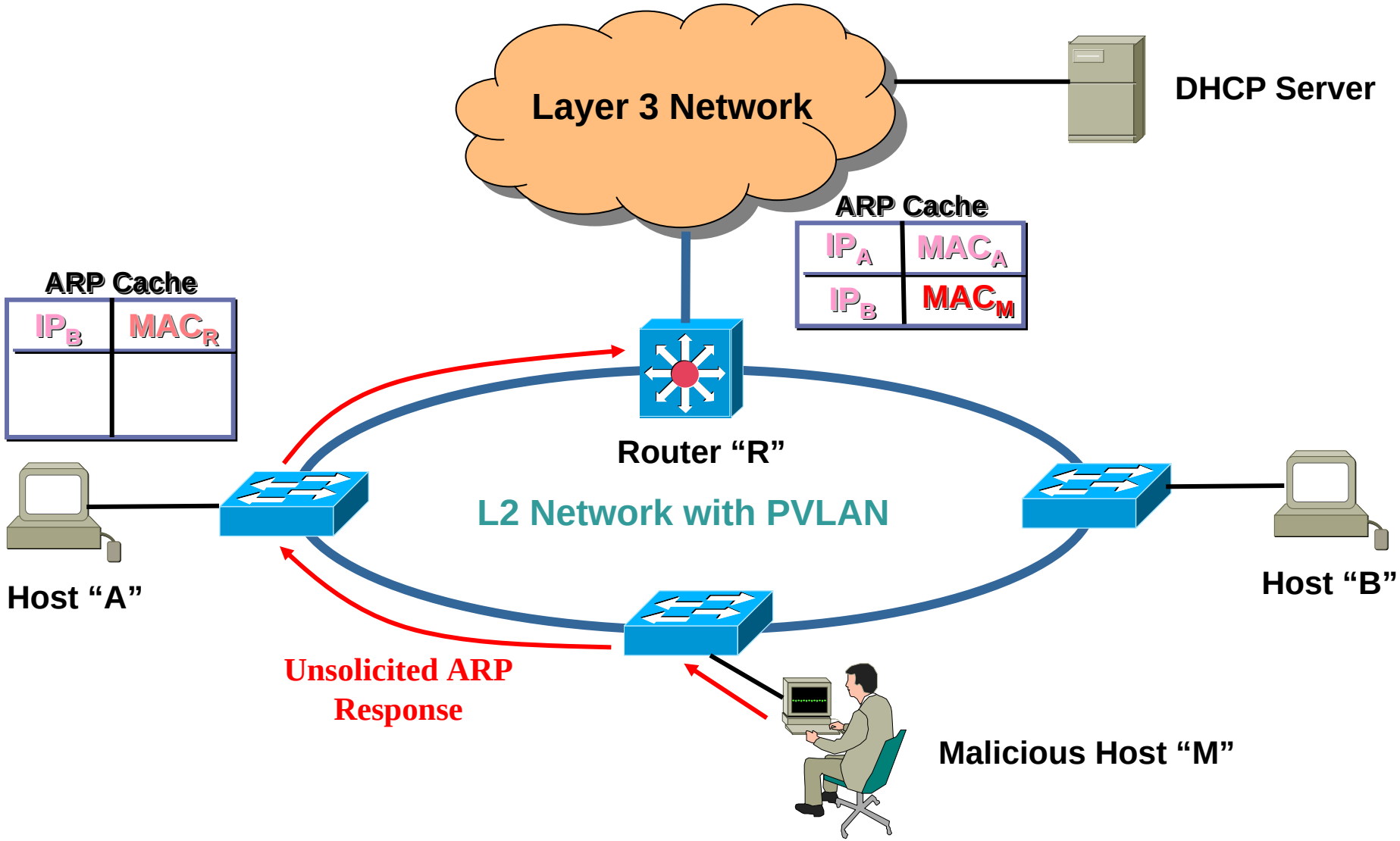
DOS Attack – Attacking the default gateway



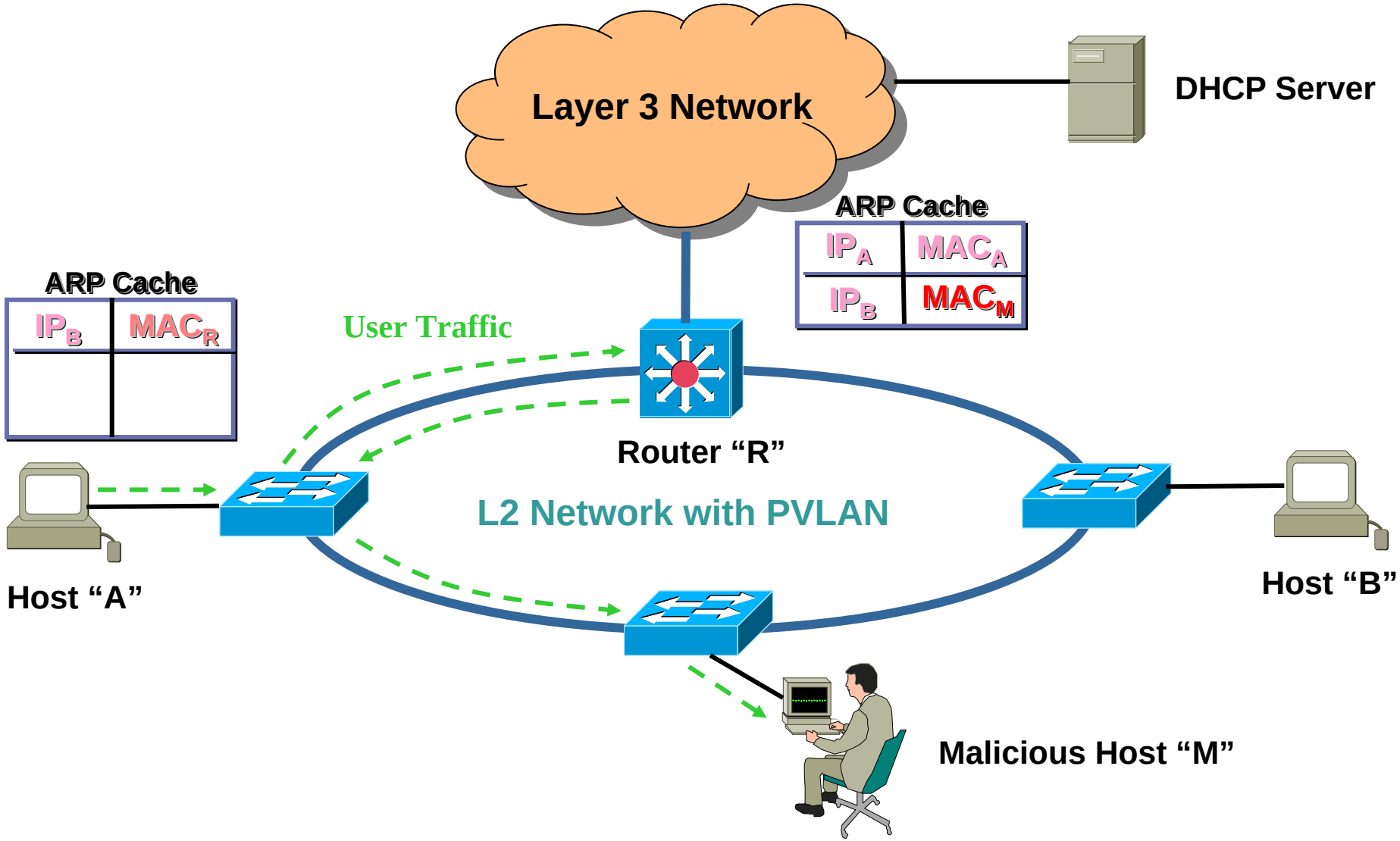
DOS Attack – Attacking the default gateway



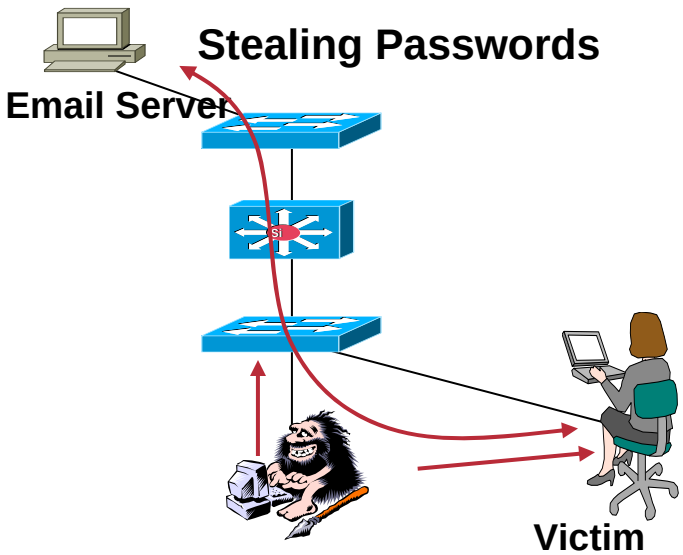
DOS Attack – Attacking the default gateway



DOS Attack – Attacking the default gateway



ARP Poisoning: Serious Business

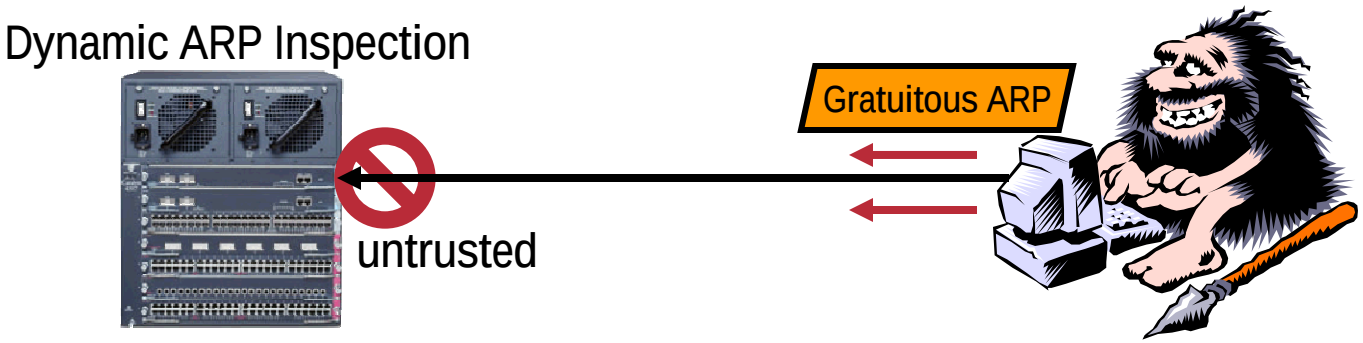


- Avaya demonstrated a variation of ARP poisoning at their customer briefing center using Cisco gear
- After intercepting a network connection, packets containing G.711 voice data are collected and the phone conversation is recorded and then replayed
- Demonstrated live to Cisco senior executives in 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

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

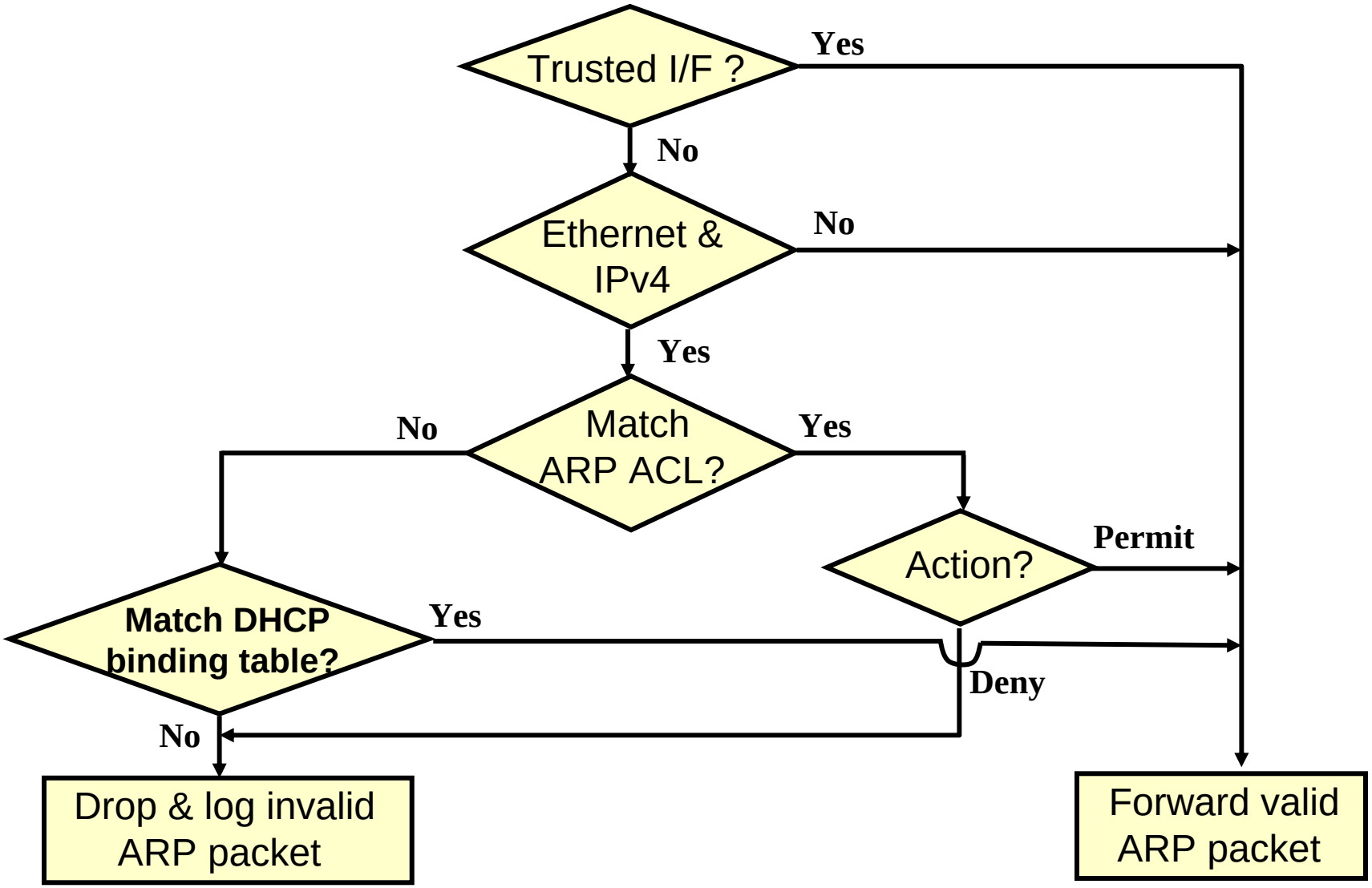
- **Bindings of client IP address, client MAC address, port, VLAN number are built dynamically by DHCP snooping**
- **Switch intercepts all ARP requests and replies on the untrusted access ports**
- **Each intercepted packet is verified for valid IP-to-MAC binding**
- **A solution with no change to the 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.**

ARP Inspection Procedure



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

Dest MAC Addr	Source MAC Addr	Frame Type	H/W Type	Prot Type	H/W Size	Prot Size	Op Code	Sender MAC Addr	Sender IP Addr	Target MAC Addr	Target IP Addr
		0x0806 (ARP)	0x01 (Ethernet)	0x0800 (IPv4)	6	4					

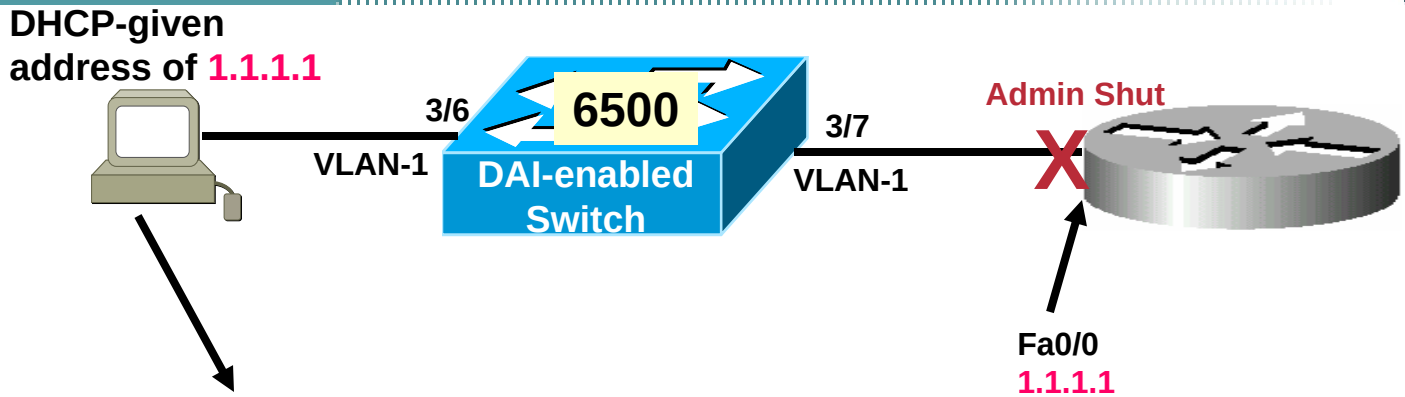
Basic DAI Configuration

Cisco.com

- **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
```

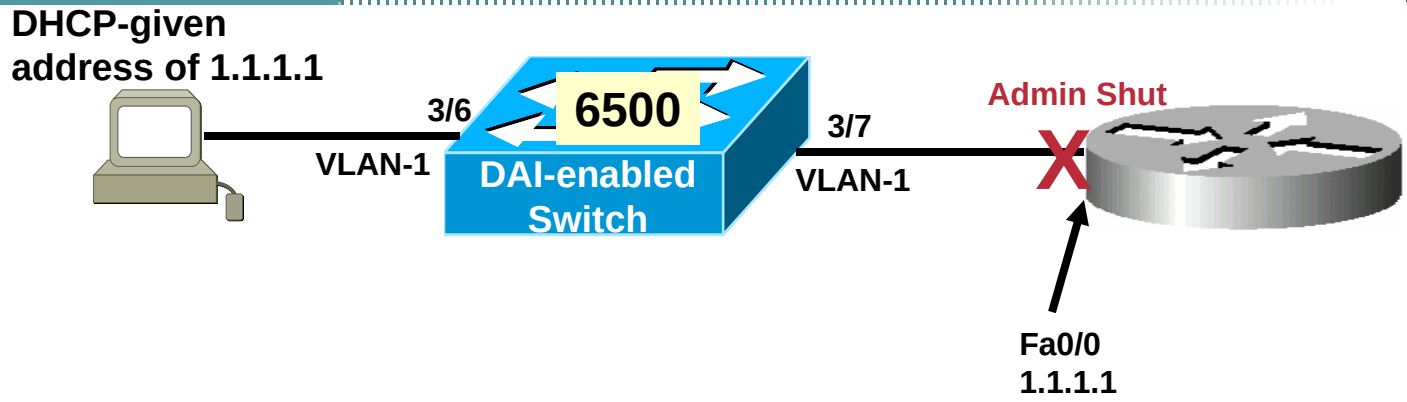
DAI in action!! (1)




```
Cat6500#sho ip dhcp snooping bind
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ------------------
--
00:11:5C:16:4F:60   1.1.1.1          206234      dhcp-snooping   1    FastEthernet3/6
Total number of bindings: 1
```

```
Cat6500#sho 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
```

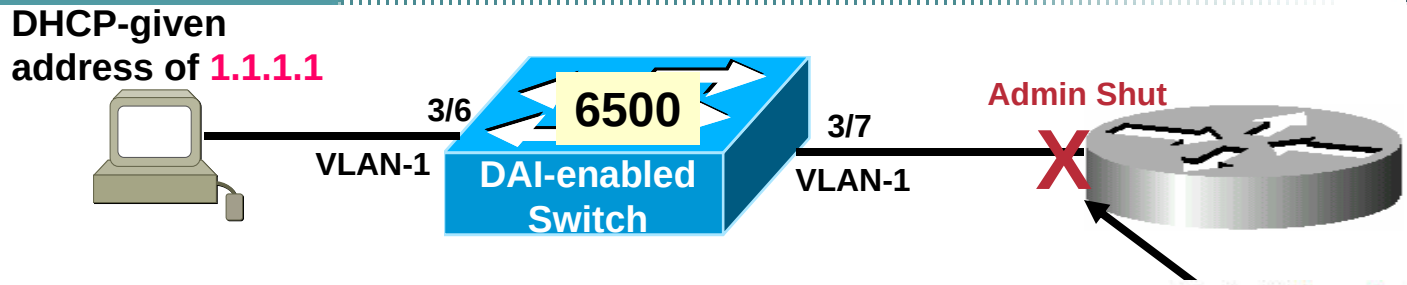
DAI in action!! (2)




```
Cat6500# sho ip arp inspection interface

 Interface          Trust State      Rate (pps)     Burst Interval
 ---------------    -----------      ----------     --------------
 Gi1/1              Untrusted                15                   1
 Gi1/2              Untrusted                15                   1
 Fa3/1              Untrusted                15                   1
 Fa3/2              Untrusted                15                   1
 Fa3/3              Untrusted                15                   1
 Fa3/4              Untrusted                15                   1
 Fa3/5              Untrusted                15                   1
 Fa3/6              Untrusted                15                   1
 Fa3/7              Untrusted                15                   1
```

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)




```
Router(config)#int fast 0/0
Router(config-if)#no shutdown
Router(config-if)#^Z
Router#
*Apr 27 02:42:29.805: IP ARP: sent rep src 1.1.1.1 0011.5c10.8340,
                      dst 1.1.1.1 ffff.ffff.ffff FastEthernet0/0
```

```
Router#sh run int fast0/0
!
interface FastEthernet0/0
 ip address 1.1.1.1 255.255.255.0
 shutdown
 duplex auto
 speed auto
```

```
Cat6500#
.Mar 20 08:59:28.610: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa3/7, vlan
1.([0011.5c10.8340/1.1.1.1/ffff.ffff.ffff/1.1.1.1/08:59:27 PDT Thu Mar 20 2008])
Cat6500#
```

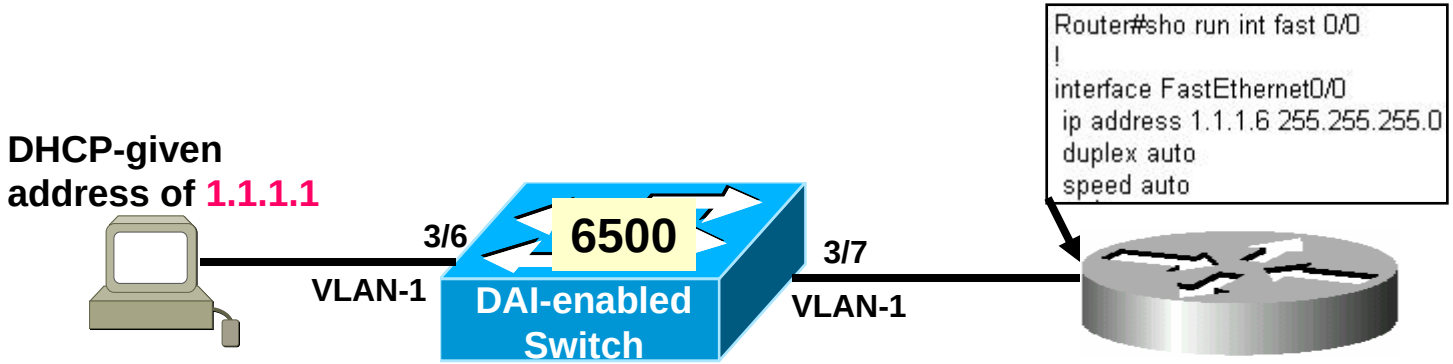
Gratuitous ARP from Router is dropped by DAI on switch.

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!

```
PC#ping 1.1.1.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.6, timeout is 2 seconds:

*Mar 23 04:52:14.175: IP ARP: creating incomplete entry for IP address: 1.1.1.6
interface FastEthernet0/0
*Mar 23 04:52:14.175: IP ARP: sent req src 1.1.1.1 0011.5c16.4f60,
                      dst 1.1.1.6 0000.0000.0000 FastEthernet0/0.
```

```
Cat6500#
.Mar 20 09:31:37.550: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa3/7, vlan
1.([0011.5c10.8340/1.1.1.6/0011.5c16.4f60/1.1.1.1/09:31:37 PDT Thu Mar 20 2008])
```



DAI for non-DHCP hosts (2)

The Solution: ARP Access-List

```
Cat6500#sh run
!
ip arp inspection vlan 1-12
ip arp inspection filter test vlan  1
!
arp access-list test
 permit response ip host 1.1.1.6 any mac host 0011.5c10.8340 any
```

Sender of ARP Response

"any" target IP address

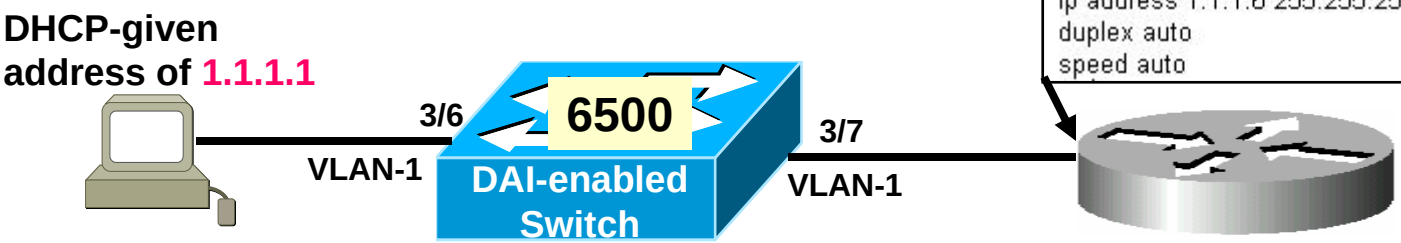
Senders MAC address

"any" target MAC address

```
PC#ping 1.1.1.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
Router#show int fast 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0011.5c10.8340
```

```
Router#sho run int fast 0/0
!
interface FastEthernet0/0
 ip address 1.1.1.6 255.255.255.0
 duplex auto
 speed auto
```



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".

Without the "static" keyword DAI will continue to look for a matching entry in the DHCP Snooping Database if nothing matches the ACL.

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
```

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

Cisco.com

- **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.**

```
Cat6500#
.Mar 20 16:36:50.180: %SW_DAI-4-PACKET_RATE_EXCEEDED: 16 packets received in 32
milliseconds on Fa3/7.
.Mar 20 16:36:50.592: %SW_DAI-4-DHCP_SNOOPING_DENY: 16 Invalid ARPs (Req) on Fa3
/7, vlan 1.([0011.5c10.8340/1.1.1.6/0011.5c10.8340/1.1.1.6/16:36:50 PDT Thu Mar
20 2008])
Mar 20 16:36:50.184: %PM-SP-4-ERR_DISABLE: arp-inspection error detected on Fa3/
7, putting Fa3/7 in err-disable state
```

CISCO SYSTEMS

EMPOWERING THE
INTERNET GENERATION