UNDERSTANDING, PREVENTING, AND DEFENDING AGAINST LAYER 2 ATTACKS

SESSION SEC-2002

Agenda

• Layer 2 Attack Landscape
• Attacks and Countermeasures
  VLAN “Hopping”
  MAC Attacks
  DHCP Attacks
  ARP Attack
  Spoofing Attacks
  Other Attacks
• Summary
Caveats

- All attacks and mitigation techniques assume a switched Ethernet network running IP
  
  If it is a shared Ethernet access (WLAN, Hub, etc) most of these attacks get much easier
  
  If you are not using Ethernet as your L2 protocol, some of these attacks may not work, but chances are, you are vulnerable to different ones

- New theoretical attacks can move to practical in days

- All testing was done on Cisco Ethernet Switches
  
  Ethernet switching attack resilience varies widely from vendor to vendor

- This is not a comprehensive talk on configuring Ethernet switches for security; the focus is on L2 attacks and their mitigation.

Reference Materials

- SAFE Blueprints
  
  http://www.cisco.com/go/safe

- Cisco Catalyst® 4000 Security Features
  
  Best Practices for Supervisor
  
  
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_1_20/cmdref/snmp_vtp.htm#1144883

- Cisco Catalyst® 6500
  

- Cisco Catalyst® 3750
  
  http://www.cisco.com/univercd/cc/td/doc/product/lan/c3550/12120ea2/
Associated Sessions

- SEC-2000: Secure Enterprise Design
- SEC-2004: Responding to Security Incidents
- SEC-2030: Deploying Network-Based Intrusion Detection and Prevention Systems
- SEC-2031: Understanding and Deploying Host-Based Intrusion Protection Technology
- SEC-2040: Understanding and Deploying Network Admission Control

Recommended Reading

- Stealing the Network: How to Own the Box by Ryan Russell, Tim Mullen, Dan Kaminsky, Joe Grand, Ken Pfeil, Ido Dubrawsky, Mark Burnett, Paul Craig, ISBN: 1931836876
- Defense and Detection Strategies Against Internet Worms by Jose Nazario, ISBN: 1580533572

Available on-site at the Cisco Company Store
Why Worry about Layer 2 Security?

OSI Was Built to Allow Different Layers to Work Without the Knowledge of Each Other

Host A

Application
Presentation
Session
Transport
Network
Data Link
Physical

Application Stream
Protocols/Ports
IP Addresses
MAC Addresses
Physical Links

Host B

Application
Presentation
Session
Transport
Network
Data Link
Physical
Lower Levels Effect Higher Levels

- Unfortunately this means if one layer is hacked, communications are compromised without the other layers being aware of the problem
- Security is only as strong as the weakest link
- When it comes to networking, layer 2 can be a VERY weak link

NetOPS/SecOPS, Who’s Problem Is It?

Questions:

- What is your stance on L2 security issues?
- Do you use VLANs often?
- Do you ever put different security levels on the same switch using VLANs?
- What is the process for allocating addresses for segments?

Most NetOPS:

- There are L2 Security issues?
- I use VLANs all the time
- Routing in and out of the same switch is OK by me! That’s what VLANs are for
- The security guy asks me for a new segment, I create a VLAN and assign him an address space

Most SecOPS:

- I handle security issues at L3 and above
- I have no idea if we are using VLANs
- Why would I care what the network guy does with the switch?
- I ask Netops for a segment, they give me ports and addresses
FBI/CSI Risk Assessment

- CSI/FBI survey shows information theft as the #1 growing trend
- 99% of all enterprises network ports are OPEN
- Any laptop can plug into the network and gain access to the network
- 75% of attacks that caused monetary loses were from the inside.
- Highest source of loss was theft of proprietary information—with a average of 2.7 million per incident
- Insider attack by disgruntled employees was listed as likely source by 77% of respondents

ATTACKS AND COUNTERMEASURES: VLAN HOPPING ATTACKS
Basic Trunk Port Defined

- Trunk ports have access to all VLANs by default
- Used to route traffic for multiple VLANs across the same physical link (generally between switches or phones)
- Encapsulation can be 802.1q or ISL

Dynamic Trunk Protocol (DTP)

- What is DTP?
  Automates 802.1x/ISL Trunk configuration
  Operates between switches (Cisco IP phone is a Switch)
  Does not operate on routers
  Support on the 29xx.35xx??
- DTP synchronizes the trunking mode on end links
- DTP state on 802.1q/ISL trunking port can be set to “Auto”, “On”, “Off”, “Desirable”, or “Non-Negotiate”
Basic VLAN Hopping Attack

• An end station can spoof as a switch with ISL or 802.1q
• The station is then a member of all vlans
• Requires a trunking configuration of the Native VLAN to be VLAN 1

Double 802.1q Encapsulation VLAN Hopping Attack

• Send 802.1q double encapsulated frames
• Switch performs only one level of decapsulation
• Unidirectional traffic only
• Works even if trunk ports are set to off

Note: Only works if Trunk has the same VLAN as the Attacker
Security Best Practices for VLANs and Trunking

- Always use a dedicated VLAN ID for all trunk ports
- Disable unused ports and put them in an unused VLAN
- Be paranoid: Do not use VLAN 1 for anything
- Disable auto-trunking on user facing ports (DTP off)
- Explicitly configure trunking on infrastructure ports
- Use all tagged mode for the native VLAN on trunks

ATTACKS AND COUNTERMEASURES:
MAC ATTACKS
MAC Address/CAM Table Review

48 Bit Hexadecimal Number Creates Unique Layer Two Address

1234.5678.9ABC

First 24 bits = Manufacture Code Assigned by IEEE
Second 24 bits = Specific Interface, Assigned by Manufacture

0000.0cXX.XXXX  0000.0cXX.XXXX

All F’s = Broadcast

FFFF.FFFF.FFFF

- CAM Table stands for Content Addressable Memory
- The CAM Table stores information such as MAC addresses available on physical ports with their associated VLAN parameters
- CAM Tables have a fixed size

Normal CAM Behavior 1/3

MAC Port
A 1
C 3

ARP for B

MAC A

B Is Unknown—Flood the Frame

Port 1

Port 2

ARP for B

MAC B

MAC C

Port 3

ARP for B
**Normal CAM Behavior 2/3**

<table>
<thead>
<tr>
<th>MAC</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1</td>
</tr>
<tr>
<td>B</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
</tr>
</tbody>
</table>

- **MAC A** is on Port 1.
- **MAC B** is on Port 2.
- **MAC C** is on Port 3.

**Learn:** B is on Port 2.

**A** is on Port 1.

**Normal CAM Behavior 3/3**

<table>
<thead>
<tr>
<th>MAC</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1</td>
</tr>
<tr>
<td>B</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
</tr>
</tbody>
</table>

- **Traffic A -> B**
- **MAC A**
- **MAC B**

**Does Not See Traffic to B**

**MAC C**
CAM Overflow 1/3

- macof tool since 1999
  About 100 lines of perl
  Included in “dsniff”
- Attack successful by exploiting the size limit on CAM tables

CAM Overflow 2/3

<table>
<thead>
<tr>
<th>MAC</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>3</td>
</tr>
<tr>
<td>Z</td>
<td>3</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
</tr>
</tbody>
</table>

Assume CAM Table Now Full

Port 1
- Traffic A -> B
- Z Is on Port 3

Port 2
- Traffic A -> B
- Y Is on Port 3

Port 3
- Traffic A -> B
- I See Traffic to B!

MAC A

MAC B

MAC C
Catalyst CAM Tables

- Catalyst switches use hash to place MAC in CAM table

|   | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| 1 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 2 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 3 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 16,000 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |

- 63 bits of source (MAC, VLAN, misc) creates a 14 bit hash value
- If the value is the same there are 8 buckets to place CAM entries, if all 8 are filled the packet is flooded

Mac Flooding Switches with macof

- Macof sends random source MAC and IP addresses
- Much more aggressive if you run the command

```
macof -i eth1
```

```
macof -i eth1 2> /dev/null
```

macof (part of dsniff) - [http://monkey.org/~dugsong/dsniff/](http://monkey.org/~dugsong/dsniff/)
Mac Flooding Switches with macof

- Once the CAM table on the switch is full, traffic without a CAM entry is flooded out every port on that VLAN
- This will turn a VLAN on a switch basically into a hub
- This attack will also fill the CAM tables of adjacent switches

CAM Table FULL!

10.1.1.22 -> (broadcast) ARP C Who is 10.1.1.1, 10.1.1.1 ?
10.1.1.22 -> (broadcast) ARP C Who is 10.1.1.19, 10.1.1.19 ?
10.1.1.26 -> 10.1.1.25    ICMP Echo request (ID: 256 Sequence number: 7424) 💥
10.1.1.25 -> 10.1.1.26    ICMP Echo reply (ID: 256 Sequence number: 7424) 💥
Countermeasures for MAC Attacks

Port Security Limits the Amount of MAC’s on an Interface

Solution:
• Port security limits MAC flooding attack and locks down port and sends an SNMP trap

Only 3 MAC Addresses Allowed on the Port: Shutdown

132,000 Bogus MACs

Solution:
• Port security limits MAC flooding attack and locks down port and sends an SNMP trap

Port Security: Example Config

CatOS
set port security 5/1 enable
set port security 5/1 port max 3
set port security 5/1 violation restrict
set port security 5/1 age 2
set port security 5/1 timer-type inactivity

IOS
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity

3 MAC addresses encompass the phone, the switch in the phone, and the PC
“Restrict” rather than “error disable” to allow only 3, and log more than 3
Aging time of 2 and aging type inactivity to allow for phone CDP of 1 minute

If violation error–disable, the following log message will be produced:
4w6d: %PM-4-ERR_DISABLE: psecure-violation error detected on Gi3/2, putting Gi3/2 in err-disable state
Port Security

Not All Port Security Created Equal

• In the past you would have to type in the ONLY MAC you were going to allow on that port
• You can now put a limit to how many MAC address a port will learn
• You can also put timers in to state how long the MAC address will be bound to that switch port
• You might still want to do static MAC entries on ports that there should be no movement of devices, as in server farms
• If you are going to be running Cisco IPT, you will need a minimum of 3 MAC addresses on each port
• New feature called “Sticky Port Security”, settings will survive reboot (not on all switches)

Port Security: What to Expect

Notice: When Using the Restrict Feature of Port Security, if the Switch Is Under Attack, You Will See a Performance Hit on the CPU

• The performance hit seen with multiple attacks happening at one time is up to 99% CPU utilization
• Because the process is a low priority, on all switches packets were not dropped
• Telnet and management were still available
Building the Onion

- Port security prevents CAM attacks

ATTACKS AND COUNTERMEASURES:
DHCP ATTACKS
DHCP Function: High Level

- Server dynamically assigns IP address on demand
- Administrator creates pools of addresses available for assignment
- Address is assigned with lease time
- DHCP delivers other configuration information in options

DHCP Function: Lower Level

- DHCP Defined by RFC 2131
- DHCP Discover (Broadcast)
  - DHCP Offer (Unicast)
  - DHCP Request (Broadcast)
  - DHCP Ack (Unicast)
DHCP Function: Lower Level

IPv4 DHCP Packet Format

<table>
<thead>
<tr>
<th>OP Code</th>
<th>Hardware Type</th>
<th>Hardware Length</th>
<th>HOPS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction ID (XID)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seconds</td>
<td>Flags</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client IP Address (CIADDR)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Your IP Address (YIADDR)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server IP Address (SIADDR)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway IP Address (GIADDR)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Client Hardware Address (CHADDR)—16 bytes</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Name (SNAME)—64 bytes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Filename—128 bytes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP Options</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DHCP Request/Reply Types

<table>
<thead>
<tr>
<th>Message</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPDISCOVER</td>
<td>Client broadcast to locate available servers.</td>
</tr>
<tr>
<td>DHCPOFFER</td>
<td>Server to client in response to DHCPDISCOVER with offer of configuration parameters.</td>
</tr>
<tr>
<td>DHCPREQUEST</td>
<td>Client message to servers either (a) requesting offered parameters from one server and implicitly declining offers from all others, (b) confirming correctness of previously allocated address after, e.g., system reboot, or (c) extending the lease on a particular network address.</td>
</tr>
<tr>
<td>DHCPACK</td>
<td>Server to client with configuration parameters, including committed network address.</td>
</tr>
<tr>
<td>DHCPNAK</td>
<td>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</td>
</tr>
<tr>
<td>DHCPDECLINE</td>
<td>Client to server indicating network address is already in use.</td>
</tr>
<tr>
<td>DHCPRELEASE</td>
<td>Client to server relinquishing network address and canceling remaining lease.</td>
</tr>
<tr>
<td>DHCPINFORM</td>
<td>Client to server, asking only for local configuration parameters; client already has externally configured network address.</td>
</tr>
</tbody>
</table>
### DHCP Attack Types

#### DHCP Starvation Attack

- **Client**
- **Gobbler**
- **DHCP Server**

- **DHCP Discovery (Broadcast) x (Size of Scope)**
- **DHCP Offer (Unicast) x (Size of DHCPScope)**
- **DHCP Request (Broadcast) x (Size of Scope)**
- **DHCP Ack (Unicast) x (Size of Scope)**

- **Gobbler** looks at the entire DHCP scope and tries to lease all of the DHCP addresses available in the DHCP scope.
- **This is a Denial of Service DoS attack using DHCP leases**

### Countermeasures for DHCP Attacks

#### DHCP Starvation Attack = Port Security

- **Client**
- **Gobbler**
- **DHCP Server**

- **CatOS**
  - set port security 5/1 enable
  - set port security 5/1 port max 1
  - set port security 5/1 violation restrict
  - set port security 5/1 age 2
  - set port security 5/1 timer-type inactivity

- **IOS**
  - switchport port-security
  - switchport port-security maximum 1
  - switchport port-security violation restrict
  - switchport port-security aging time 2
  - switchport port-security aging type inactivity
DHCP Attack Types
Rogue DHCP Server Attack

- What can the attacker do if he is the DHCP server?

  IP Address: 10.10.10.101
  Subnet Mask: 255.255.255.0
  Default Routers: 10.10.10.1
  DNS Servers: 192.168.10.4, 192.168.10.5
  Lease Time: 10 days

  Here is Your Configuration

- What do you see as a potential problem with incorrect information?
  Wrong Default Gateway—Attacker is the gateway
  Wrong DNS Server—Attacker is DNS server
  Wrong IP Address—Attacker does DOS with incorrect IP
Countermeasures for DHCP Attacks
Rogue DHCP Server = DHCP Snooping

- Rogue DHCP Server = DHCP Snooping
  - By default all ports in the vlan are untrusted
  - Table is build by “Snooping” the DHCP reply to the client
  - Entries stay in table until DHCP lease time expires

DHCP Snooping Enabled

Shut Down the Rogue DHCP Server

DHCP Snooping Untrusted Client

DHCP Snooping Trusted Server

DHCP Snooping Binding Table

IOs Global Commands
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping

IOS Interface Commands
no ip dhcp snooping trust (Default)
ip dhcp snooping limit rate 10 (pps)

- By default all ports in the vlan are untrusted

Countermeasures for DHCP Attacks
Rogue DHCP Server = DHCP Snooping

DHCP Snooping Enabled

DHCP Snooping Untrusted Client

DHCP Snooping Trusted Server or uplink

DHCP Snooping Binding Table

sh ip dhcp snooping binding
MacAddress    IpAddress    Lease(sec)  Type   VLAN  Interface
00:03:47:85:9F:AD  10.120.4.10  193185    dhcp-snooping  4     FastEthernet3/18

OK DHCP Responses: offer, ack, nak
BAD DHCP Responses: offer, ack, nak
Advanced Configuration DHCP Snooping

- Not all operating system (Linux) re DHCP on link down
- In the event of switch failure, the DHCP Snooping Binding Table can be written to bootflash, ftp, rcp, slot0, and tftp
- This will be critical in the next section

```
ip dhcp snooping database write-delay 60
```

Advanced Configuration DHCP Snooping

- Gobbler uses a unique mac for each DHCP request and Port Security prevents Gobbler
- What if the attack used the same interface MAC address, but changed the Client Hardware Address in the request?
- Port security would not work for that attack
- The switches now check the CHADDR field of the request to make sure it matches the hardware MAC in the DHCP Snooping Binding Table
- If there is not a match, the request is dropped at the interface

<table>
<thead>
<tr>
<th>OP Code</th>
<th>Hardware Type</th>
<th>Hardware Length</th>
<th>HOPS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Some Switches Have This on by Default, and Others Don’t Please Check the Documentation for Settings
DHCP Rogue Server

• If there are switches in the network that will not support DHCP Snooping, you can configure VLAN ACL’s to block UDP Port 68

set security acl ip ROGUE-DHCP permit udp host 192.0.2.1 any eq 68
set security acl ip ROGUE-DHCP deny udp any any eq 68
set security acl ip ROGUE-DHCP permit ip any any
set security acl ip ROGUE-DHCP permit udp host 10.1.1.99 any eq 68

• Will not prevent the CHADDR DHCP Starvation attack

Summary of DHCP Attacks

• DHCP starvation attacks can be mitigated by port security
• Rogue DHCP servers can be mitigated by DHCP Snooping features
• When configured with DHCP Snooping, all ports in the vlan will be “Untrusted” for DHCP replies
• Check default settings to see if the CHADDR field is being checked during the DHCP request
• Unsupported switches can run ACL’s for partial attack mitigation (can not check the CHADDR field)
Building the Onion

- Port security prevents CAM attacks
- DHCP Snooping prevents Rogue DHCP server attacks
ARP Function Review

• Before a station can talk to another station it must do an ARP request to map the IP address to the MAC address
  This ARP request is broadcast using protocol 0806

• All computers on the subnet will receive and process the ARP request; the station that matches the IP address in the request will send an ARP reply

• According to the ARP RFC, a client is allowed to send an unsolicited ARP reply; this is called a gratuitous ARP; other hosts on the same subnet can store this information in their ARP tables

• Anyone can claim to be the owner of any IP/MAC address they like

• ARP attacks use this to redirect traffic
ARP Attack Tools

- Two major tools on the Net for ARP man-in-the-middle attacks
  - dsniff—http://monkey.org/~dugsong/dsniff/
    Both “tools” function similar to each other
- ettercap is the second generation of ARP attack tools
  - ettercap has a nice GUI, and is almost point and click
  - Interesting features of ettercap
    - Packet insertion, many to many ARP attack
- Both capture the traffic/passwords of applications (over 30)
  - FTP, Telnet, SMTP, HTTP, POP, NNTP, IMAP, SNMP, LDAP, RIP, OSPF, PPTP, MS-CHAP, SOCKS, X11, IRC, ICQ, AIM, SMB, Microsoft SQL, `
ARP Attack Tools: SSH/SSL

- Using these tools SSL/SSH sessions can be intercepted and bogus certificate credentials can be presented
- Once you have excepted the certificate, all SSL/SSH traffic for all SSL/SSH sites can flow through the attacker

ARP Attack in Action

- Attacker “poisons” the ARP tables
ARP Attack in Action

- All traffic flows through the attacker

Transmit/Receive Traffic to 10.1.1.2 MAC C

ARP Attack Clean Up

- Attacker corrects ARP tables entries
- Traffic flows return to normal

ARP 10.1.1.1 Saying 10.1.1.2 is MAC B

ARP 10.1.1.2 Saying 10.1.1.1 is MAC A
Countermeasures to ARP Attacks: Dynamic ARP Inspection

- Uses the information from the DHCP Snooping Binding table

```
sh ip dhcp snooping binding

MacAddress   IPAddress           Lease(sec)  Type             VLAN  Interface
------------- ------------------------ ---------- ------------------ ---- ----------------------
00:03:47:85:9F:AD   10.120.4.10      193185     dhcp-snooping      4     FastEthernet3/18
00:03:47:4C:6f:83  10.120.4.11      213454     dhcp-snooping      4     FastEthernet3/21
```

- Looks at the MacAddress and IpAddress fields to see if the ARP from the Interface is in the binding, if not, traffic is blocked
Countermeasures to ARP Attacks: Dynamic ARP Inspection

Configuration of Dynamic ARP Inspection (DAI)

- DHCP snooping had to be configured so the binding table it built
- DAI is configured by VLAN
- You can trust an interface like DHCP snooping
- Be careful with rate limiting—Varies between platforms
- Suggested for voice is to set the rate limit above the default

Dynamic ARP Inspection Commands

**IOS**

Global Commands
- ip dhcp snooping vlan 4,104
- no ip dhcp snooping information option
- ip dhcp snooping
- ip arp inspection vlan 4,104
- ip arp inspection log-buffer entries 1024
- ip arp inspection log-buffer logs 1024 interval 10

Interface Commands
- ip dhcp snooping trust
- ip arp inspection trust

**IOS**

Interface Commands
- no ip arp inspection trust (default)
- ip arp inspection limit rate 15 (pps)
Countermeasures to ARP Attacks: Dynamic ARP Inspection

Error Messages in Show Log

```
sh log:
4w6d: %SW_DAI-4-PACKET_RATE_EXCEEDED: 16 packets received in 296 milliseconds on Gi3/2.
4w6d: %PM-4-ERR_DISABLE: arp-inspection error detected on Gi3/2, putting Gi3/2 in err-disable state
4w6d: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi3/2, vlan 183.([0003.472d.8b0f/10.10.10.62/0000.0000.0000/10.10.10.2/12:19:27 UTC Wed Apr 19 2000])
4w6d: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi3/2, vlan 183.([0003.472d.8b0f/10.10.10.62/0000.0000.0000/10.10.10.3/12:19:27 UTC Wed Apr 19 2000])
```

Summary of ARP Attacks

- Dynamic ARP inspection prevents ARP Attacks by intercepting all ARP requests and responses
- DHCP snooping must be configured first, otherwise there is no binding table for dynamic ARP inspection to use
- The DHCP snooping table it built from the DHCP request, but you can put in static entries
  - If you have a device that does not DHCP, but you would like to turn on dynamic ARP inspection, you would need a static entry in the table
More ARP Attack Information

- Some IDS systems will watch for an unusually high amount of ARP traffic
- ARPWatch is a freely available tool that will track IP/MAC address pairings
  - Caution—you will need an ARPWatch server on every VLAN
  - Hard to manage and scale
  - You can still do static ARP for critical routers and hosts (administrative pain)

Building the Onion

- Port security prevents CAM attacks
- DHCP Snooping prevents Rouge DHCP server attacks
- Dynamic ARP Inspection prevents current ARP Attacks
Spoofing Attacks

- **MAC Spoofing**
  
  If MAC’s are used for network access an attacker can gain access to the network.
  
  Also can be used to take over someone’s identity already on the network.

- **IP Spoofing**
  
  Ping of death
  
  ICMP unreachable storm
  
  SYN flood
Spoofing Attack: MAC

- Attacker sends packets with the incorrect source MAC address
- If network control is by MAC Address, the attacker now looks like 10.1.1.2

Spoofing Attack: IP

- Attacker sends packets with the incorrect source IP Address
- Whatever device the packet is sent to will never reply to the attacker
Spoofing Attack: IP/MAC

- Attacker sends packets with the incorrect source IP and MAC address
- Now looks like a device that is already on the network

Traffic Sent with IP 10.1.1.2 MAC B Source

Received Traffic Source IP 10.1.1.2 MAC A

Traffic Sent with IP 10.1.1.3 MAC C

10.1.1.1 MAC A

10.1.1.2 MAC B

10.1.1.3 MAC C

Received Traffic Source IP 10.1.1.2 MAC B

Countermeasures to Snooping Attacks: IP Source Guard

- Uses the DHCP Snooping Binding Table Information
- IP Source Guard
  - Operates just like Dynamic ARP Inspection, but looks at every packet, not just ARP Packet

Traffic Sent with IP 10.1.1.3 MAC B

Non Matching Traffic Dropped

DHCP Snooping Enabled
Dynamic ARP inspection Enabled
IP Source Guard Enabled

Traffic Sent with IP 10.1.1.2 MAC B

Traffic Sent with IP 10.1.1.2 MAC C

10.1.1.2 MAC B
Countermeasures to Snooping Attacks: IP Source Guard

- Uses the information from the DHCP snooping binding table

```
sh ip dhcp snooping binding
+-------------------+-----------------+-----------------+---------------+--------+---------------------+
<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>00:03:47:85:9F:AD</td>
<td>10.120.4.10</td>
<td>193185</td>
<td>dhcp-snooping</td>
<td>4</td>
<td>FastEthernet3/18</td>
</tr>
<tr>
<td>00:03:47:04:6f:83</td>
<td>10.120.4.11</td>
<td>213494</td>
<td>dhcp-snooping</td>
<td>4</td>
<td>FastEthernet3/21</td>
</tr>
</tbody>
</table>
```

- Looks at the MacAddress and IpAddress fields to see if the traffic from the Interface is in the binding, it not, traffic is blocked

Configuration of IP Source Guard

- DHCP Snooping had to be configured so the binding table it built
- IP Source Guard is configured by port
- IP Source Guard with MAC does not learn the MAC from the device connected to the switch, it learns it from the DHCP Offer
- MAC and IP checking can be turned on Separately or together
  - For IP—
    - Will work with the information in the binding table
  - For mac—
    - Must have an Option 82 enabled DHCP server
      - (Microsoft does not support option 82)
    - Have to Change all router configuration to support Option 82
    - All Layer 3 devices between the DHCP request and the DHCP server will need to be configured to trust the Option 82 DHCP Request—ip dhcp relay information trust

Note: There Are at Least 2 DHCP Servers That Support Option 82 Field
Cisco Network Registrar and Avaya
Countermeasures to Snooping Attacks: IP Source Guard

IP Source Guard

<table>
<thead>
<tr>
<th>IP Source Guard Configuration</th>
<th>IP Source Guard Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP/MAC Checking Only (Opt 82)</td>
<td>IP Checking Only (no Opt 82)</td>
</tr>
</tbody>
</table>

**IOS**

**Global Commands**

- ip dhcp snooping vlan 4,104
- ip dhcp snooping information option
- ip dhcp snooping

**Interface Commands**

- ip verify source vlan dhcp-snooping
- port-security

**Building the Onion**

- Port security prevents CAM attacks
- DHCP snooping prevents rogue DHCP server attacks
- Dynamic ARP inspection prevents current ARP attacks
- IP source guard prevents IP/MAC spoofing
Spanning Tree Basics

- STP Purpose: To maintain loop-free topologies in a redundant Layer 2 infrastructure

  A ‘Tree-Like’ Loop-Free Topology Is Established from the perspective of the root bridge

  A Switch Is Elected as Root
  Root selection is based on the lowest configured priority of any switch 0–65535

- STP is very simple; messages are sent using Bridge Protocol Data Units (BPDUs); basic messages include: configuration, topology change notification/acknowledgment (TCN/TCA); most have no “payload”

- Avoiding loops ensures broadcast traffic does not become storms
Spanning Tree Attack Example

- Send BPDU messages to become root bridge

The attacker then sees frames he shouldn't

MITM, DoS, etc. all possible

Any attack is very sensitive to the original topology, trunking, PVST, etc.

Although STP takes link speed into consideration, it is always done from the perspective of the root bridge. Taking a Gb backbone to half-duplex 10 Mb was verified

Requires attacker is dual homed to two different switches (with a hub, it can be done with just one interface on the attacking host)
STP Attack Mitigation

- Try to design loop-free topologies wherever possible, so you do not need STP
- Don’t disable STP, introducing a loop would become another attack
- BPDU Guard
  - Should be run on all user-facing ports and infrastructure-facing ports
    - Disables ports using portfast upon detection of a BPDU message on the port
    - Globally enabled on all ports running portfast
    - Available in Catalyst OS 5.4.1 for Cat 2K, 4K, 5K, and 6K; 12.0XE for native Cisco IOS 6K; 12.1(8a)EW for 4K IOS; 12.1(4)E for 3550; 12.1(6)E2 for 2950

  ```
  CatOS> (enable) set spantree portfast bpdu-guard enable
  IOS(config)#spanning-tree portfast bpduguard
  ```

- Root Guard
  - Disables ports who would become the root bridge due to their BPDU advertisement
  - Configured on a per-port basis
  - Available in Catalyst OS 6.1.1 for Catalyst 29XX, 4K, 5K, and 6K; 12.0(7) <X> for native Cisco IOS 6K, 12.1(8a)EW for 4K Cisco IOS; 29/3500XL in 12.0(5) <X>; 3550 in 12.1(4)E; 2950 in 12.1(6)E2

  ```
  CatOS> (enable) set spantree guard root 1/1
  IOS(config)#spanning-tree guard root (or rootguard)
  ```

Cisco Discovery Protocol (CDP)

- NOT normally an attack
- Runs at Layer 2 and allows Cisco devices to chat with one another
- Can be used to learn sensitive information about the CDP sender (IP address, software version, router model …)
- CDP is in the clear and unauthenticated
- Consider disabling CDP, or being very selective in its use in security-sensitive environments
- Used by Cisco IPT for Network Management
- Note: there was a reason Cisco developed CDP, some Cisco apps make use of it!

  ```
  CatOS> (enable) set cdp disable <mod>/<port> | all
  IOS(config)#no cdp run
  IOS(config-if)#no cdp enable
  ```
CDP Attacks

- Besides the information gathering benefit CDP offers an attacker, there was a vulnerability in CDP that allowed Cisco devices to run out of memory and potentially crash if you sent it tons of bogus CDP packets.
- If you need to run CDP, be sure to use Cisco IOS code with minimum version numbers: 12.2(3.6)B, 12.2(4.1)S, 12.2(3.6)PB, 12.2(3.6)T, 12.1(10.1), 12.2(3.6) or CatOS code 6.3, 5.5, or 7.1 and later.
- Problem was due to improper memory allocation for the CDP process (basically there was no upper limit).
- For more information:
  - [http://www.kb.cert.org/vuls/id/139491](http://www.kb.cert.org/vuls/id/139491)

Switch Management

- Management can be your weakest link.
  - All the great mitigation techniques we talked about aren’t worth much if the attacker telnets into your switch and disables them.
- Most of the network management protocols we know and love are insecure (syslog, SNMP, TFTP, Telnet, FTP, etc.).
- Consider secure variants of these protocols as they become available (SSH, SCP, SSL, OTP etc.), where impossible, consider out of band (OOB) management.
  - Put the management VLAN into a dedicated non-standard VLAN where nothing but management traffic resides.
  - Consider physically back-hauling this interface to your management network.
- When OOB management is not possible, at least limit access to the management protocols using the “set ip permit” lists on the management protocols.
- SSH is available on Catalyst 6K with Catalyst OS 6.1 and Catalyst 4K/29XXG with Catalyst OS 6.3; 3550 in 12.1(11)EA1; 2950 in 12.1(12c)EA1; Cisco IOS 6K 12.1(5c)E12; IOS 4K in 12.1(13)EW.
Countermeasures for DHCP Attacks
Rogue DHCP Server = DHCP Snooping

- Table is build by “Snooping” the DHCP reply to the client
- Entries stay in table until DHCP lease time expires
Countermeasures to ARP Attacks: Dynamic ARP Inspection

- Uses the DHCP Snooping Binding Table Information
- Dynamic ARP Inspection
  All ARP packets must match the IP/MAC Binding table entries
  If the entries do not match, throw them in the bit bucket

DHCP Snooping Enabled
Dynamic ARP inspection Enabled

Countermeasures to Snooping Attacks: IP Source Guard

- Uses the DHCP Snooping Binding Table Information
- IP Source Guard
  Operates just like Dynamic ARP inspection, but looks at every packet, not just ARP Packet

DHCP Snooping Enabled
Dynamic ARP inspection Enabled
IP Source Guard Enabled
### Matrix for Security Features 1 of 2

<table>
<thead>
<tr>
<th>Feature/Platform</th>
<th>6500/ Catalyst OS</th>
<th>6500/Cisco IOS</th>
<th>4500/ Catalyst OS</th>
<th>4500/Cisco IOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Port Security</td>
<td>Now 7.6(1)</td>
<td>Now 12.1(13)E</td>
<td>Now 5.1(1)</td>
<td>Now 12.1(13)EW</td>
</tr>
<tr>
<td>DHCP Snooping</td>
<td>8.3(1)</td>
<td>Q1CY '05 12.2(18)SXD2</td>
<td>N/A</td>
<td>Now** 12.1(12c)EW</td>
</tr>
<tr>
<td>DAI</td>
<td>8.3(1)</td>
<td>Q1CY '05 12.2(18)SXD2</td>
<td>N/A</td>
<td>Now ** 12.1(19)EW</td>
</tr>
<tr>
<td>IP Source Guard</td>
<td>8.3(1)*</td>
<td>Q1CY '05* 12.2(18)SXD2</td>
<td>N/A</td>
<td>Now ** 12.1(19)EW</td>
</tr>
</tbody>
</table>

* Requires Sup720
** For the Catalyst 4500/IOS-based platforms, this requires Sup2+, Sup3, Sup4, Sup 5. These Sups are supported on the Catalyst 4006, 4503, 4506, and 4507R chassis.

NOTE: There are no plans to support these features for any Catalyst 4000/4500 platform running CatOS, or any 2900 platform.

### Matrix for Security Features 2 of 2

<table>
<thead>
<tr>
<th>Feature/Platform</th>
<th>3750 EMI/SMI</th>
<th>3550 EMI/SMI</th>
<th>2970 EI</th>
<th>2950 EI</th>
<th>2950 SI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Port Security</td>
<td>Now 12.1(11)AX</td>
<td>Now 12.1(4)EA1</td>
<td>Now 12.1(11)AX</td>
<td>Now 12.0(5.2)WC1</td>
<td>Now 12.0(5.2)WC1</td>
</tr>
<tr>
<td>DHCP Snooping</td>
<td>Now 12.1(19)EA1</td>
<td>Now 12.1(19)EA1</td>
<td>Now 12.1(19)EA1</td>
<td>Now 12.1(19)EA1</td>
<td>N/A</td>
</tr>
<tr>
<td>DAI</td>
<td>Now 12.2(20)SE</td>
<td>Q3CY '04 *** 12.2(XX)SE</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>IP Source Guard</td>
<td>Now 12.2(20)SE</td>
<td>Q3CY '04 *** 12.2(XX)SE</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

*** Current target. Also, 3750/3550 will support DAI and Source Guard on EMI image only.
**** 3550 EMI only

NOTE: There are no plans to support these features for any Catalyst 4000/4500 platform running CatOS, or any 2900 platform.
Layer 2 Security Best Practices 1 of 2

- Manage switches in as secure a manner as possible (SSH, OOB, permit lists, etc.)
- Always use a dedicated VLAN ID for all trunk ports
- Be paranoid: do not use VLAN 1 for anything
- Set all user ports to non trunking (unless you are Cisco VoIP)
- Deploy port-security where possible for user ports
- Selectively use SNMP and treat community strings like root passwords
- Have a plan for the ARP security issues in your network (ARP Inspection, IDS, etc.)

Layer 2 Security Best Practices 2 of 2

- Enable STP attack mitigation (BPDU Guard, Root Guard)
- Decide what to do about DHCP attacks (DHCP Snooping, VACLs)
- Use MD5 authentication for VTP
- Use CDP only where necessary
- Disable all unused ports and put them in an unused VLAN

All of the Preceding Features Are Dependent on Your Own Security Policy
Lessons Learned

• Carefully consider any time you must count on VLANs to operate in a security role
  If properly configured, our testing did not discover a method of VLAN Hopping using Cisco switches
  Pay close attention to the configuration
  Understand the organizational implications

• Evaluate your security policy while considering the other issues raised in this session
  Is there room for improvement?
  What campus risks are acceptable based on your policy?

• Deploy, where appropriate, L2 security best practices
Complete Your Online Session Evaluation!

**WHAT:** Complete an online session evaluation and your name will be entered into a daily drawing

**WHY:** Win fabulous prizes! Give us your feedback!

**WHERE:** Go to the Internet stations located throughout the Convention Center

**HOW:** Winners will be posted on the onsite Networkers Website; four winners per day