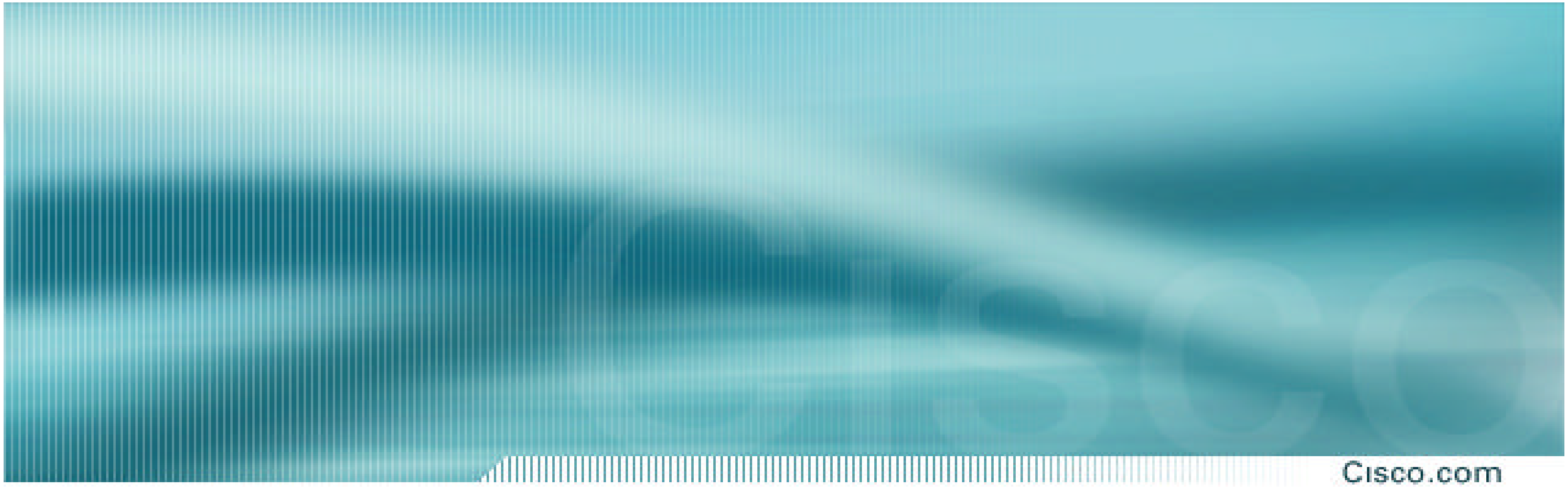


Metro Ethernet Security

© 2002, Cisco Systems, Inc. All rights reserved.

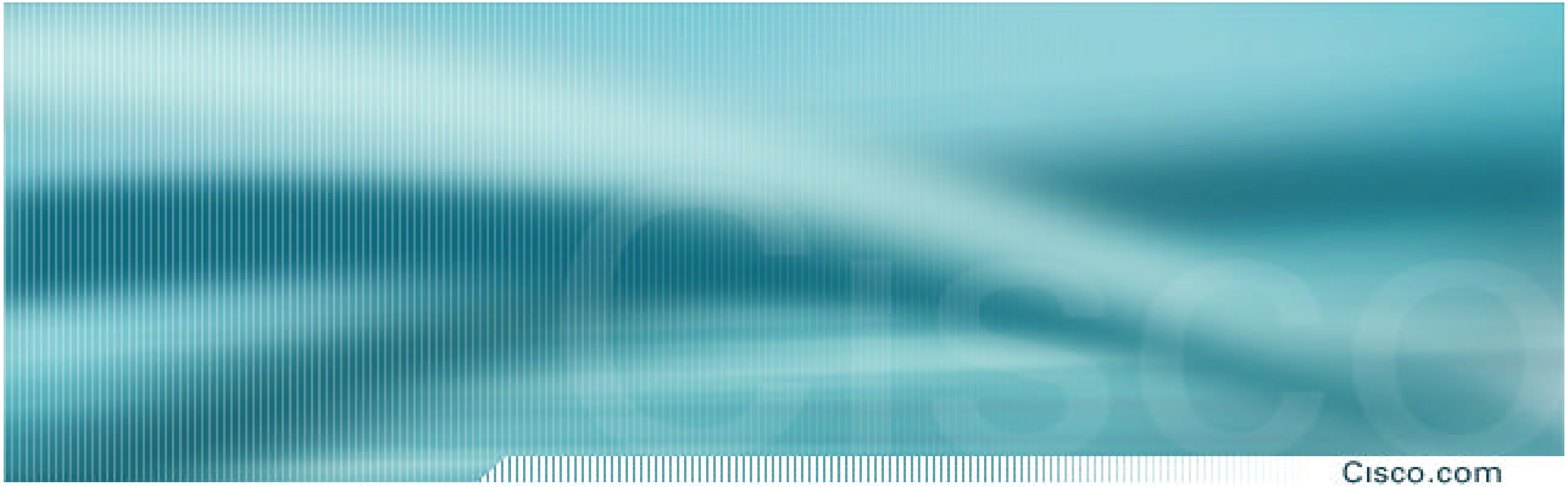
Agenda

- **Feature Overview**
- Box security

  SNMP, pwd recovery, telnet/consol
- Networking protocols

  IGP, EGP, HSRP, VRRP, Spanning-tree, cdp, ip spoofing
- User protection

  Security between users



Feature overview

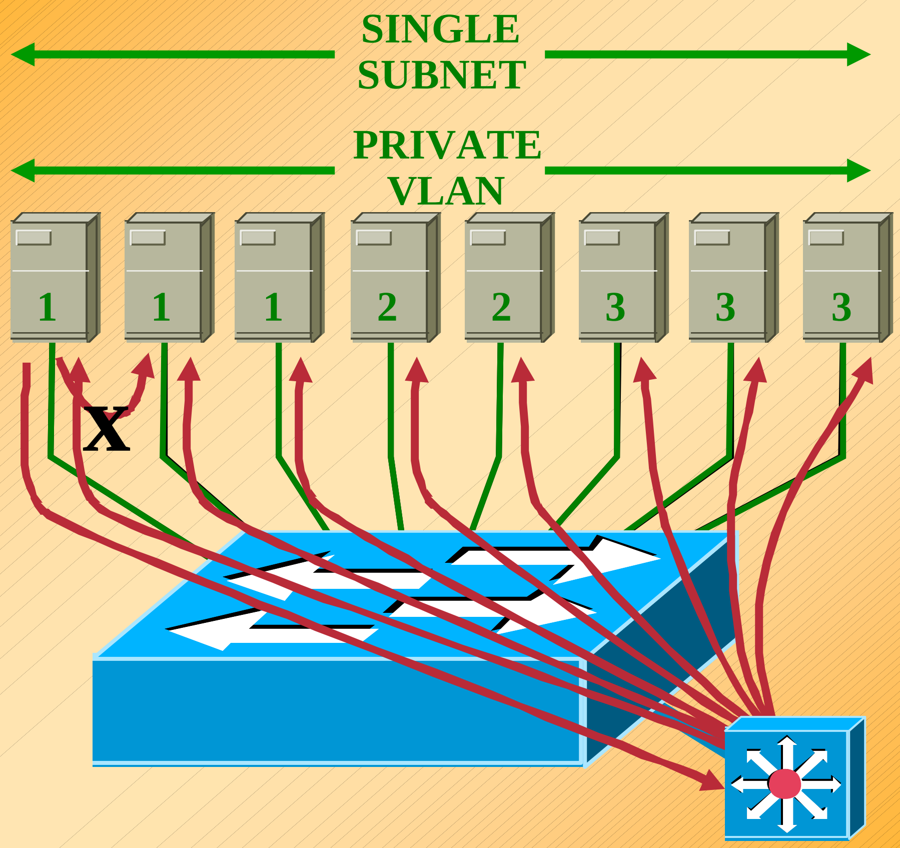
Private vlan

Private vlan

- To get more efficiency when creating the ip-subnets, there is a need to have large vlans (especially if using real ip addresses)
- From a security perspective, it would be best if every user belongs to his own subnet

Private vlan

Access
Layer 2



© 2003, Cisco Systems, Inc. All rights r

Private vlan, limitations

- For security reasons, private VLAN interface learned ARP entries do not age out.
- This is a problem in a DHCP environment

  If a customer shuts down his pc it is not possible to assign “his old” ip address to a new customer.

  This is however possible to turn off from 12.1.11E

```
MSFC:
dr1.row2.lab(config)# int vlan 310
dr1.row2.lab(config-if)# Description public part of pvlan
dr1.row2.lab(config-if)# no ip pvlan-sticky-arp
```

http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/1687_pp.htm

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

Feature overview

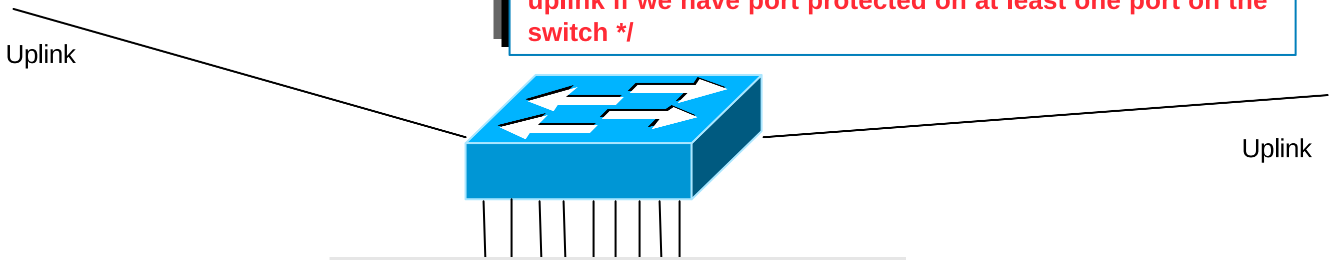
Private vlan edge

© 2002, Cisco Systems, Inc. All rights reserved.

Private vlan edge

- A one box only version of the pvlan feature
- Modes are uplink or user-ports, can’t span over several devices

```
interface GigabitEthernet0/1
 description ******uplink ******
/* no pvlan edge config needed, all ports that doesn’t have
port protected configured will automatically be seen as
uplink if we have port protected on at least one port on the
switch */
```



```
interface FastEthernet0/2
 description ****** clientport ******
 port protected
```

Pvlan / edge, neighbour communication?

- **This is an ISP service, we can’t live with a limitation where two customers connected to the same switch can’t talk to each other!**
- **Local proxy arp**

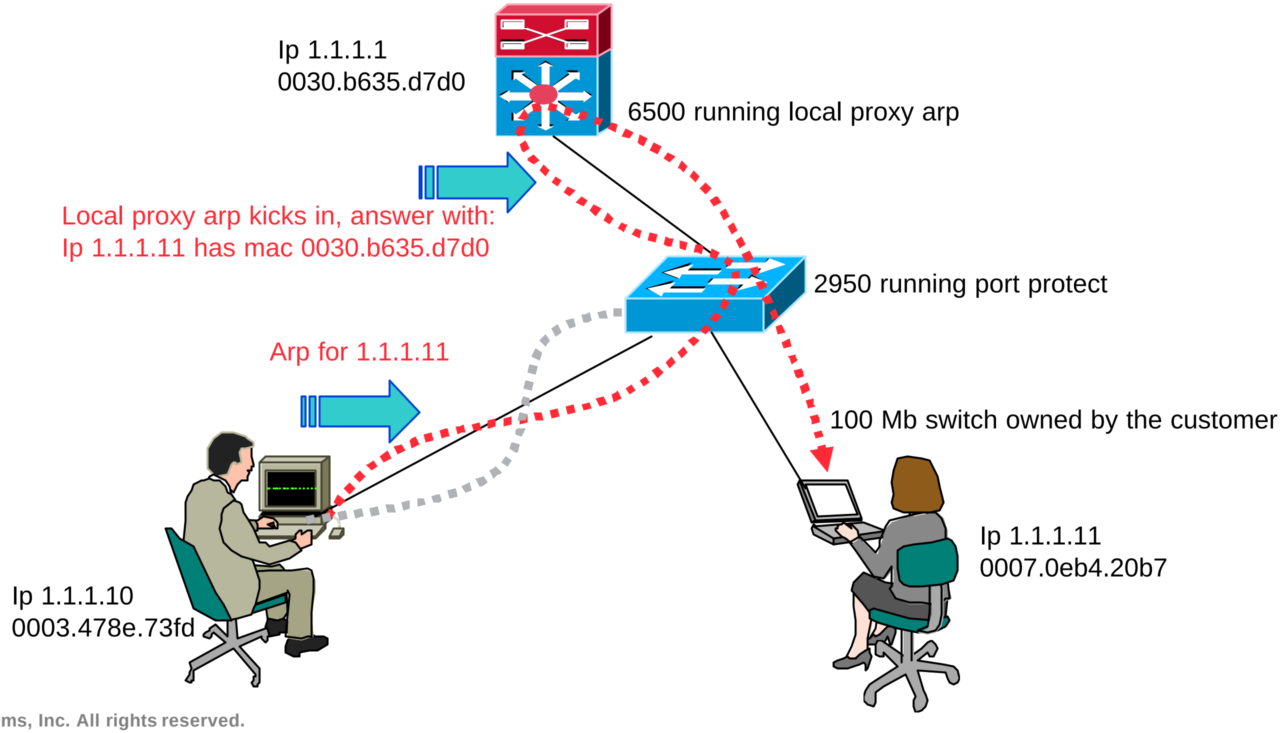
  Answer on behalf of someone else

```
MSFC:
dr1.ank1.se(config)# interface  vlan 30
dr1.ank1.se(config-if)#  ip local-proxy-arp
```

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

Pvlan / edge, neighbour cont 1

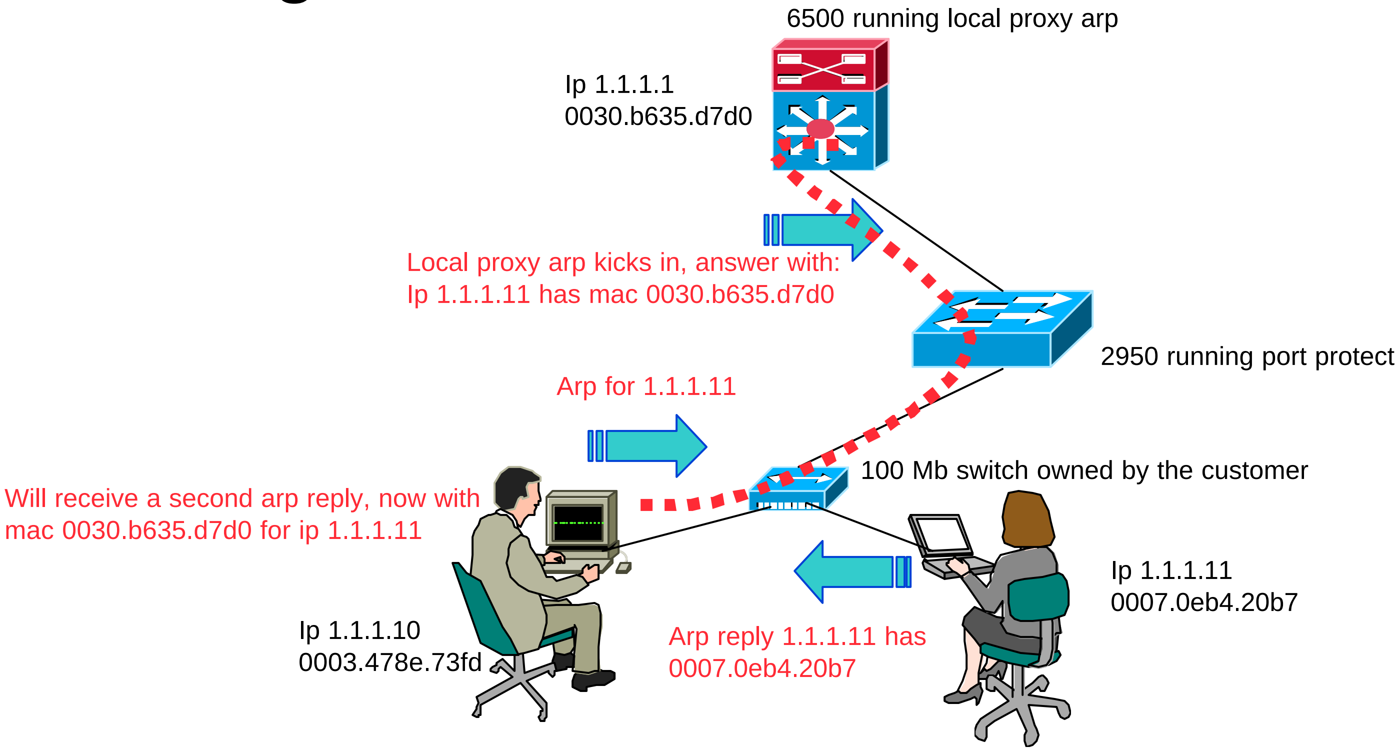
- For local data traffic, between users on the same switch, all data will go via the router


Ip 1.1.1.1
0030.b635.d7d0
6500 running local proxy arp
Local proxy arp kicks in, answer with:
Ip 1.1.1.11 has mac 0030.b635.d7d0
2950 running port protect
Arp for 1.1.1.11
100 Mb switch owned by the customer
Ip 1.1.1.11
0007.0eb4.20b7
Ip 1.1.1.10
0003.478e.73fd

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

Pvlan / edge, neighbour cont 2

- There is a drawback with this approach
- Same user have two pcs connected to a hub, doing file-transfers between them


6500 running local proxy arp
Ip 1.1.1.1
0030.b635.d7d0
Local proxy arp kicks in, answer with:
Ip 1.1.1.11 has mac 0030.b635.d7d0
2950 running port protect
Arp for 1.1.1.11
100 Mb switch owned by the customer
Will receive a second arp reply, now with
mac 0030.b635.d7d0 for ip 1.1.1.11
Ip 1.1.1.11
0007.0eb4.20b7
Ip 1.1.1.10
0003.478e.73fd
Arp reply 1.1.1.11 has
0007.0eb4.20b7

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

Private vlan, why bother?

- Why bother with private vlan / edge if we anyway plan to allow traffic using local proxy arp???
- We have a possibility on switches to filter on L3 even within the same vlan, VACL [vlan access list], even on PVLAN* configurations

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

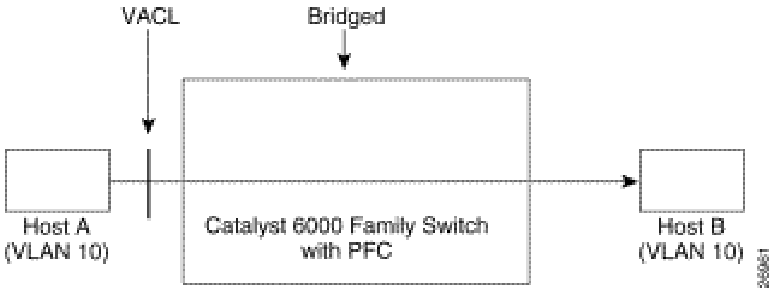
Feature overview

VACL [Vlan ACcess List]

© 2002, Cisco Systems, Inc. All rights reserved.

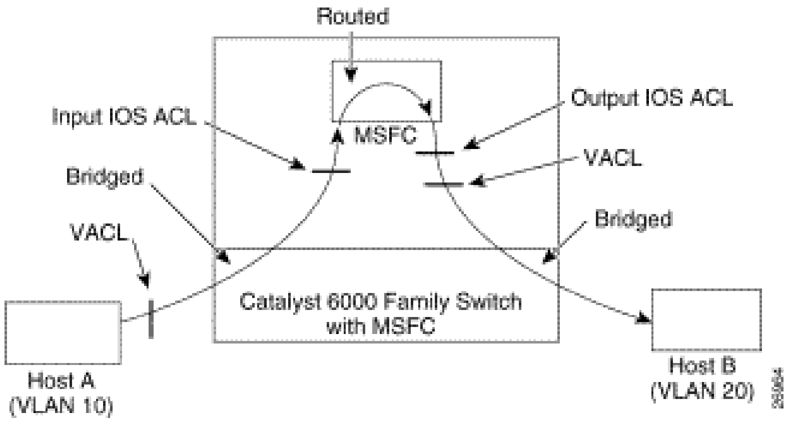
VACL, function 1

Within the same vlan



VACL, function 2

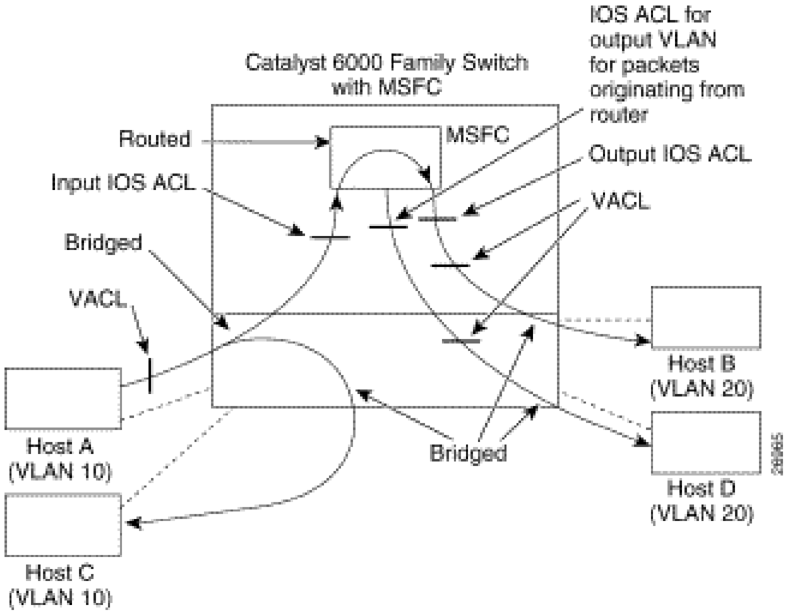
Between different vlans



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

VACL, function 3

All together



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

VACL, what to filter

- We are providing a broadband isp, IP service

  Other protocols should be filtered out

- NetBIOS is a security threat, shared disks can be mapped, vulnerabilities can be used

- If customers would like to do gaming over the network, they should be forced to use IP, no IPX

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

Agenda

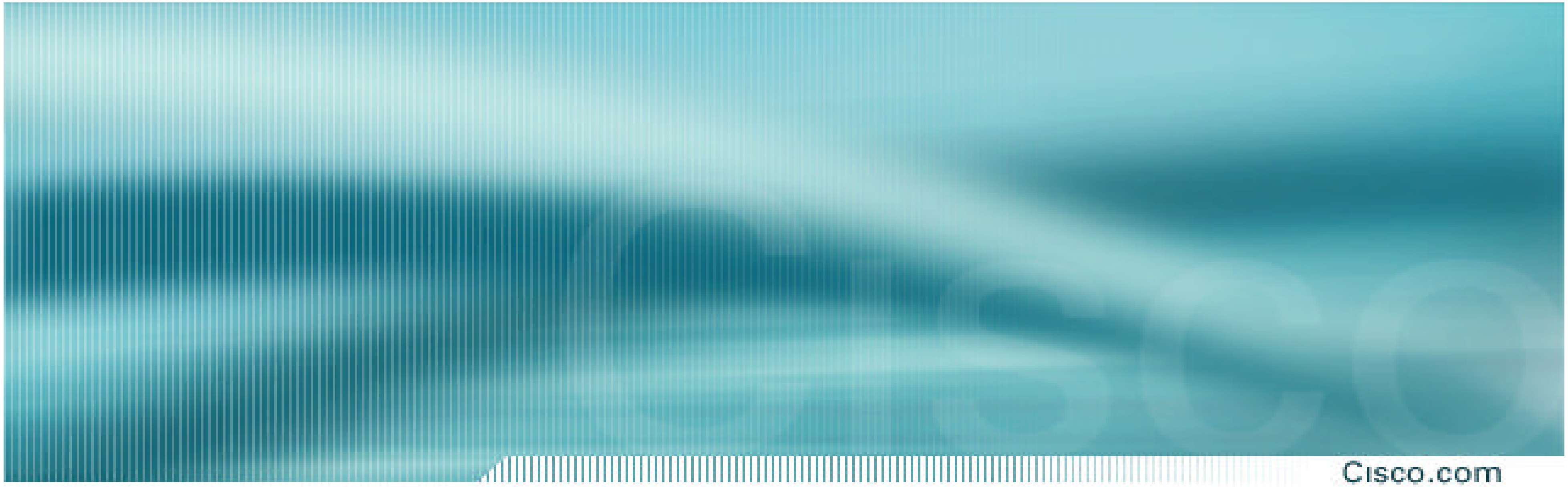
- Feature Overview
- Box security

  SNMP, pwd recovery, telnet/consol
- Networking protocols

  IGP, EGP, HSRP, VRRP, Spanning-tree, cdp, ip spoofing
- User protection

  Security between users

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



Box security

Environmental security

© 2002, Cisco Systems, Inc. All rights reserved.

Environmental security

- We have seen occurrences of physical “break in” to get access to the console of the access device
- This is something we should keep in mind when it comes to SNMP communities, access-lists, enable secret and logging of configuration changes

```
No Service password-recovery
```

Box security

Mac address flooding

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

0000.0cXX.XXXX

Second 24 Bits = Specific Interface, Assigned by Manufacturer

XXXX.XX00.0001

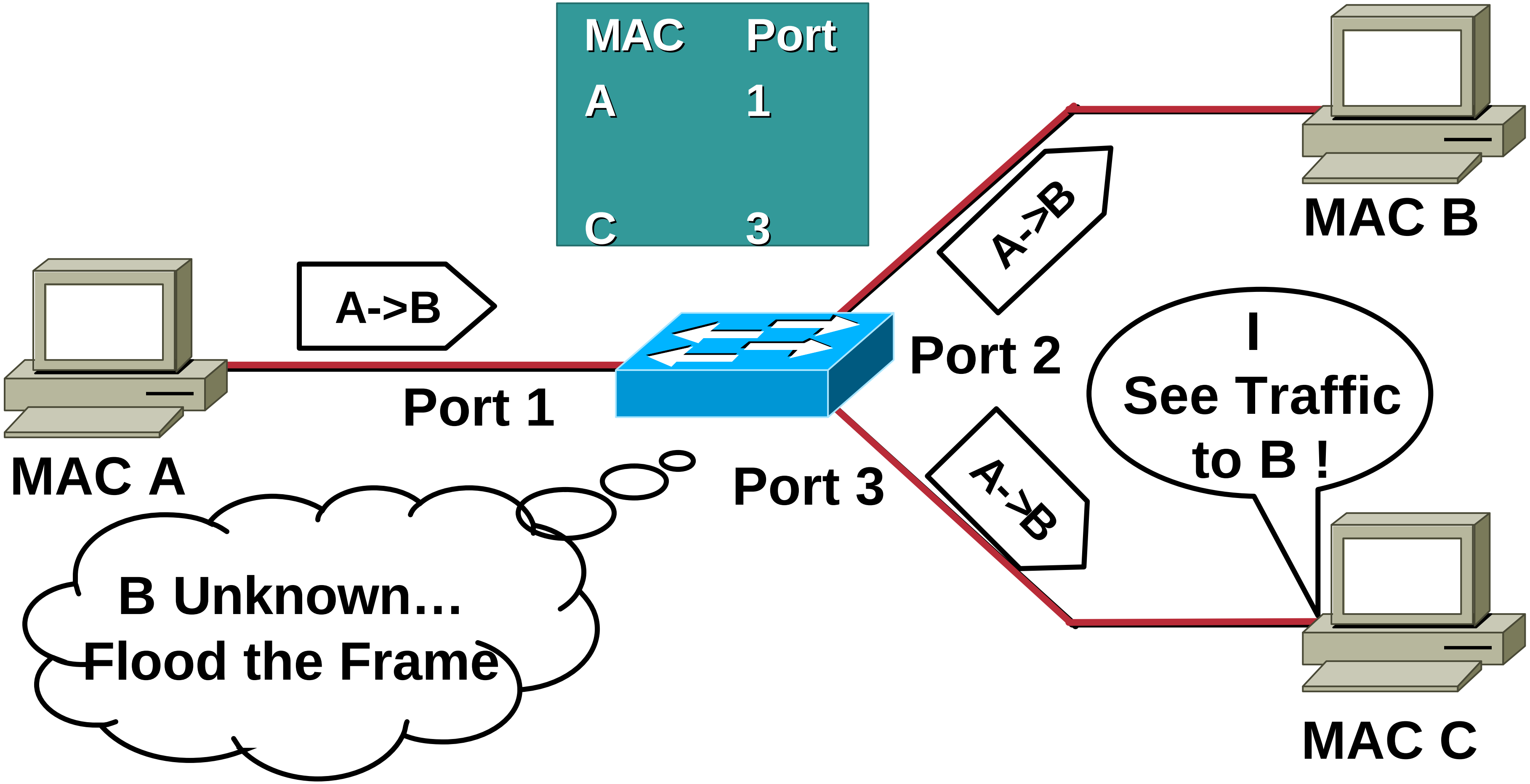
All F's = Broadcast

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**

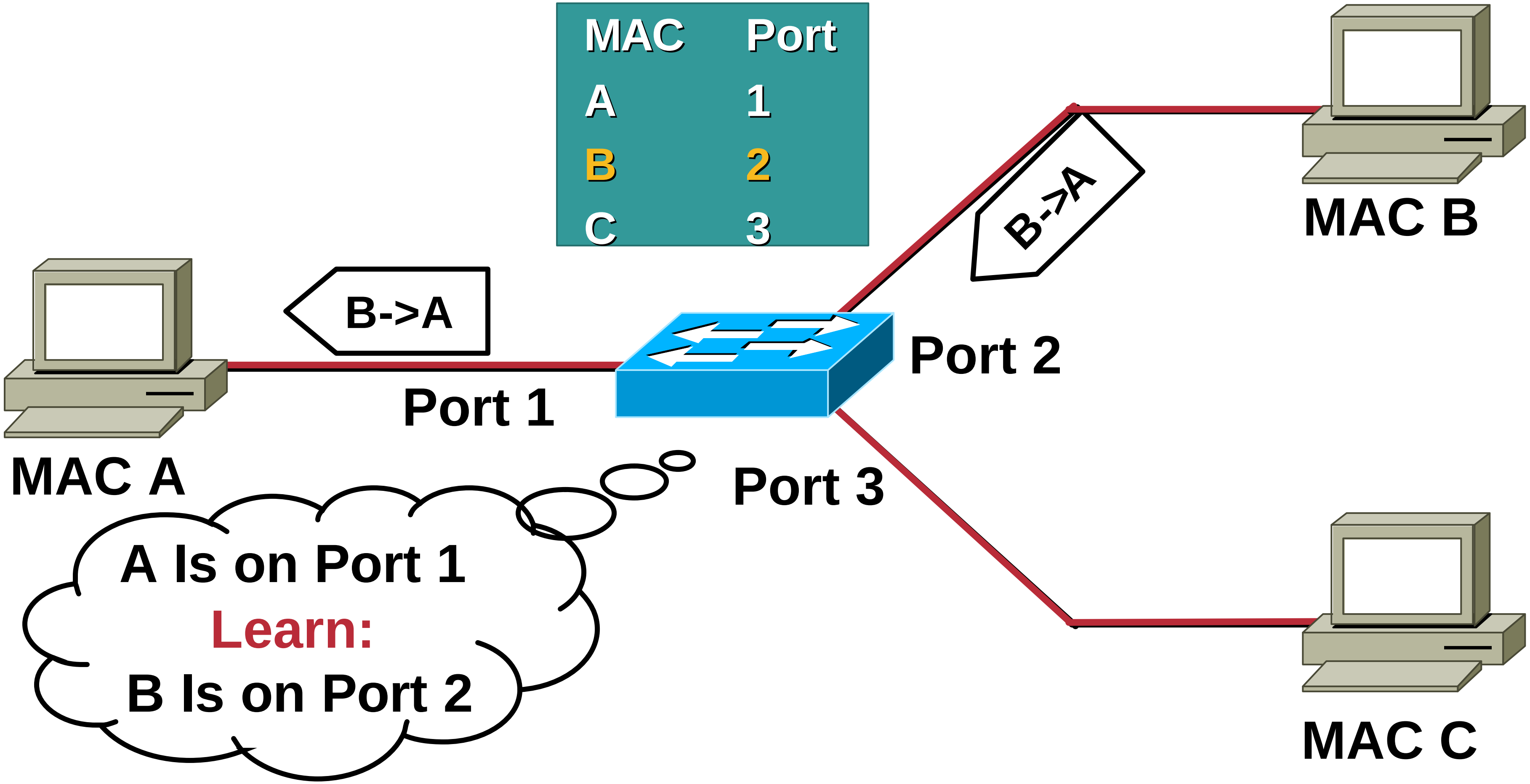
© 2003, Cisco Systems, Inc. All rights reserved.

Normal CAM Behaviour 1/3



MAC	Port
A	1
C	3

Normal CAM Behaviour 2/3

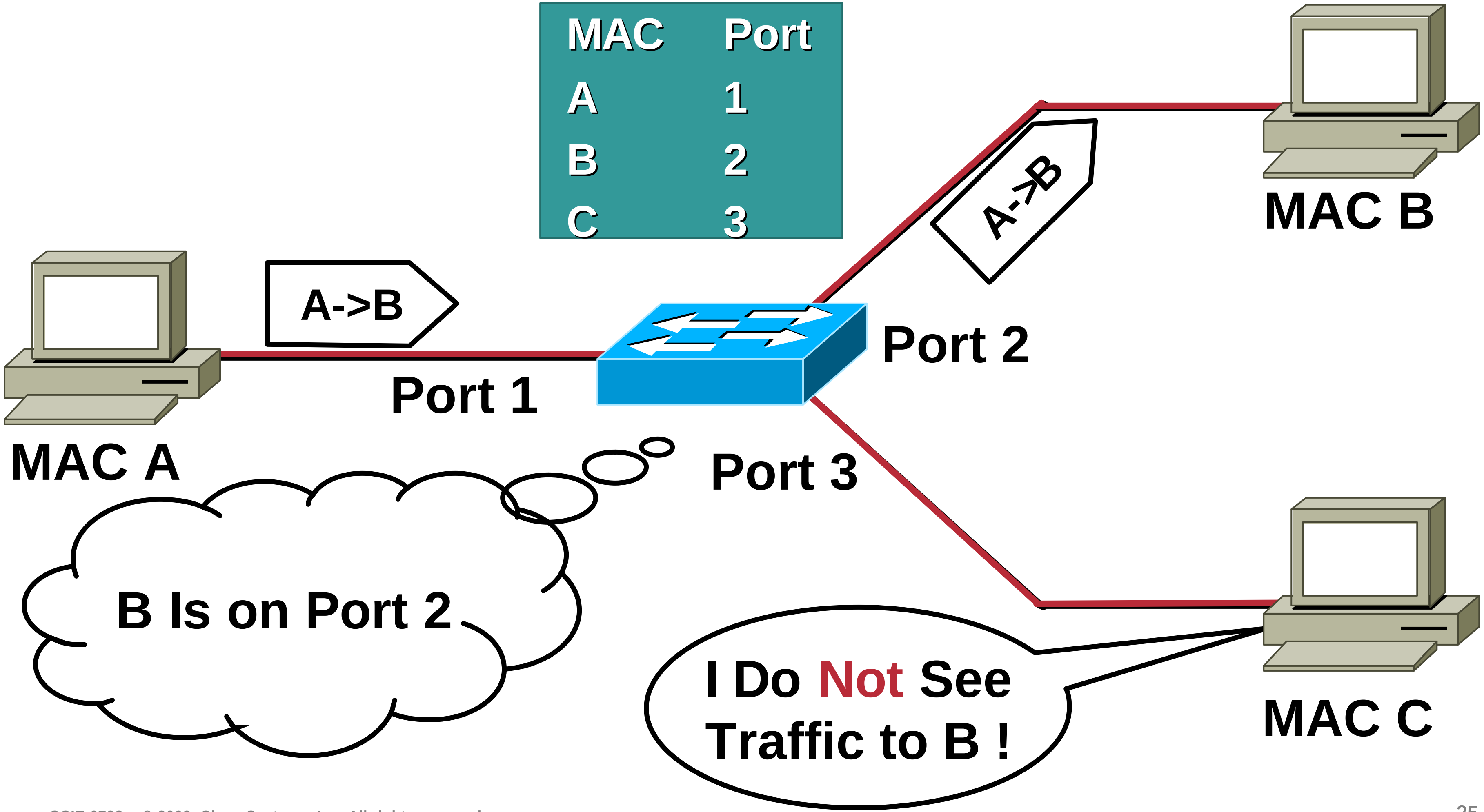


MAC	Port
A	1
B	2
C	3

A Is on Port 1
Learn:
B Is on Port 2

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

Normal CAM Behaviour 3/3



MAC	Port
A	1
B	2
C	3

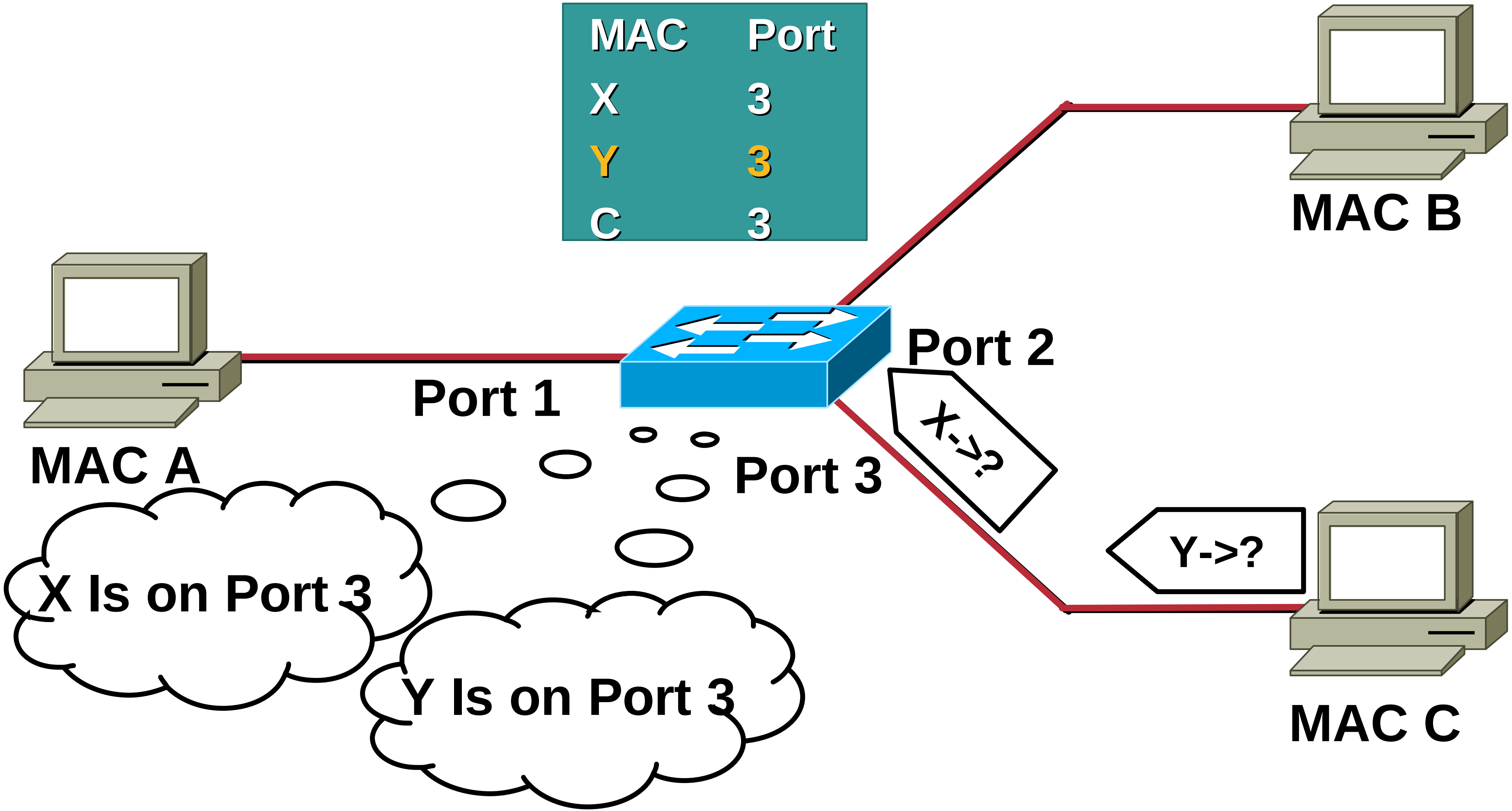
B Is on Port 2

I Do Not See Traffic to B !

CAM Overflow 1/3

- Theoretical attack until May 1999
- *macof* tool since May 1999
  - About 100 lines of perl from Ian Vitek
  - Later ported to C by Dug Song for “dsniff”
- Based on CAM Table’s limited size

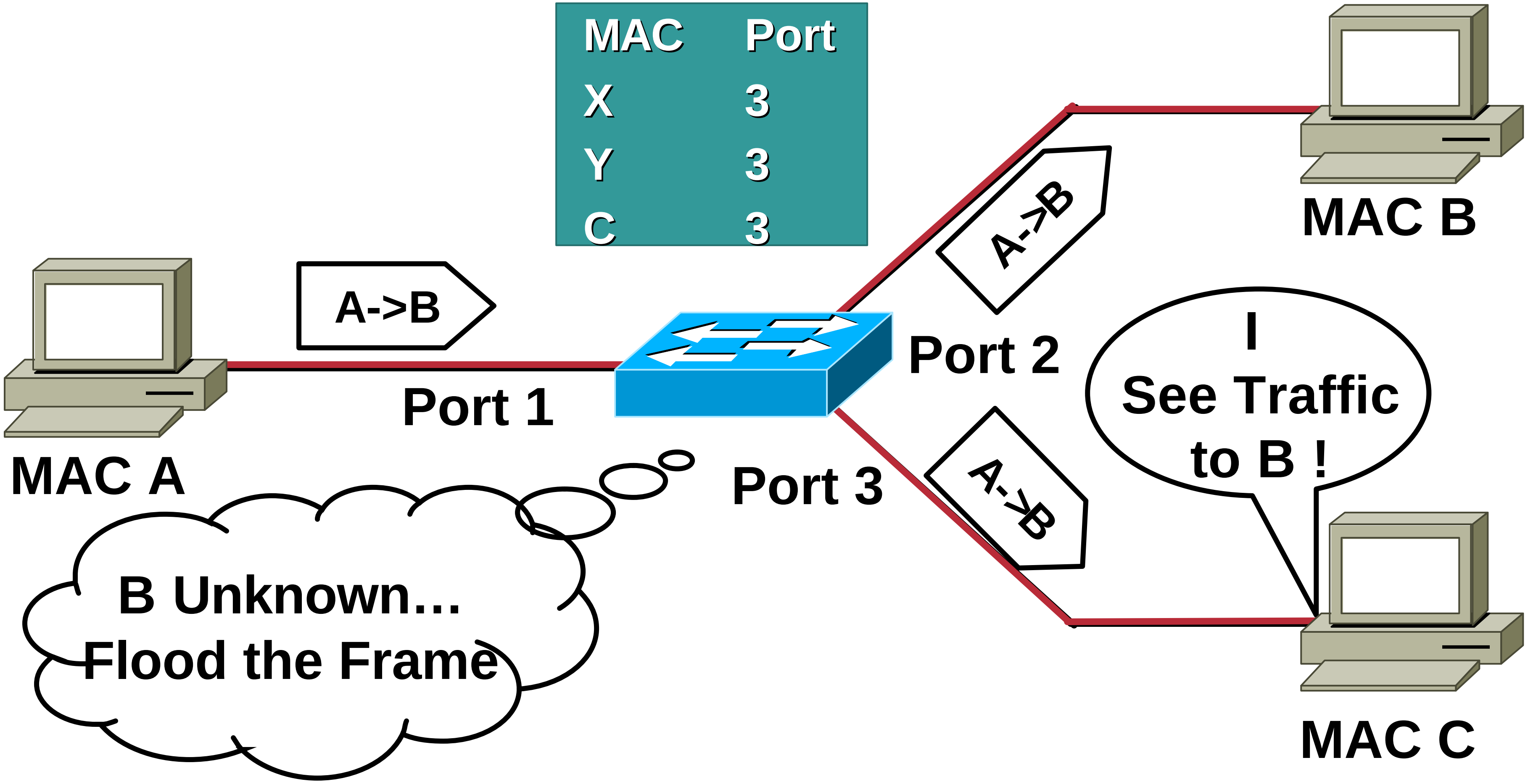
CAM Overflow 2/3



MAC	Port
X	3
Y	3
C	3

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

CAM Overflow 3/3



MAC	Port
X	3
Y	3
C	3

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

MAC Flooding Switches with Macof

```
[root@attack-lnx dsniff-2.3]# ./macof
b5:cf:65:4b:d5:59 2c:01:12:7d:bd:36 0.0.0.0.4707 > 0.0.0.0.28005: S 106321318:106321318(0) win 512
68:2a:55:6c:1c:1c bb:33:bb:4d:c2:db 0.0.0.0.44367 > 0.0.0.0.60982: S 480589777:480589777(0) win 512
1e:95:26:5e:ab:4f d7:80:6f:2e:aa:89 0.0.0.0.42809 > 0.0.0.0.39934: S 1814866876:1814866876(0) win 512
51:b5:4a:7a:03:b3 70:a9:c3:24:db:2d 0.0.0.0.41274 > 0.0.0.0.31780: S 527694740:527694740(0) win 512
51:75:2e:22:c6:31 91:a1:c1:77:f6:18 0.0.0.0.36396 > 0.0.0.0.15064: S 1297621419:1297621419(0) win 512
7b:fc:69:5b:47:e2 e7:65:66:4c:2b:87 0.0.0.0.45053 > 0.0.0.0.4908: S 976491935:976491935(0) win 512
19:14:72:73:6f:ff 8d:ba:5c:40:be:d5 0.0.0.0.867 > 0.0.0.0.20101: S 287657898:287657898(0) win 512
63:c8:58:03:4e:f8 82:b6:ae:19:0f:e5 0.0.0.0.58843 > 0.0.0.0.40817: S 1693135783:1693135783(0) win 512
33:d7:e0:2a:77:70 48:96:df:20:61:b4 0.0.0.0.26678 > 0.0.0.0.42913: S 1128100617:1128100617(0) win 512
f2:7f:96:6f:d1:bd c6:15:b3:21:72:6a 0.0.0.0.53021 > 0.0.0.0.5876: S 570265931:570265931(0) win 512
22:6a:3c:4b:05:7f 1a:78:22:30:90:85 0.0.0.0.58185 > 0.0.0.0.51696: S 1813802199:1813802199(0) win 512
f6:60:da:3d:07:5b 3d:db:16:11:f9:55 0.0.0.0.63763 > 0.0.0.0.63390: S 1108461959:1108461959(0) win 512
bc:fd:c0:17:52:95 8d:c1:76:0d:8f:b5 0.0.0.0.55865 > 0.0.0.0.20361: S 309609994:309609994(0) win 512
bb:c9:48:4c:06:2e 37:12:e8:19:93:4e 0.0.0.0.1618 > 0.0.0.0.9653: S 1580205491:1580205491(0) win 512
e6:23:b5:47:46:e7 78:11:e3:72:05:44 0.0.0.0.18351 > 0.0.0.0.3189: S 217057268:217057268(0) win 512
c9:89:97:4b:62:2a c3:4a:a8:48:64:a4 0.0.0.0.23021 > 0.0.0.0.14891: S 1200820794:1200820794(0) win 512
56:30:ac:0b:d0:ef 1a:11:57:4f:22:68 0.0.0.0.61942 > 0.0.0.0.17591: S 1535090777:1535090777(0) win 512
```

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

CAM Table Full!

- Dsniff (macof) can generate 155,000 MAC entries on a switch per minute
- Assuming a perfect hash function, the CAM table will be completely filled after 131,052 (approx. 16,000 x 8) entries

  Since hash isn't perfect it actually takes 70 seconds to fill the CAM table

```
CAT6506 (enable) sho cam count dynamic

Total Matching CAM Entries = 131052
```

- Once table is full, traffic without a CAM entry floods on the local VLAN, but NOT existing traffic with an existing CAM entry
- This attack will also fill CAM tables of adjacent switches

Snoop Output on Non-SPAN Port 10.1.1.50

```
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) ← OOPS
10.1.1.25 -> 10.1.1.26    ICMP Echo reply (ID: 256 Sequence number: 7424) ← OOPS
```

MAC Flooding Attack Mitigation

- Port security

  Capabilities are dependent on the platform

  Allows you to specify MAC addresses for each port, or to learn a certain number of MAC addresses per port

  Upon detection of an invalid MAC the switch can be configured to block only the offending MAC or just shut down the port

  Port security prevents macof from flooding the CAM table

http://cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_4/config/sec_port.htm

Port Security Details

- Beware management burden and performance hit
- Lots of platform specific options besides just “ON/OFF”

```
CatOS> (enable) set port security mod/ports... [enable | disable]
[mac_addr] [age {age_time}] [maximum {num_ of_mac}] [shutdown
{shutdown_time}] [violation{shutdown | restrict}]

IOS(config-if)# port security [action {shutdown | trap} | max-mac-
count addresses]
```

- MAC Tables do not have unlimited size (platform dependent)
- “Restrict” option may fail under macof load and disable the port, shutdown option is more appropriate

```
2002 Apr 03 15:40:32 %SECURITY-1-PORTSHUTDOWN:Port 3/21 shutdown due to no space
```

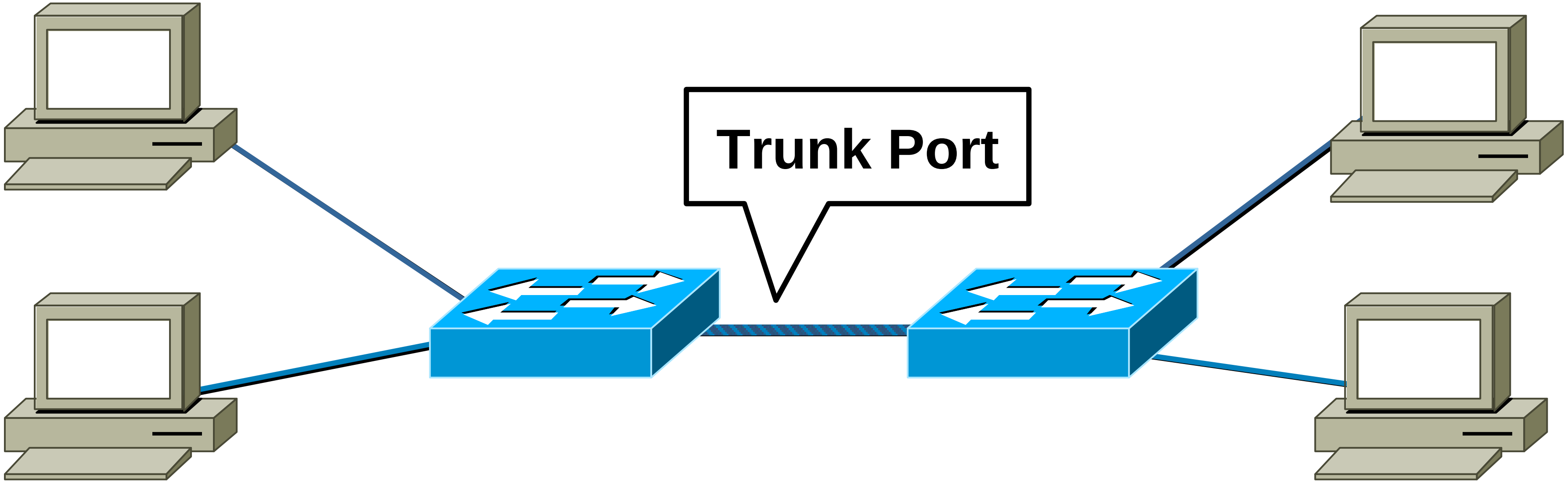
© 2003, Cisco Systems, Inc. All rights reserved.

Box security

VLAN Hopping

© 2002, Cisco Systems, Inc. All rights reserved.

Trunk Port Refresher



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

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

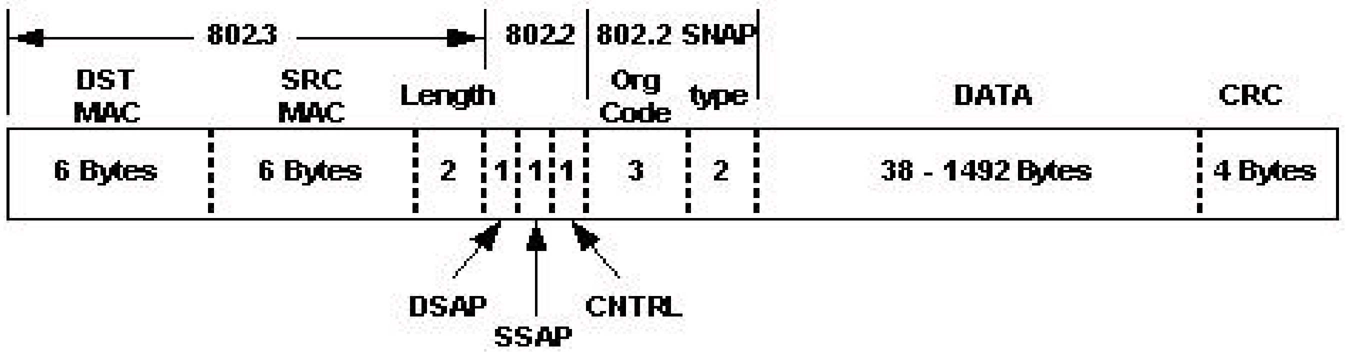
Cisco Switching Control Protocols

- **Used to negotiate trunk status, exchange VLAN information, etc.**
- **The majority use an IEEE 802.3 w/802.2 SNAP encapsulation**
  - **Includes LLC 0xAAAA03 (SNAP), and the Cisco OUI 0x00000C**
  - **Most use multicast destination addresses**
    - **Usually a variation on 0100.0ccc.cccc**
  - **Source address is derived from a bank of available addresses included in an EPROM on the chassis**
  - **SNAP Protocol Type varies and will be included through the rest of the talk**
- **CDP and VTP (two common Cisco control protocols) are passed over VLAN 1 only; if VLAN 1 is cleared from a trunk, although no user data is transmitted or received, the switch continues to pass some control protocols on VLAN 1**
  - **For this reason (and the fact that VLAN 1 can not be deleted) don't use it if you don't need to**

Lots of Detail: http://www.cisco.com/warp/public/473/103.html

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

For the Detail-Oriented: 802.3 w/802.2 SNAP



- DST MAC: Generally a variant of 0100.0ccc.cccc
- SRC MAC: Pulled from a pool in the switch EPROM
- 802.2 LLC fields

  DSAP:AA + SSAP:AA + CNTRL:03 = SNAP
- 802.2 SNAP fields

  Org Code: 0x00000c (Cisco)

  Protocol Type: Varies

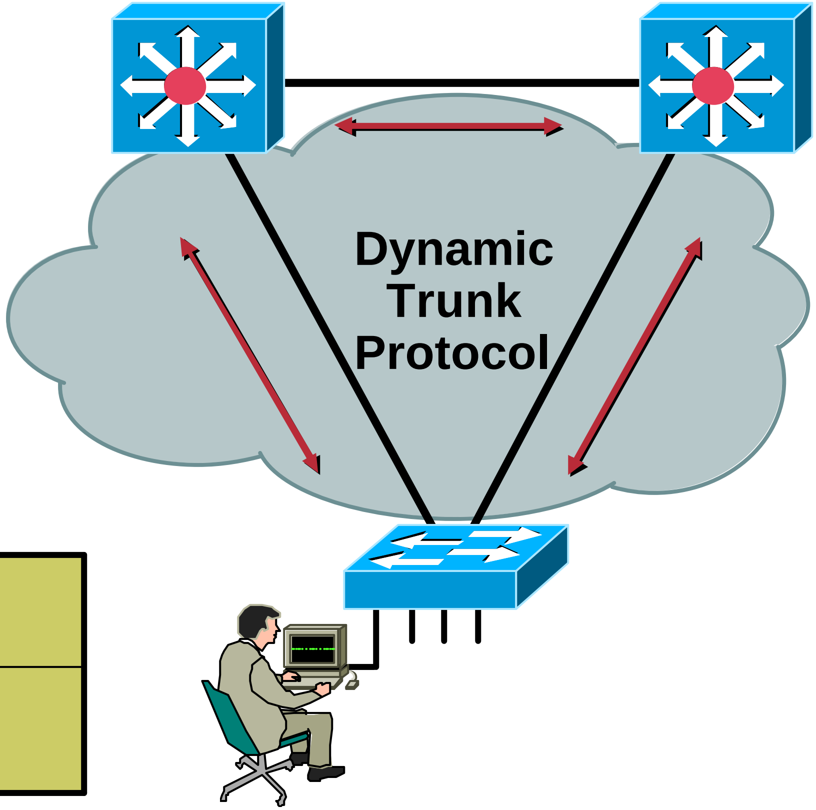
If You Like This Sort of Thing: http://www.cisco.com/warp/public/105/encheat.html

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

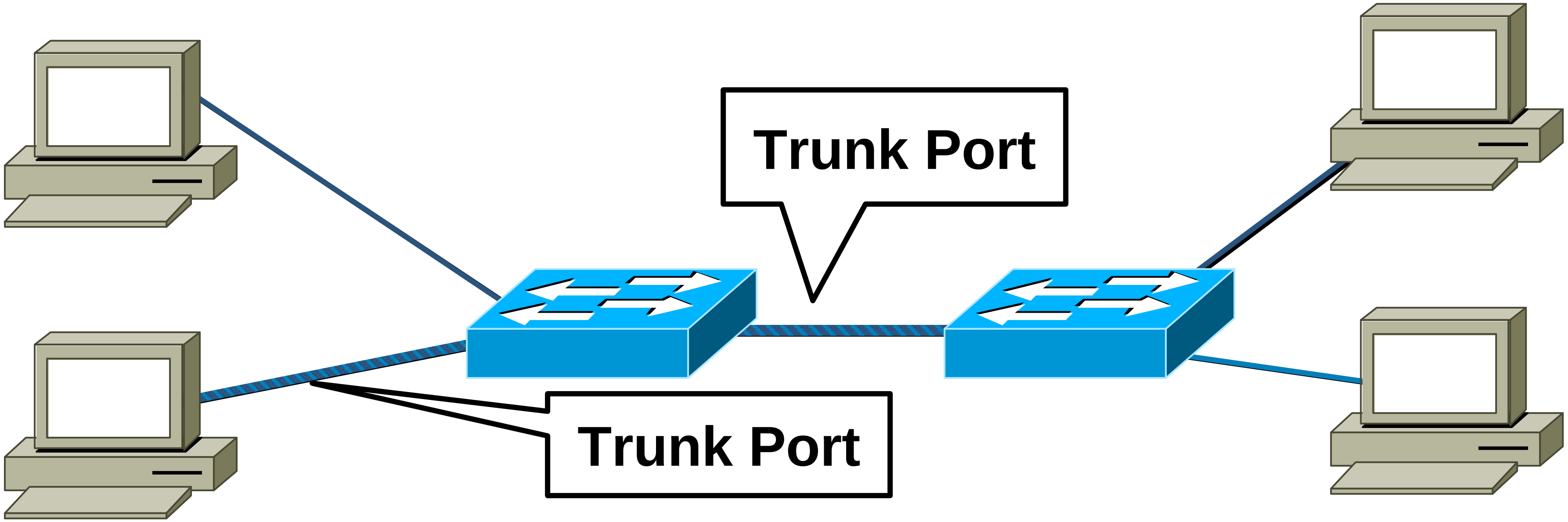
Dynamic Trunk Protocol (DTP)

- What is DTP?
  - Automates ISL/802.1Q trunk configuration
  - Operates between switches
  - Does not operate on routers
  - Not supported on 2900XL or 3500XL
- DTP synchronizes the trunking mode on link ends
- DTP state on ISL/1Q trunking port can be set to “Auto”, “On”, “Off”, “Desirable”, or “Non-Negotiate”

DST MAC	0100.0ccc.cccc
SNAP Proto	0x2004



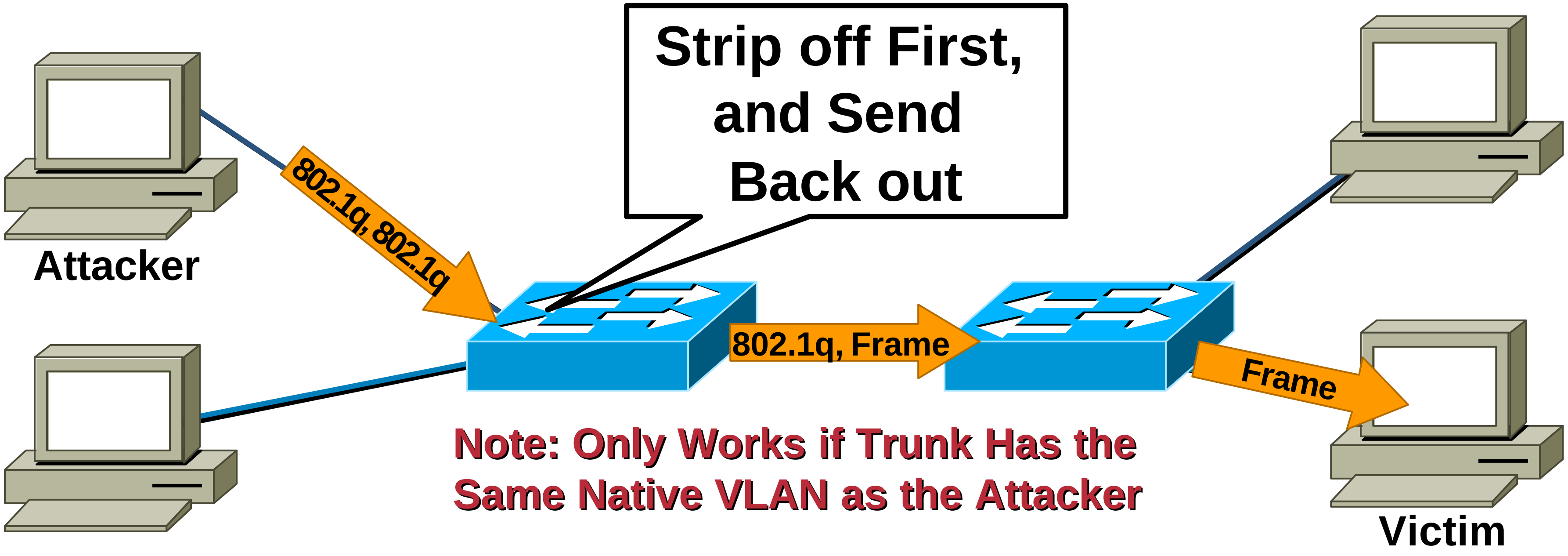
Basic VLAN Hopping Attack



- A station can spoof as a switch with ISL or 802.1Q signaling (DTP signaling is usually required as well, or a rogue DTP speaking switch)
- The station is then member of all VLANs
- Requires a trunking favorable setting on the port

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

Double Tagged 802.1q VLAN Hopping Attack

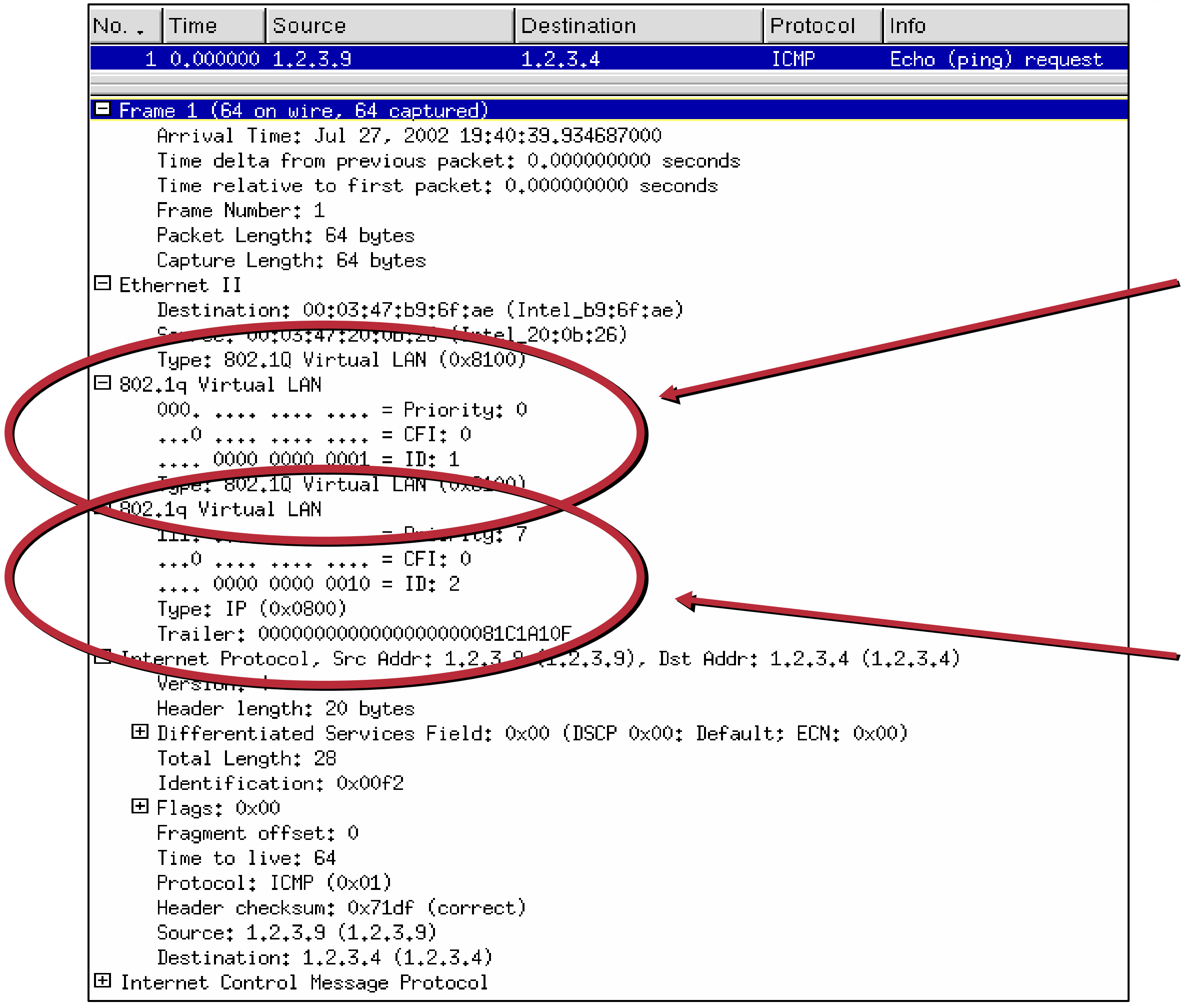


Note: Only Works if Trunk Has the Same Native VLAN as the Attacker

- Send double tagged 802.1Q frames
- Switch performs only one level of decapsulation
- Unidirectional traffic only
- Works even if trunk ports are set to off

Ulf Vinneras CCIE 6798 © 2003, Cisco Systems, Inc. All rights reserved.

Double Tagged 802.1Q Ethereal Capture



```
No. .  Time      Source        Destination   Protocol  Info
  1 0.000000  1.2.3.9       1.2.3.4       ICMP      Echo (ping) request

⊟ Frame 1 (64 on wire, 64 captured)
      Arrival Time: Jul 27, 2002 19:40:39.934687000
      Time delta from previous packet: 0.000000000 seconds
      Time relative to first packet: 0.000000000 seconds
      Frame Number: 1
      Packet Length: 64 bytes
      Capture Length: 64 bytes
⊟ Ethernet II
      Destination: 00:03:47:b9:6f:ae (Intel_b9:6f:ae)
      Source: 00:03:47:20:0b:26 (Intel_20:0b:26)
      Type: 802.1Q Virtual LAN (0x8100)
⊟ 802.1q Virtual LAN
      000. .... .... .... = Priority: 0
      ...0 .... .... .... = CFI: 0
      .... 0000 0000 0001 = ID: 1
      Type: 802.1Q Virtual LAN (0x8100)
⊟ 802.1q Virtual LAN
      111. .... .... .... = Priority: 7
      ...0 .... .... .... = CFI: 0
      .... 0000 0000 0010 = ID: 2
      Type: IP (0x0800)
      Trailer: 00000000000000000000081C1A10F
⊟ Internet Protocol, Src Addr: 1.2.3.9 (1.2.3.9), Dst Addr: 1.2.3.4 (1.2.3.4)
      Version: 4
      Header length: 20 bytes
    ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
      Total Length: 28
      Identification: 0x00f2
    ⊞ Flags: 0x00
      Fragment offset: 0
      Time to live: 64
      Protocol: ICMP (0x01)
      Header checksum: 0x71df (correct)
      Source: 1.2.3.9 (1.2.3.9)
      Destination: 1.2.3.4 (1.2.3.4)
⊞ Internet Control Message Protocol
```

Outer Tag, Attacker VLAN

Inner Tag, Victim VLAN

Disabling Auto-Trunking

```
CatOS> (enable) set trunk <mod/port> off

or

CatOS> (enable) set port host <mod/port>
IOS(config-if)#switchport mode access
```

- **Defaults change depending on switch; always check:**

  From the Cisco docs: “The default mode is dependent on the platform…”

  To check from the CLI:

```
CatOS> (enable) show trunk [mod|mod/port]
IOS# show interface type number switchport
```

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
- Set all user ports to non-trunking (DTP Off)

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

Box security

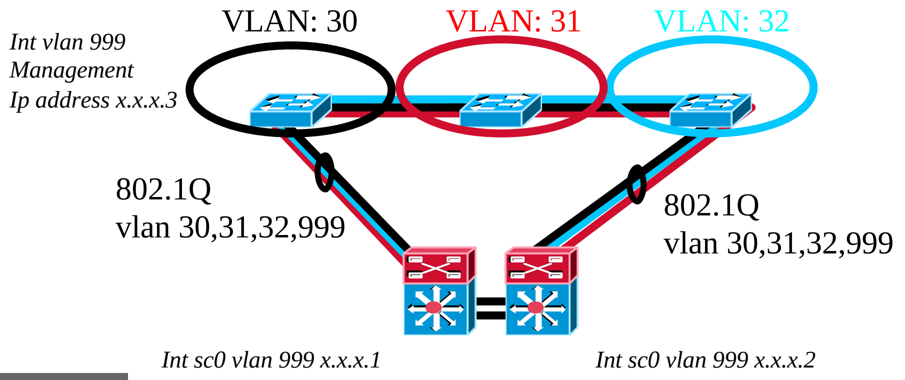
Access security

© 2002, Cisco Systems, Inc. All rights reserved.

Access security

Design your network with isolated management vlan

There is no need to permit unauthorised traffic to the management vlan at all !!!



VLAN: 30

VLAN: 31

VLAN: 32

Int vlan 999
Management
Ip address x.x.x.3

802.1Q
vlan 30,31,32,999

802.1Q
vlan 30,31,32,999

Int sc0 vlan 999 x.x.x.1

Int sc0 vlan 999 x.x.x.2

On the MSFC

```
Int vlan 999
access-group 101 out
!
Access-list 101 permit tcp host bastion1.domain.com any eq 23
Access-list 101 permit tcp host bastion2.domain.com any eq 23
Access-list 101 permit tcp host snmpsrv1.domain.com any eq 161
```

Should be combined with telnet access-lists!!!

Access security, cont 1

- SNMP community, no public / private, acl attached
- Use SNMP v3

```
snmp-server host 195.22.1.3 f4ult1
snmp-server host 195.22.2.3 fa6lt2
/* snmp host is used for snmp traps */
snmp-server community k4llekula RO 2
snmp-server community 87gf6v3c RW 3
snmp-server trap-source Loopback0
```

```
access-list 2 permit 195.20.1.160 0.0.0.31
access-list 3 permit 195.21.1.160 0.0.0.31
```

Different community on access devices compared to the rest of the network

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

Access security, cont 2

Enable secret, aaa authentication and accounting

```
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication enable default enable
aaa accounting commands 15 default start-stop group tacacs+
```

This will give you a searchable database holding all applied level 15 commands, sorted per user

Access security, cont 3

- Important to be in control over who has made a configuration change and when. Store config history and changes (Rancid or Natkit).
- Use Rancid to collect all core and distribution configurations every 15 min, all access configurations every 24 hours.
- This is like FW, only install RANCID if you intend to have one engineer responsible for following up config changes.

http://www.shrubbery.net/rancid/

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

Agenda

- Feature Overview
- Box security

  SNMP, pwd recovery, telnet/consol

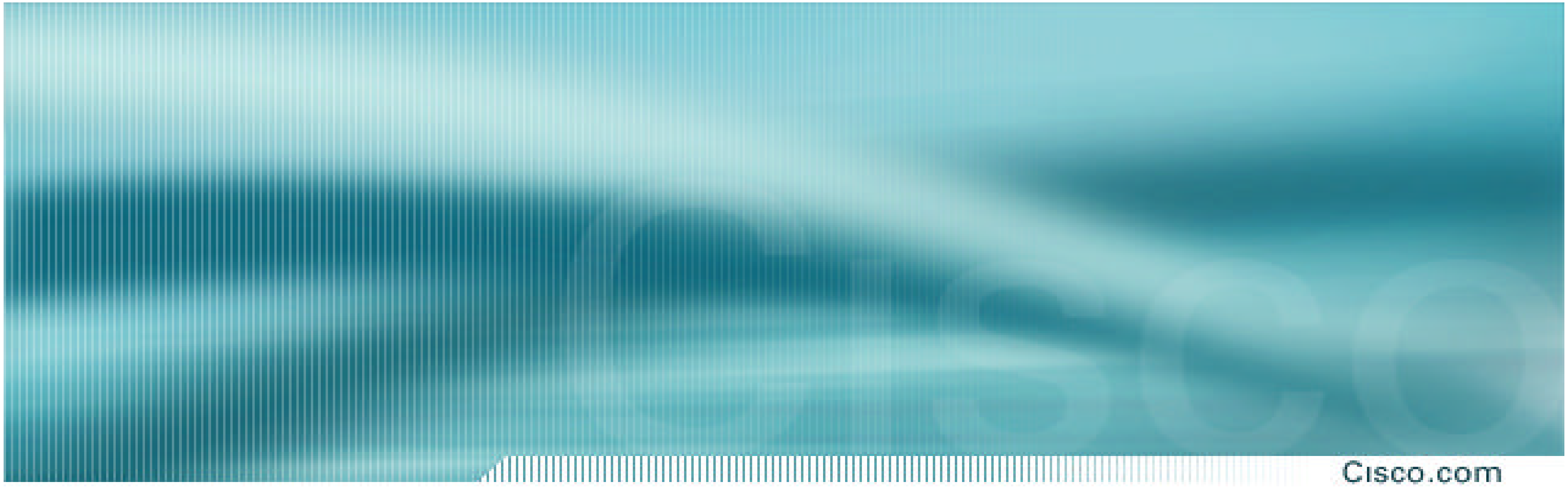
- **Networking protocols**

  IGP, EGP, HSRP, VRRP, Spanning-tree, cdp, ip spoofing

- User protection

  Security between users

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



Networking protocol security

CDP [Cisco Discovery Protocol] security

© 2002, Cisco Systems, Inc. All rights reserved.

CDP security, function

- Cdp is Cisco proprietary

  An L2 protocol informing the neighbour of the device existence. CDP works over different media. Gives information regarding ip address, physical port, sw version, hw platform.

- In the ETTx environment (many L2 switches) CDP is an outstanding feature

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

CDP security, function

```
ds1-sto1-se> (enable) sh cdp nei det
Port (Our Port): 1/1
Device-ID: cr1.sto1.se
Device Addresses:
  IP Address: 197.154.18.1
    CLNS Address: 39752f:0100:4242:0000:0000:0000:1971:5401:8001:00
Holdtime: 169 sec
Capabilities: ROUTER
Version:
  Cisco Internetwork Operating System Software
  IOS (tm) GS Software (GSR-K4P-M), Version 12.0(21)S1, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
  TAC Support: http://www.cisco.com/tac
  Copyright (c) 1986-2002 by cisco Systems, Inc.
  Compiled Tue 19-Feb-02 14:47 by nmasa
Platform: cisco 12016/GRP
Port-ID (Port on Neighbors's Device): GigabitEthernet0/0
VTP Management Domain: unknown
Native VLAN: unknown
Duplex: unknown
System Name: unknown
System Object ID: unknown
Management Addresses: unknown
Physical Location: unknown
```

CDP security, attack

- Linux

  Unfortunately there are Linux sw that floods cdp updates full of crap

- BUG

  In some old IOS releases there are no limitations on how many cdp entries there can be in the memory. This fact can cause malloc failures, and even a complete crash of the switch/router.

- CDP can consume all memory

  Solved in recent IOS releases

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

CDP security, solution

- **Since CDP only can traverse one L2-hop, the workaround is pretty simple:**
- **Turn off CDP on all customer ports!!!**

On each customer port:

```
interface FastEthernet0/2
 description ****** clientport ******
 no cdp enable
```

Network protocol security

Spanning tree security

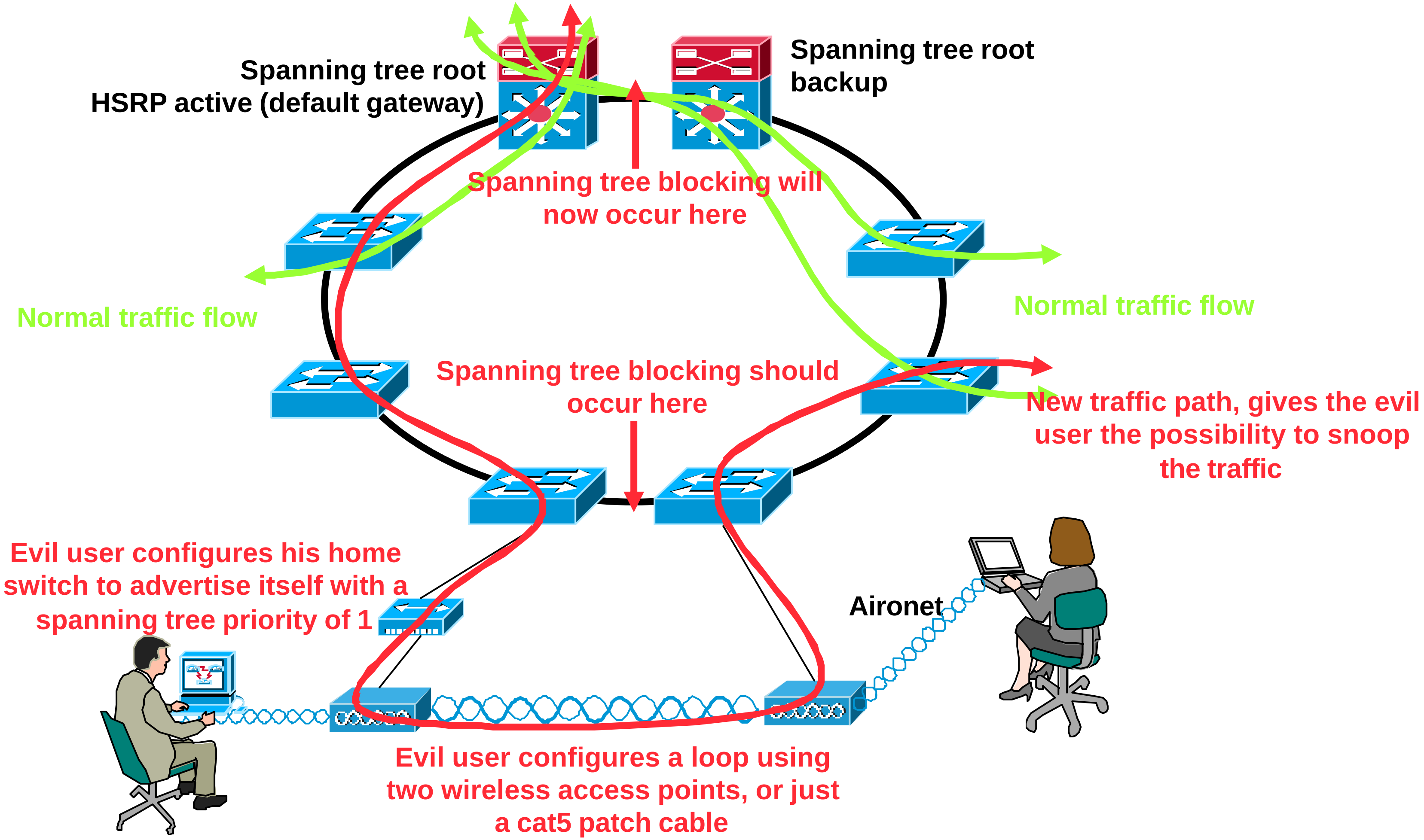
© 2002, Cisco Systems, Inc. All rights reserved.

Spanning tree security

- Spanning tree is the protocol used to avoid loops in an L2 environment
- Almost all traffic will pass via the root bridge
- Normally the root bridge is the same as or a switch close to the L3 device (the default gateway)

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

Spanning tree security, attack



Spanning tree root
HSRP active (default gateway)

Spanning tree root
backup

Spanning tree blocking will now occur here

Normal traffic flow

Normal traffic flow

Spanning tree blocking should occur here

New traffic path, gives the evil user the possibility to snoop the traffic

Evil user configures his home switch to advertise itself with a spanning tree priority of 1

Evil user configures a loop using two wireless access points, or just a cat5 patch cable

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

Spanning tree security, attack prevention 1

- **This attack will not work in a properly designed ETTx network**
  - **No trunk towards the customer**
  - **Different vlans on each switch in the ring**
- **To avoid people trying to mess with the spanning tree in the network, configure bpdu-guard or bpdu-filter on the end user ports**
  - **Even if it isn’t possible to create a “man-in-the-middle” scenario an attack might cause problems**

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

Spanning tree security, attack prevention 2

On each 2950 port:

```
spanning-tree portfast bpduguard default
interface FastEthernet0/2
 description ****** clientport ******
spanning-tree portfast
```

From the configuration guide:

At the global level, you can enable BPDU guard on Port Fast-enabled ports by using the **spanning-tree portfast bpduguard default** global configuration command. Receiving a BPDU on a Port Fast-enabled port signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the port in the error-disabled state

Networking protocol Security

Routing protocol security

© 2002, Cisco Systems, Inc. All rights reserved.

Routing protocol security

- If the network is properly designed, there will be no IGP running on the end user vlans.
- If your design requires an IGP to be run on the customer vlan, MD5 authentication together with passive interface should be used.

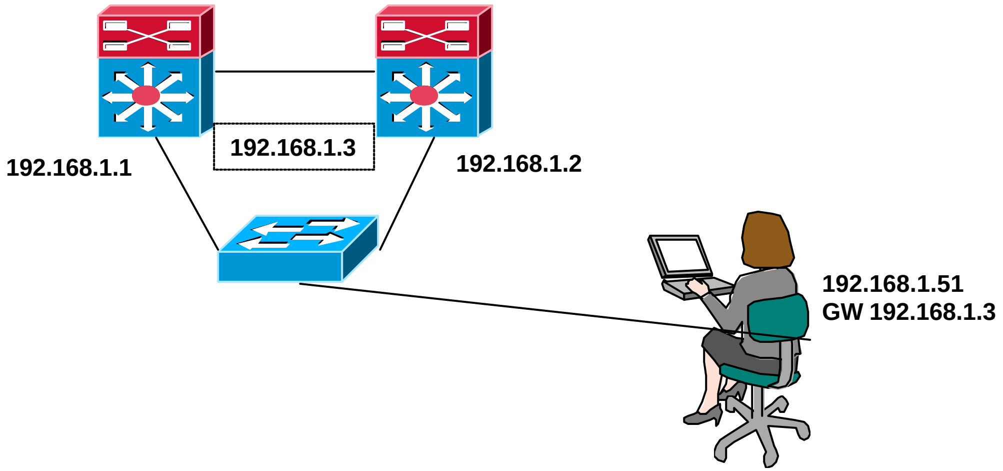
Networking protocol Security

HSRP [Hot Standby Routing Protocol] security

© 2002, Cisco Systems, Inc. All rights reserved.

HSRP security

- HSRP is a cisco proprietary solution for redundant gateways
- HSRP was designed before VRRP was available



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

HSRP security

- HSRP today relies on a clear text password
- With older code, a router went to standby even if it received an update with the wrong password (if the update had a better or the same priority)
- There is (no) way to stop end users from snooping hsrp passwords

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

HSRP security feature enhancement

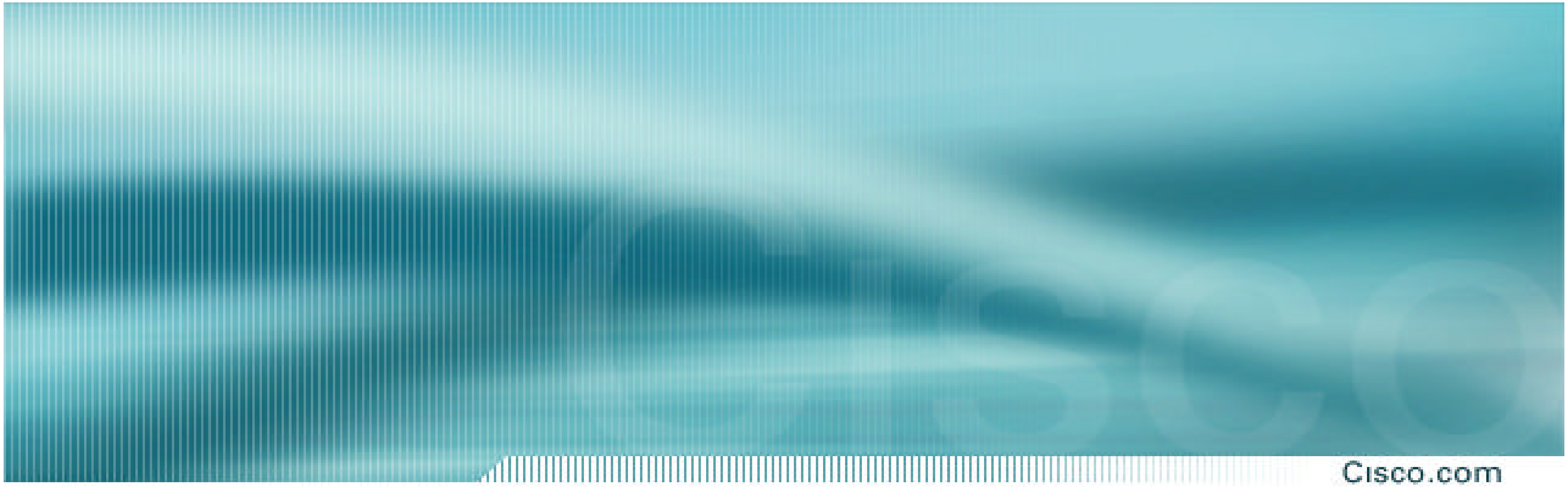
- HSRP packets will have support for encrypted password in the future

HSRP security, solution

- **A switch that supports inbound acl**
- **Deny all hsrp traffic from the customer [udp port 1985]**
- **Always configure a priority of 255 on your primary, and 254 on your standby router**
- **Customer will still see hsrp hellos, but will not be able to inject**

On each 2950/3550:

```
Access-list 101 deny udp any any eq 1985
Access-list 101 permit ip any any
!
interface FastEthernet0/2
 description ****** clientport ******
Ip access-group 101 in
```



Networking protocol Security

ICMP redirect

© 2002, Cisco Systems, Inc. All rights reserved.

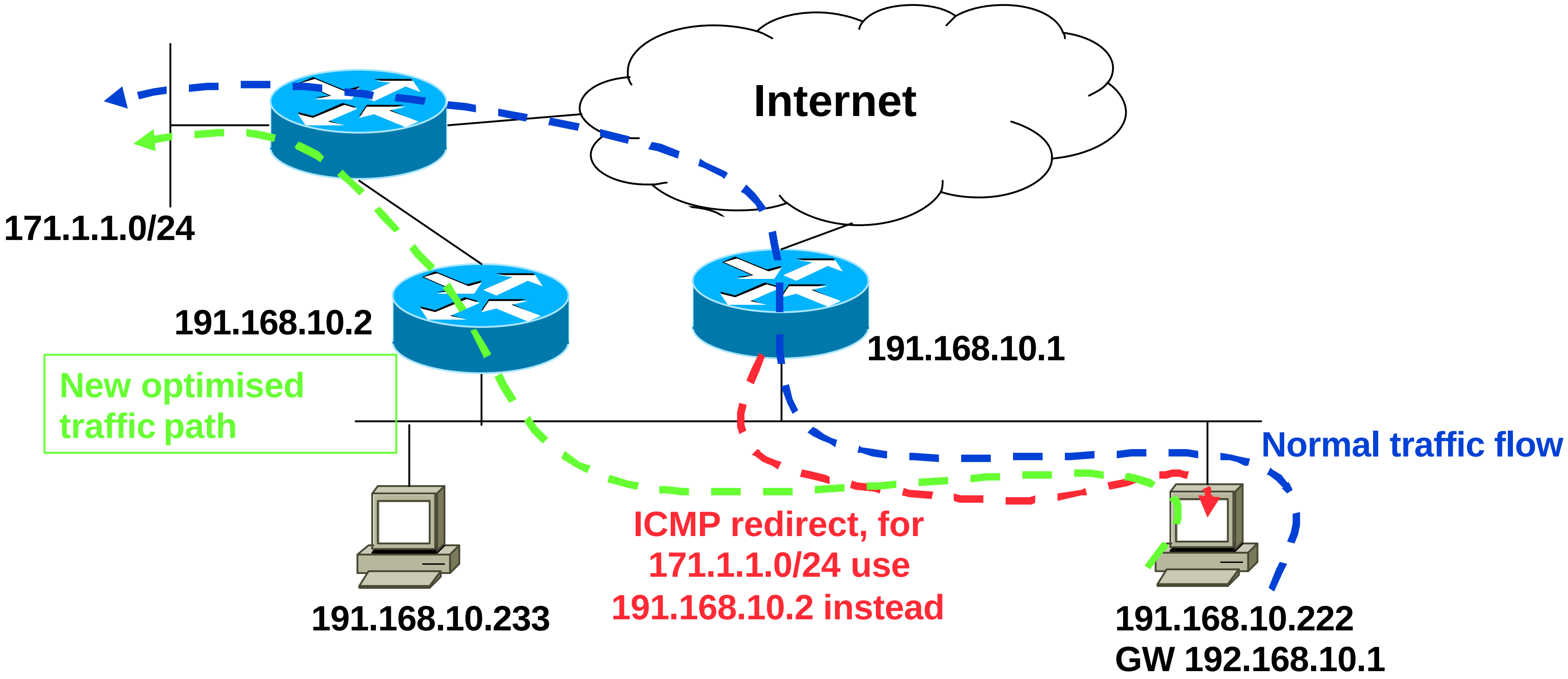
ICMP redirect

- ICMP is a control protocol within the IP stack
- ICMP redirect gives the possibility to reroute traffic
- This is not a threat in a correct designed network

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

ICMP redirect

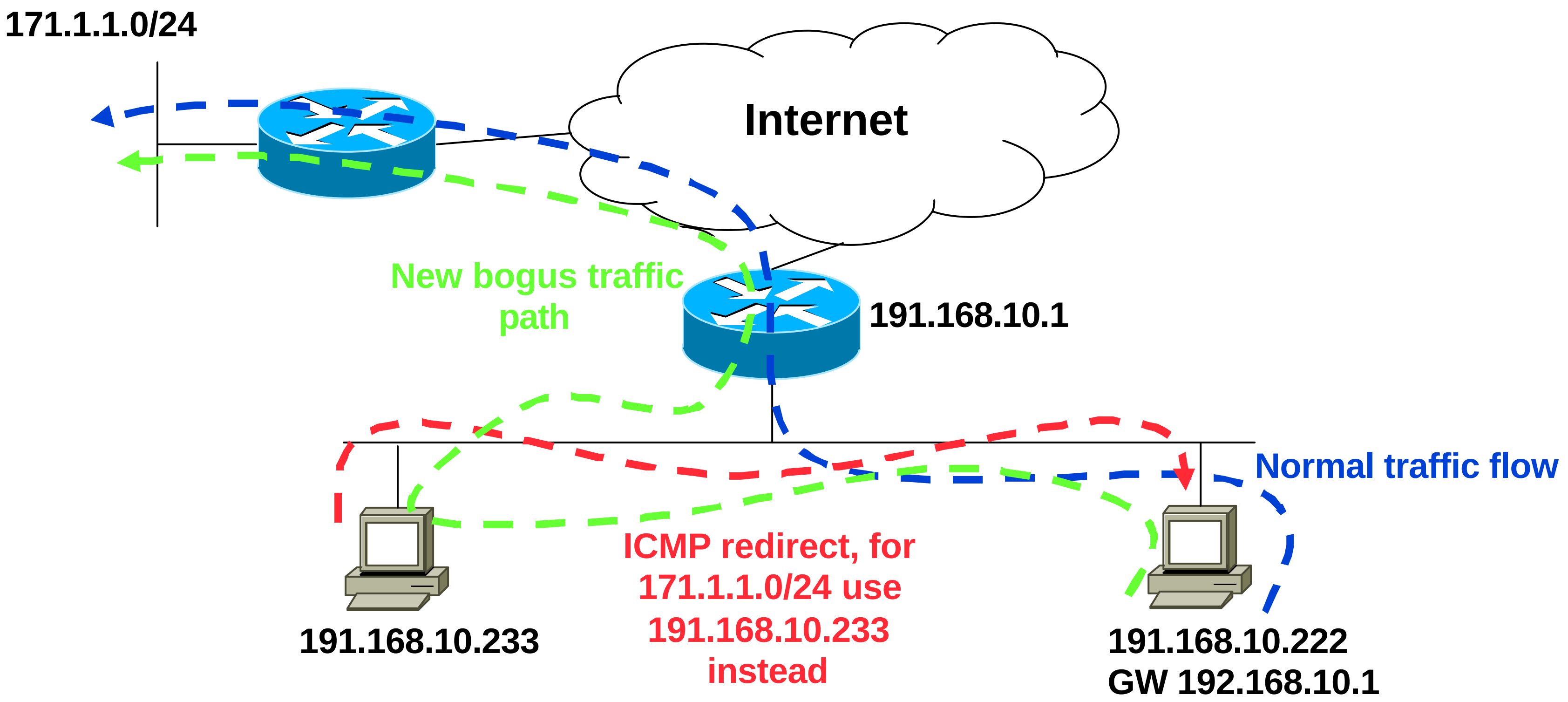
Fully automated based on routing table entries



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

ICMP redirect

What if…



171.1.1.0/24

Internet

New bogus traffic path

191.168.10.1

Normal traffic flow

191.168.10.233

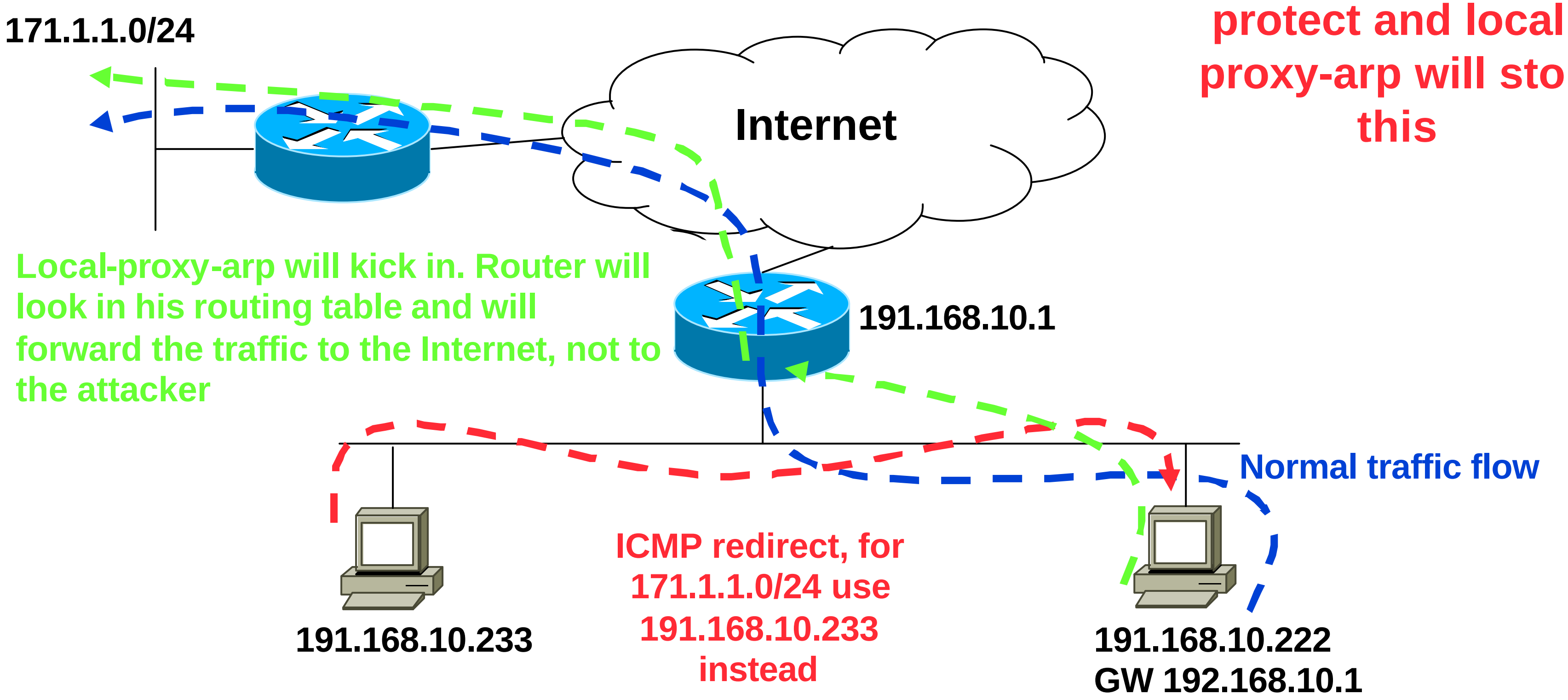
ICMP redirect, for 171.1.1.0/24 use 191.168.10.233 instead

191.168.10.222
GW 192.168.10.1

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

ICMP redirect

What if…



Private Vlan / port protect and local-proxy-arp will stop this

Local-proxy-arp will kick in. Router will look in his routing table and will forward the traffic to the Internet, not to the attacker

Normal traffic flow

ICMP redirect, for 171.1.1.0/24 use 191.168.10.233 instead

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

Cisco.com

Networking protocol Security

Multicast security

© 2002, Cisco Systems, Inc. All rights reserved.

Multicast security

- The definition of Multicast is:

  1. If you send to group address, all members receive it
  2. You must be a "member" of a group to receive its data
  3. You do not have to be a member of a group to send to a group!!!

What if you are running a multicasted tv service, and every customer were able to interfere with the content!

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

Multicast security, solution 1

- Configure a VACL to filter out multicast from the customers

```
ds1-row1-lab> (enable) set security acl ip ettx_vacl permit IGMP any any
ds1-row1-lab> (enable) set security acl ip ettx_vacl permit ip legal_source_network 224.100.0.0 15.128.255.255
ds1-row1-lab> (enable) set security acl ip ettx_vacl deny ip any 224.100.0.0 15.128.255.255
```

- Run MVR [Multicast Vlan Registration for the tv channels.

  The leaking mechanism in MVR will prevent customers from interfering with the tv content (no multicast configured on the end user vlan)

http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35wc4/sc/swsyst.htm#xtocid40

Multicast security, solution 2

- **SSM, source specific multicast and IGMP v3 would solve these problems**

  Unfortunately there is very limited support for IGMP v3 and SSM on the set-top-box market today

  Running IGMP v3 it is up to the application to sort out that the content comes from the correct source

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

Networking protocol Security

Pay per view security

© 2002, Cisco Systems, Inc. All rights reserved.

Pay per view security

- **In the legacy cable tv / digital tv network, there is a problem today with people using “smart-cards” to watch channels they haven’t paid for**
- **As soon as we rely on the security in a box that the customer has control over (placed in the customers home) there will be a risk for hacking**

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

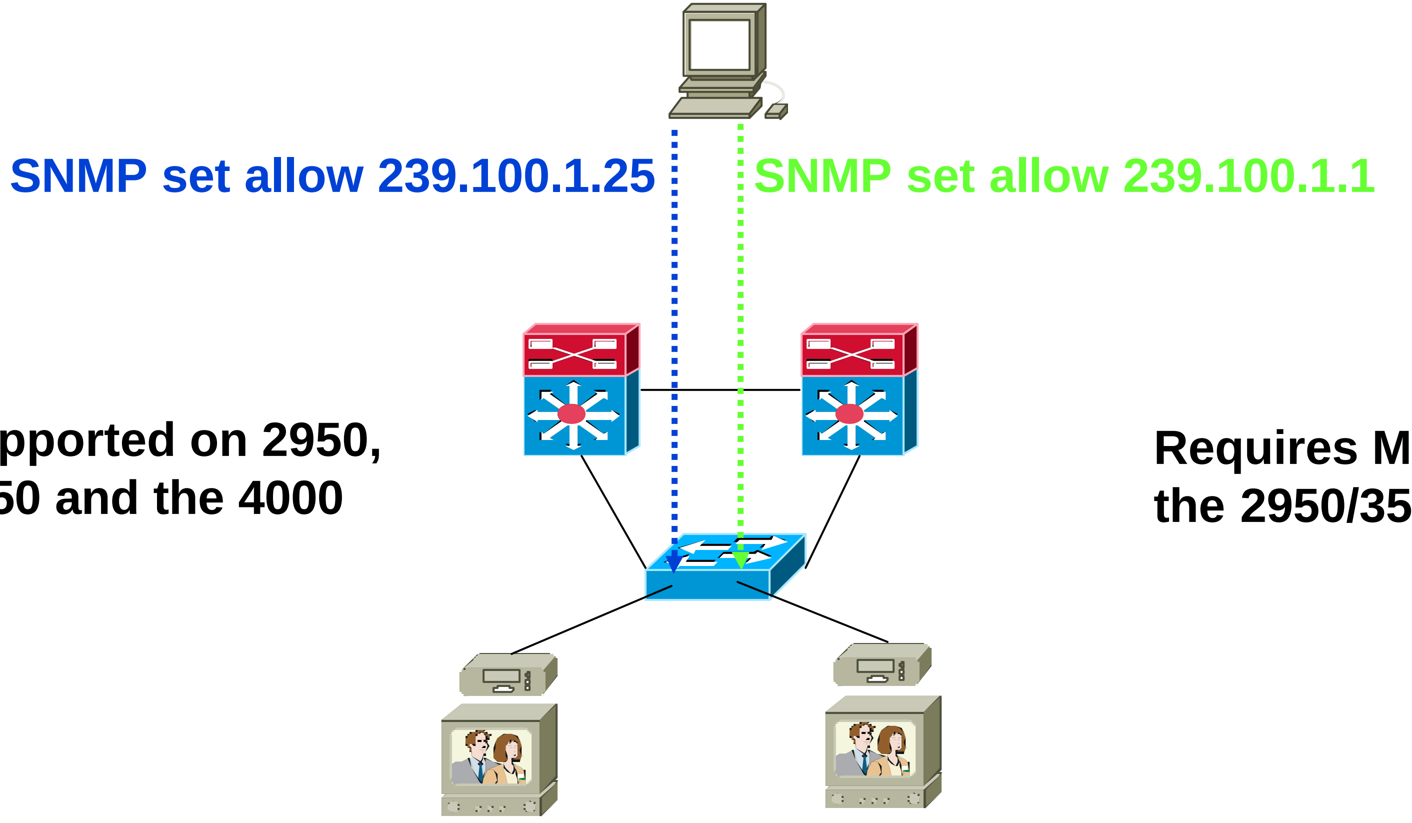
Pay per view security, igmp filtering

- On Switches we have the possibility to create igmp filters per port
- This gives us the possibility to turn on/off multicast channels per group and per port
- This is all done using SNMP set

  which makes it very easy for the service provider to integrate it in to their existing management / provisioning systems

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

Pay per view security, igmp filtering



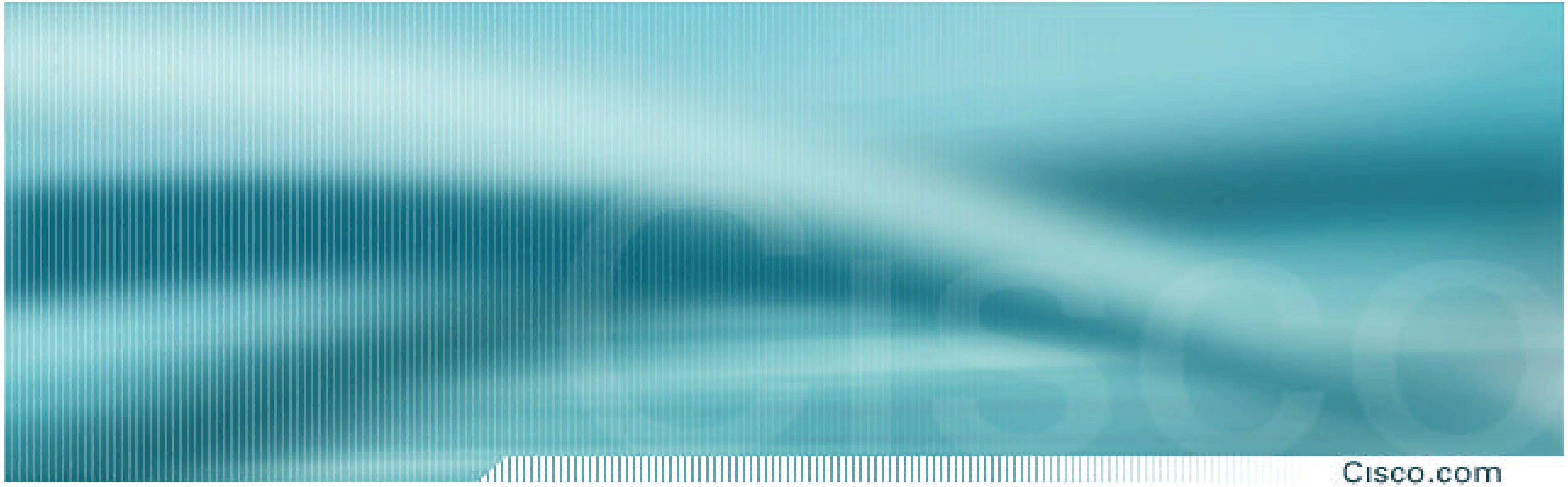
SNMP set allow 239.100.1.25

SNMP set allow 239.100.1.1

Supported on 2950, 3550 and the 4000

Requires MVR on the 2950/3550 !!!

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/1219ea1/scg/swigmp.htm#xtocid21



Networking protocol Security

IP source spoofing

Ip source spoofing

- Some users tries to change their ip address to a static one
- This can be because lack of knowledge, or a way to hide an attack

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

Ip source spoofing, attack

- Sourcing packets with a completely different network address, fooling acl, DoS attacks
- Sourcing packets with another customers ip address from the vlan he should belong to (to be able to both send and receive traffic)

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

Ip source spoofing, uRPF

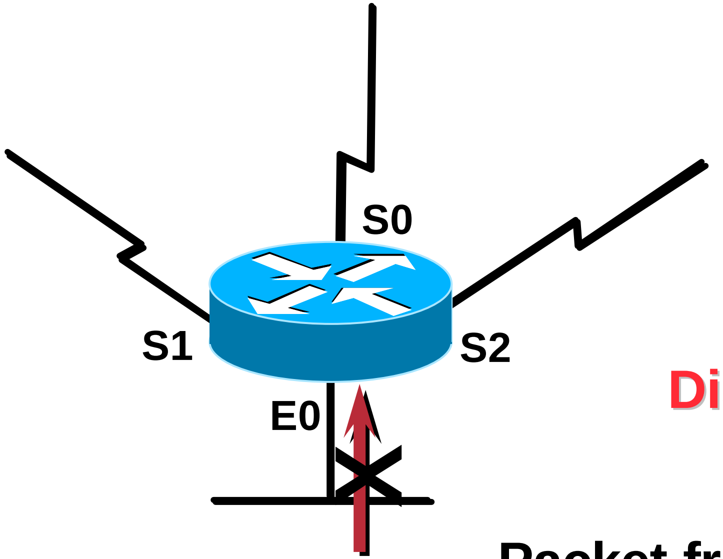
- On Routers it is possible to use uRPF [Unicast Reverse Path Forwarding]

Will prevent ip addresses from another subnet

Will not stop “stealing” another ip address in the same vlan

Ip source spoofing, uRPF 1

A closer look: RPF Check Fails



Discard Packet!

RPF Check Fails!

Unicast Route Table

Network	Interface
151.10.0.0/16	S1
198.14.32.0/24	S0
204.1.16.0/24	E0

Packet from
Source 151.10.3.21

Packet Arrived on Wrong Interface!

Ip source spoofing, uRPF 2

uRPF can be pretty cpu intensive

On all customer vlan in the 6500:

```
interface Vlan 30
 description ****** client_vlan ******
 ip verify unicast source reachable-via rx allow-self-ping
```

From the uRPF configuration guide:

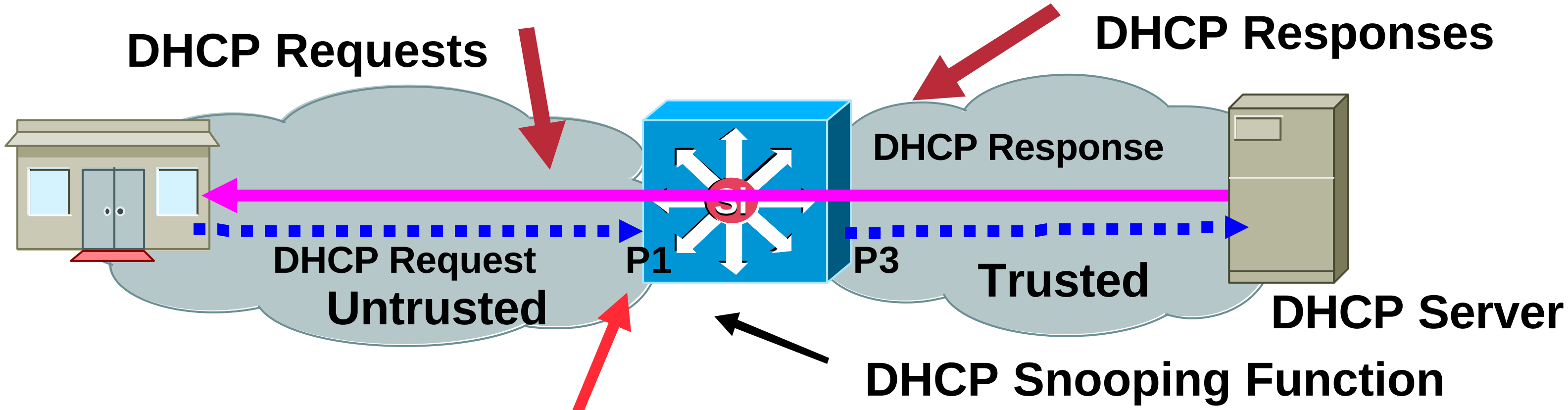
The Unicast RPF feature helps to mitigate problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by forwarding only packets that have source addresses that are valid and consistent with the IP routing table.

All done in HW on 6500 SUP2

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

IP Source Guard

- Automatically load Port ACLs and optionally port security tables with information learned from DHCP snooping
- Just like Dynamic ARP inspection, but for IP source address



IP source filter and mac security configured on port

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

Agenda

- Feature Overview
- Box security

  SNMP, pwd recovery, telnet/consol

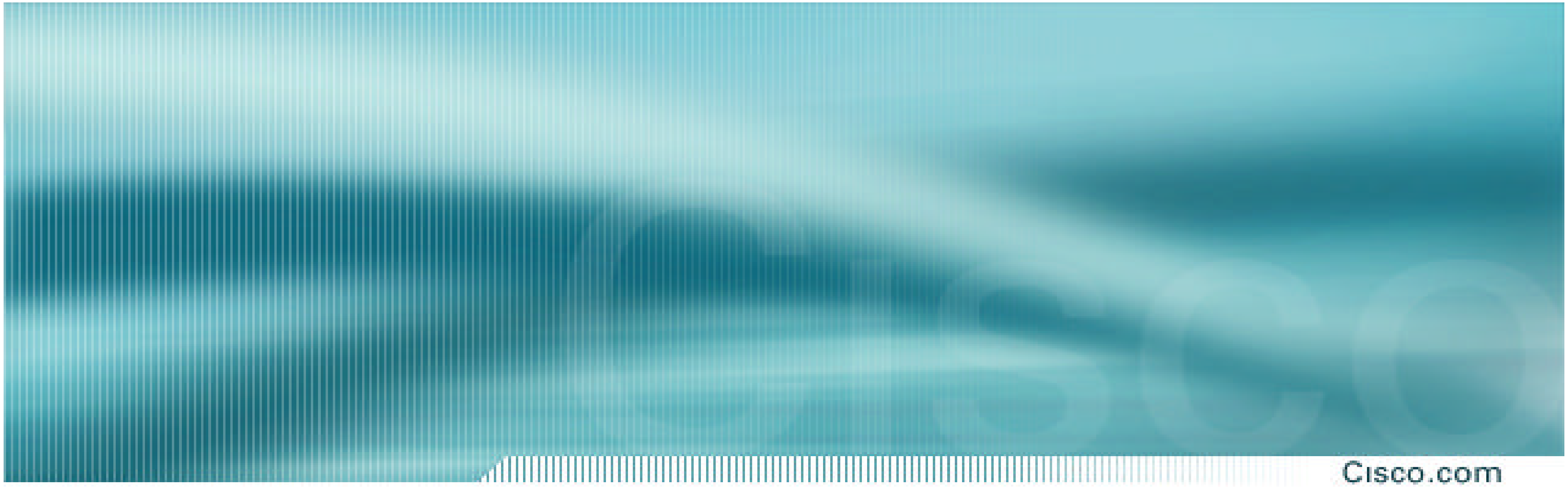
- Networking protocols

  IGP, EGP, HSRP, VRRP, Spanning-tree, cdp, ip spoofing

- **User protection**

  Security between users, user traceability

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



User protection

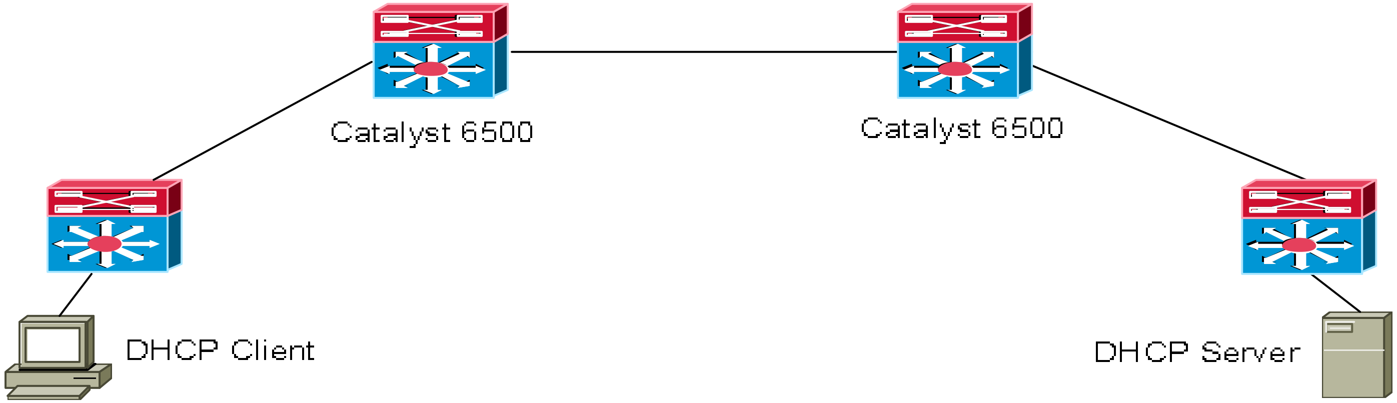
Traceability

© 2002, Cisco Systems, Inc. All rights reserved.

Traceability

- **In this type of network, it is extremely important to be able to trace the users**
- **The users have a lot of bandwidth, and can do nasty things against others**
- **We need to have a database of who had what ip address at what time**

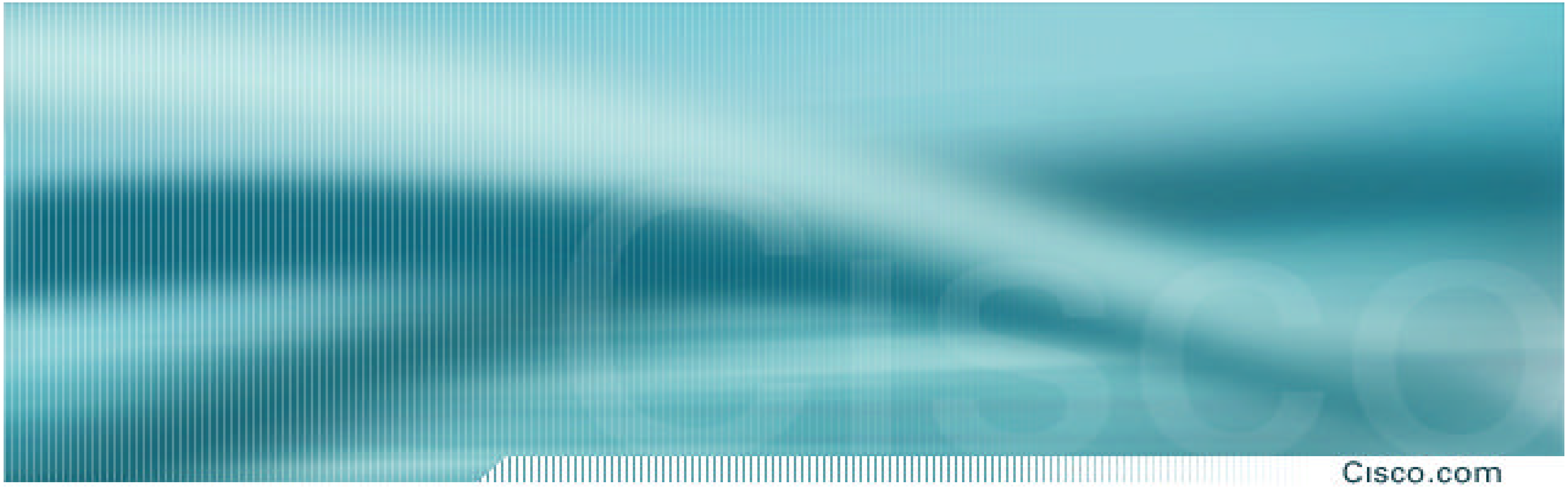
DHCP Interface Tracker (Option 82)



- DHCP Relay agent allows a router to insert information about itself when forwarding client DHCP packet to a DHCP server
- Every LAN switch has its own signature into the packet , Switch MAC address (remote-id), Port SNMP ifindex on 3550 (circuit id option), Module, Port, VLAN on 4K (circuit id)

```
3550#configure terminal
3550(config)# ip dhcp relay information option
```

- Catalyst 4500 IOS requires DHCP snooping for Option 82. Option 82: Module, VLAN, port is included with DHCP snooping



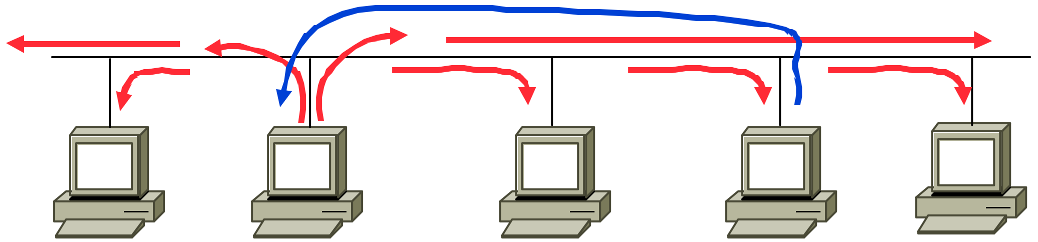
User protection

ARP security

© 2002, Cisco Systems, Inc. All rights reserved.

ARP security

- Before a pc can talk to another pc it must do an arp request to map the ip address to the physical [mac] address
- This arp request is a broadcast using ip 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



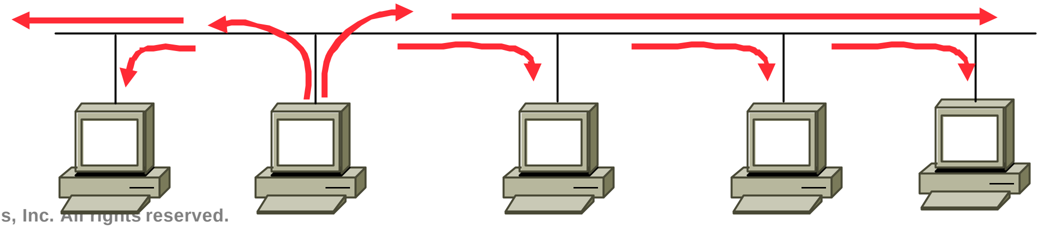
Ulf Vinneras CCIE 6798 © 2003, Cisco Systems, Inc. All rights reserved.

Arp security, gratuitous arp

- According to the arp rfc, a client is allowed to send an arp reply even if there hasn’t been a request. This is called a gratuitous arp. Other hosts on the same subnet can use this information and store it in its cache.

A gratuitous arp can be a unicast to another PC on the subnet, will not be detected by the MSFC

Hey everyone I’m host A and my IP Address is 192.168.1.1 and my MAC address is 00:03:47:8e:73:fd

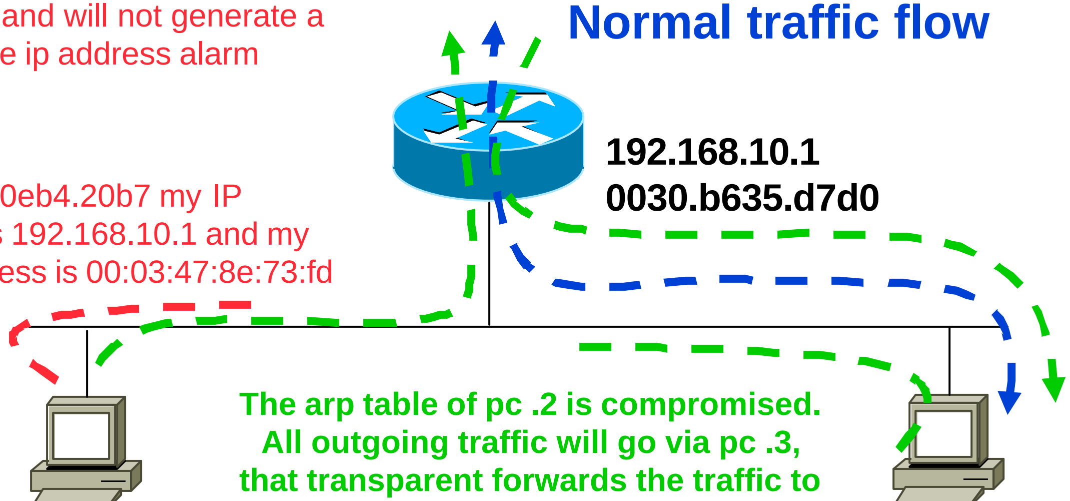


Arp security, gratuitous arp miss-use 1

- The arp rfc is from the time when everyone in a network was “friendly”
- There is no built in security in the arp function
- Anyone can claim to be the owner of any ip / mac address they like

Arp security, gratuitous arp miss-use 2

- What about if someone tries to steal an already used ip/mac address?



The router will just ignore this packet, and will not generate a duplicate ip address alarm

Normal traffic flow

192.168.10.1
0030.b635.d7d0

Hey 0007.0eb4.20b7 my IP Address is 192.168.10.1 and my MAC address is 00:03:47:8e:73:fd

The arp table of pc .2 is compromised. All outgoing traffic will go via pc .3, that transparent forwards the traffic to the router

192.168.10.3
0003.478e.73fd

192.168.10.2
0007.0eb4.20b7

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

Arp security, gratuitous arp miss-use 3

- All Traffic now flows through machine launching the attack

  Not quite a true sniffer trace but fairly close (simplex)

- Port security doesn’t help

  We are using our own mac address, the switch we are connected to can’t identify this as a faulty packet

- Note that attack could be generated in the opposite direction attacking the router to be able to sniff both directions of the stream

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

Arp security, gratuitous arp, tricky to use?

- At first this kind of attack seems pretty complex to launch
- Nice people on the internet have built tools for this, ettercap and dsniff are examples
- Ettercap includes a gui and spoofs both directions by default
- Dsniff includes "web mirroring" tools as well as "password sniffer" tools.

http://www.monkey.org/~dugsong/dsniff
http://ettercap.sourceforge.net

Arp security, protection 1

- Configuring static arp

  Many operating systems will still accept the gratuitous arp and flag the new entry as static

- Port security

  No help since all information on packet header level is valid (using our own mac address)

- Protected port (private vlan edge)

  As long as the vlan only exists on one switch, pvlan edge will protect other PCs, unfortunately it will not protect the router from being spoofed

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

Arp security, protection 2

- **Re-use of vlans**

  If the user vlan spans over more then one switch it is possible for an attacker to spoof clients on other switches, as long as they belong to the same vlan

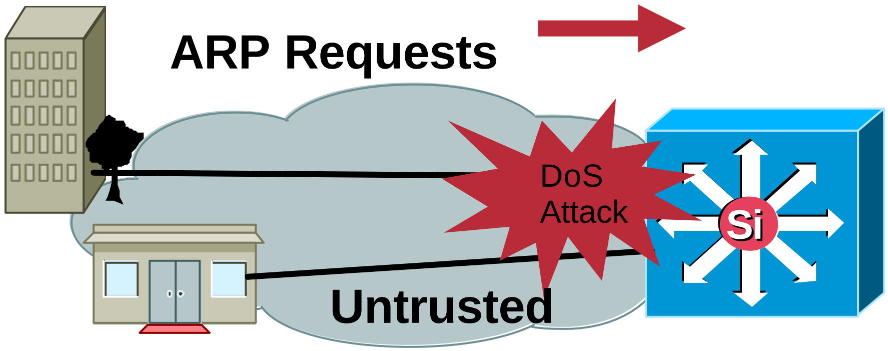
  (this is one of the major drawbacks of re-using vlans)

- **Arp security features**

  Secured arp tables, wouldn't that be nice?

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

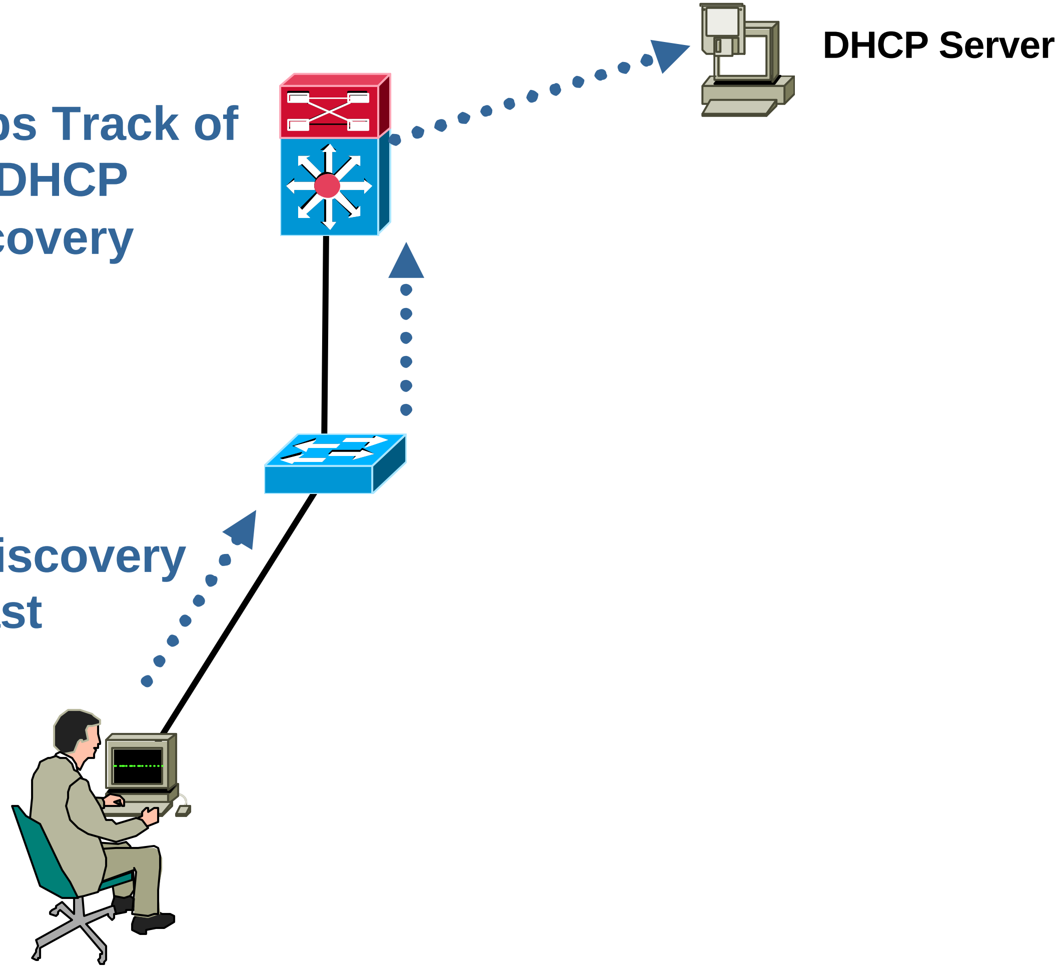
Dynamic ARP Inspection



- Uses an access list to permit or deny certain IP/MAC associations in the ARP table
- A binding table containing IP-address and MAC-address associations may be statically configured or dynamically populated using DHCP Snooping
- ARP ACLs deny (and optionally log) all invalid IP/MAC binding attempts

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

Dynamic ARP Inspection

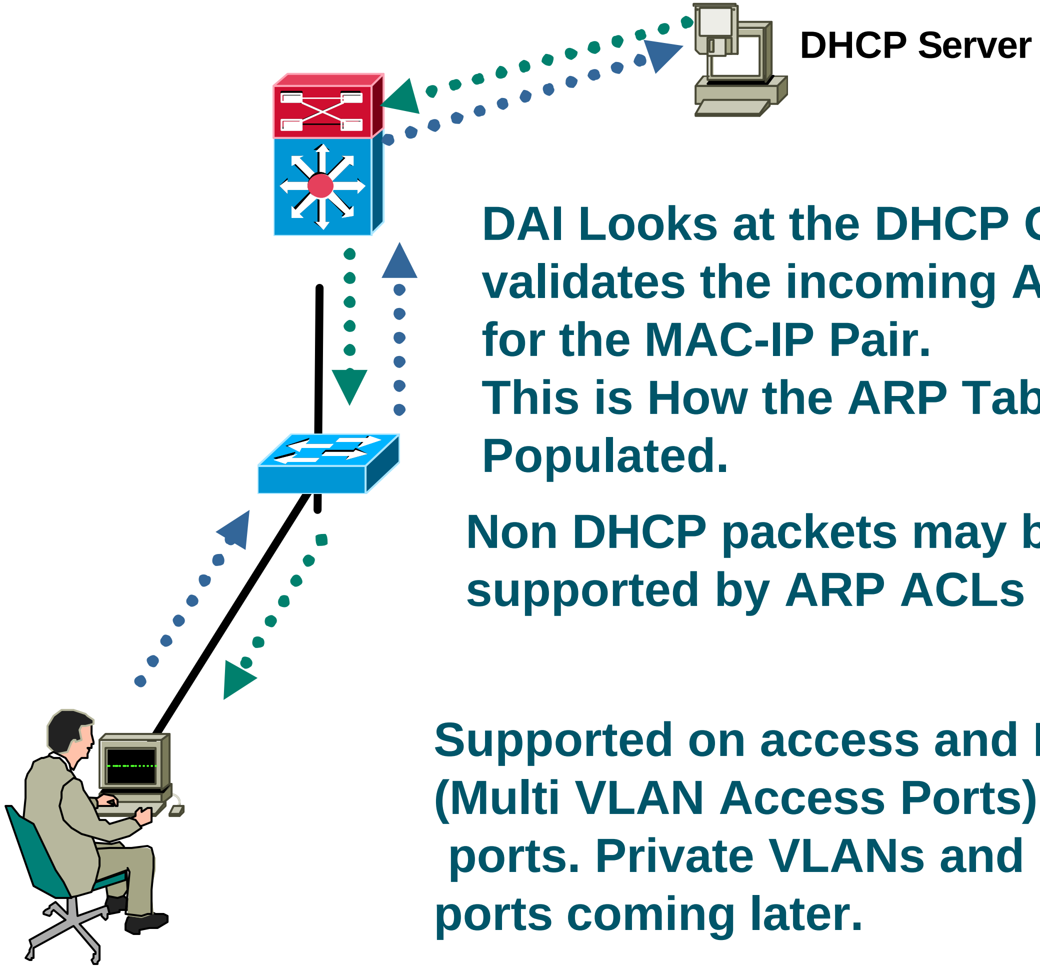


DAI Keeps Track of the DHCP Discovery

DHCP Discovery Broadcast

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

Dynamic ARP Inspection



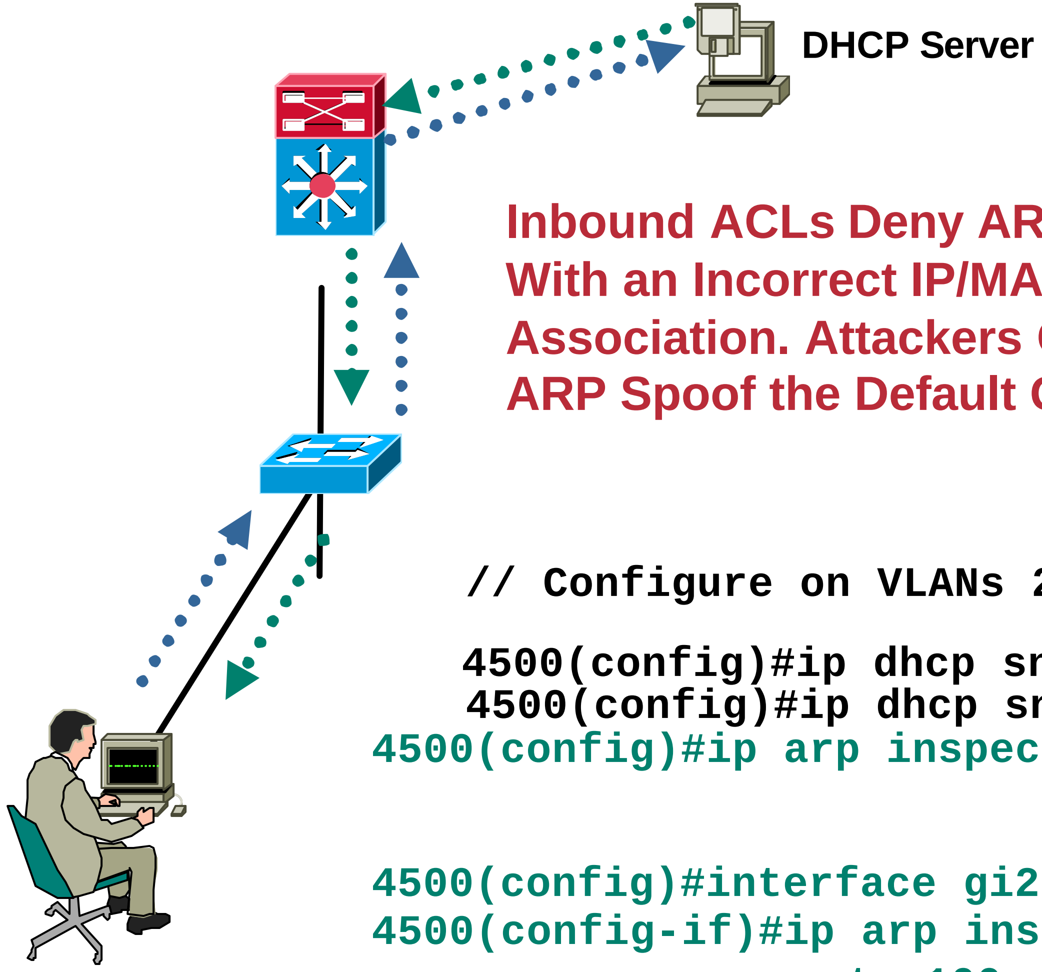
DAI Looks at the DHCP Offer, and validates the incoming ARP Entry for the MAC-IP Pair.
This is How the ARP Table Is Populated.

Non DHCP packets may be supported by ARP ACLs

Supported on access and MVAP (Multi VLAN Access Ports)
ports. Private VLANs and routed ports coming later.

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

Dynamic ARP Inspection



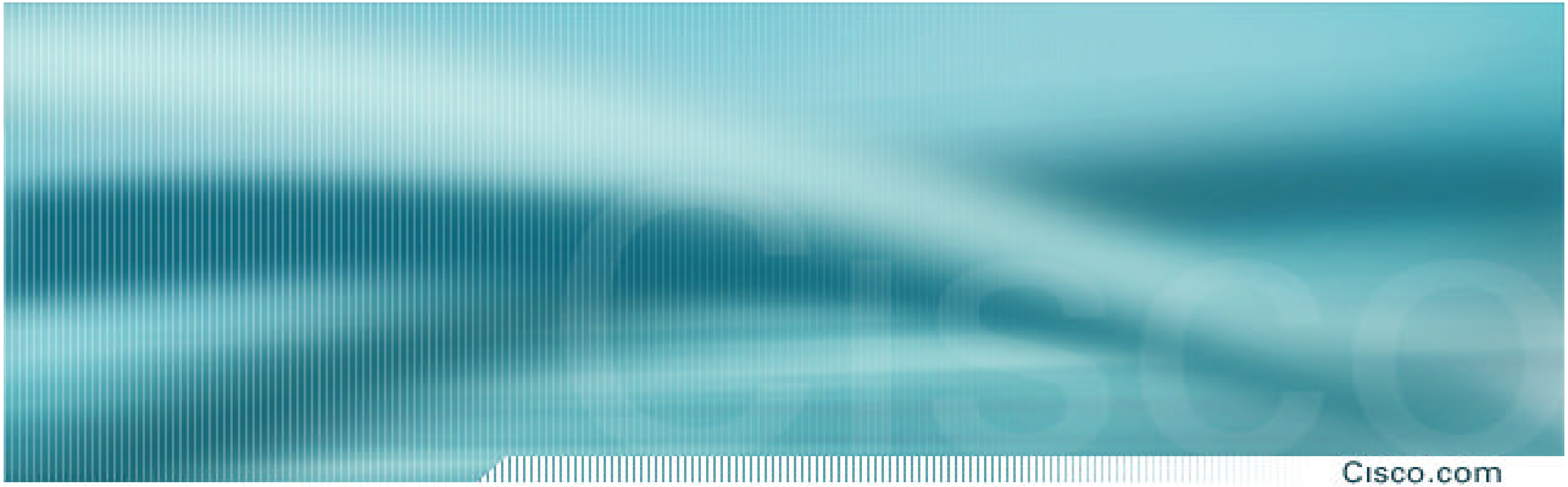
Inbound ACLs Deny ARP Packets With an Incorrect IP/MAC Association. Attackers Cannot ARP Spoof the Default Gateway.

```
    // Configure on VLANs 2 to 10

    4500(config)#ip dhcp snooping
    4500(config)#ip dhcp snoop vlan 2-10
4500(config)#ip arp inspection vlan 2-10


4500(config)#interface gi2/1
4500(config-if)#ip arp inspection limit
                 rate 100 // pps
```

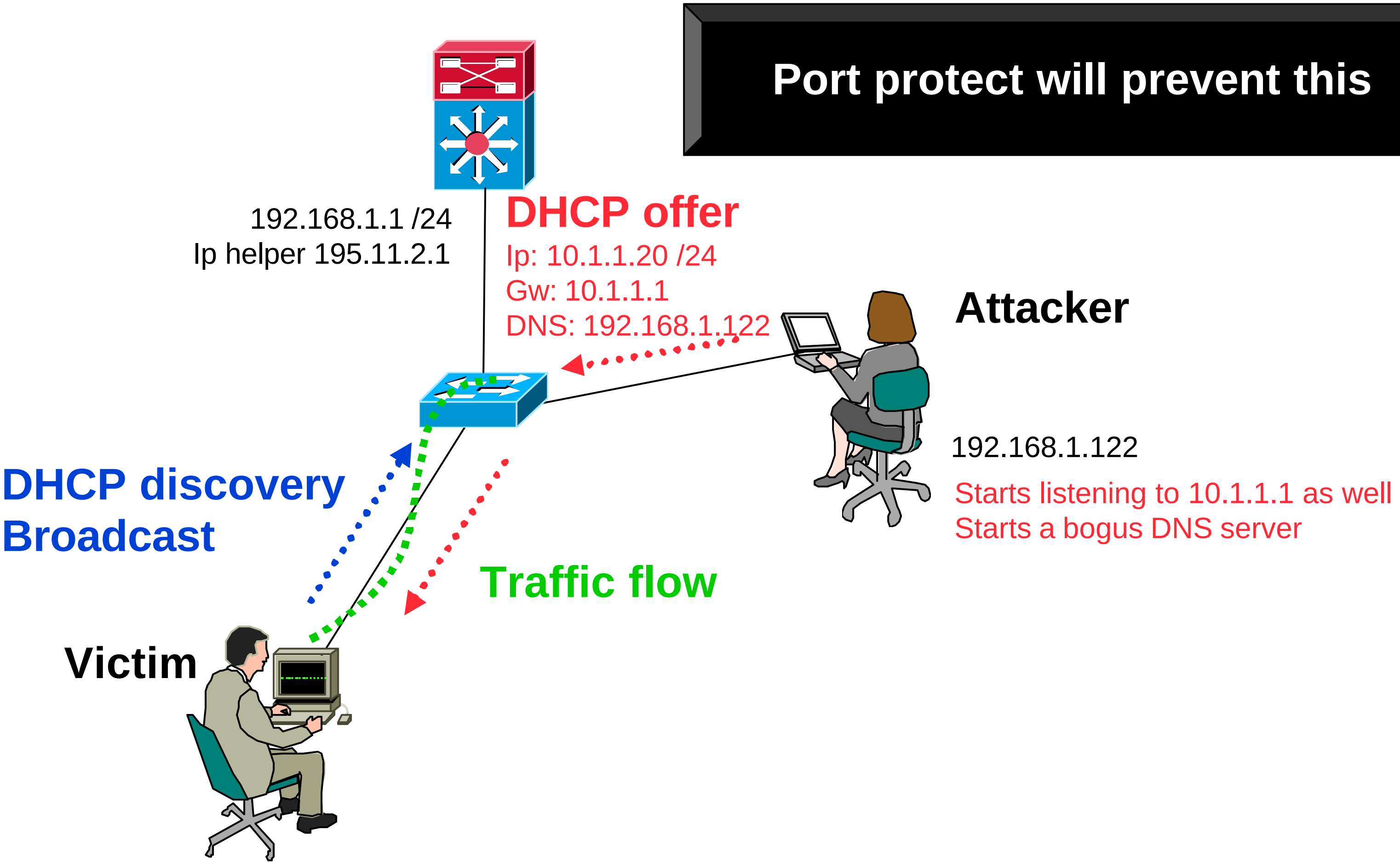
© 2003, Cisco Systems, Inc. All rights reserved.



DHCP server spoofing

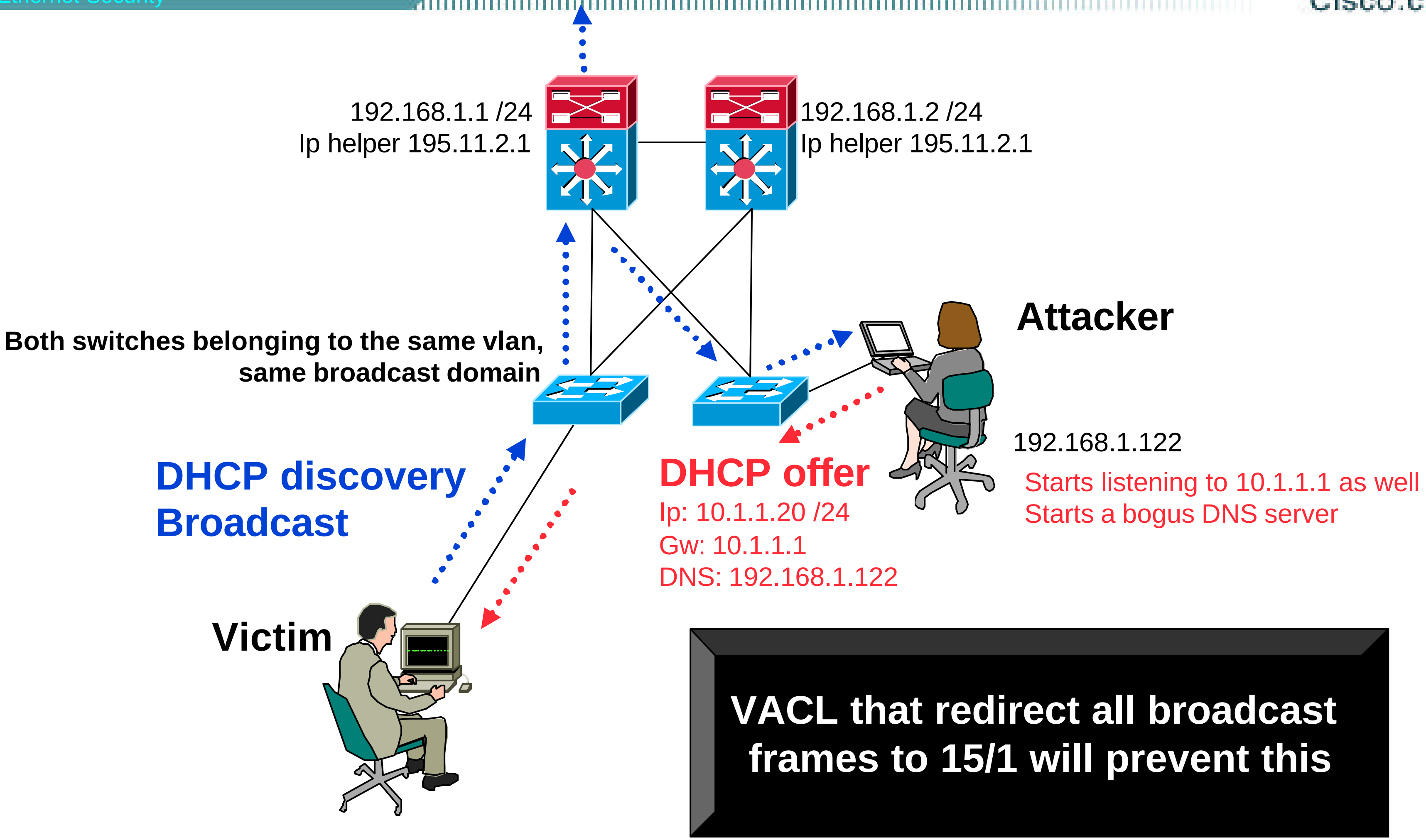
DHCP spoofing, attack 1

Port protect will prevent this



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

DHCP spoofing, attack 2



VACL that redirect all broadcast frames to 15/1 will prevent this

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

Switch Authentication

802.1X/EAP Switch Authentication

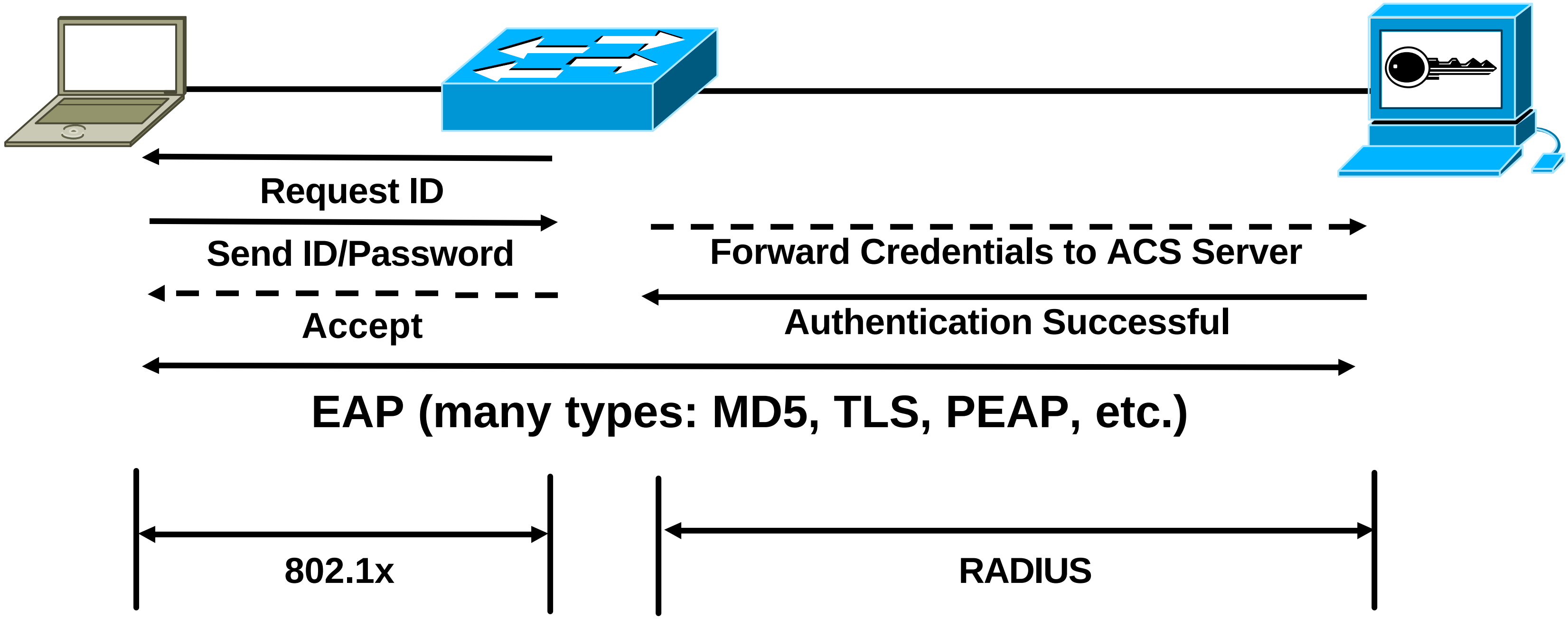
- 802.1x and EAP (Extensible Authentication Protocol) can authenticate a device before allowing access to a switch and can assign a VLAN after authentication

  EAP allows different authentication types to use the same format (TLS, MD5, OTP, PEAP)

- Works between the supplicant (client) and the authenticator (network device)
- Maintains backend communication to an authentication (RADIUS) server
- The authenticator (switch) becomes the middleman for relaying EAP received in 802.1x packets to an authentication server by using RADIUS to carry the EAP information
- Available on Cat 29XXG, 4K,6K in CatOS 6.2; Cat 3550 in 12.1(4)EA1; Cat 2950 in 12.1(6)EA2; 4K IOS in 12.1(12c)EW; 6K IOS in 12.1(13)EW

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

802.1X Port Authentication



Request ID

Send ID/Password

Accept

Forward Credentials to ACS Server

Authentication Successful

EAP (many types: MD5, TLS, PEAP, etc.)

802.1x

RADIUS

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

802.1X/EAP Deployment Considerations

- Current software stability
  - Windows 802.1X Clients have DHCP bug
    - 802.1X is independent of DHCP which sometimes results in a link-local address on the client after authentication
  - All code is new and will likely have a few issues the early adopters will find
  - Specification issues with 802.1X finite state machine: http://www.cs.umd.edu/~waa/1x.pdf
    - To be addressed in 802.1aa

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

802.1X/EAP Deployment Considerations

- Deployment/security considerations

  Understand what you are getting: 802.1X provides a MAC ACL-based on user/device credentials

    MAC spoofing is easy (insert hub, etc.)

  Many devices will not support 802.1X for some time (printers, certain OSs, etc.)

    This means switch configurations will be filled with exceptions weakening security

  Identity infrastructure (RADIUS, etc.) becomes essential to basic network operation

  Remember 802.1X only protects against unauthorized access; if an attacker is willing to breach your physical location, will 802.1X provide enough value to justify the management burden?

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

802.1X/EAP Common Uses

- **WLAN deployments**

  Provides cryptographic key distribution which allows per frame encryption

- **Wired network locations with no physical security**

  If you can’t count on physical security to prevent individuals from gaining access to your LAN ports, 802.1X adds value

- **Wired networks needing network user differentiation and mobility**

  If you have a diverse set of users with differing network access requirements, 802.1X can allow VLAN assignment to follow a user wherever the connect in the network

Security approach

Are the security threats/solutions described in this presentation applicable only in the ETTx environment

???

Summary

- 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

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

Summary

- We can today build a secure ETTx network
- It is extremely important to do the security homework before doing the overall design
- You can rely on Cisco Advanced Services to help here

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

For More Information

- **Metro ethernet, control plane concept**

  http://www.cisco.com/warp/public/cc/so/neso/meso/metes_wp.htm

- **Ethernet the first mile whitepaper**

  http://www.cisco.com/warp/public/cc/so/neso/efmsol/efm_wp.htm

Thank You!

- **Lim Wong**
  limwong@cisco.com
- **Wojciech Dec**
  wdec@cisco.com

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

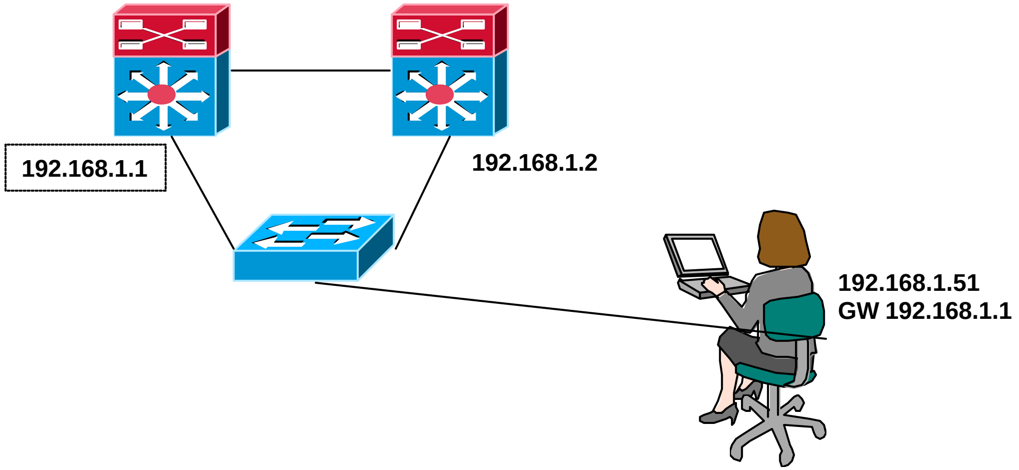
CISCO SYSTEMS®

EMPOWERING THE
INTERNET GENERATION^{SM}

© 2001, Cisco Systems, Inc. All rights reserved.

VRRP security

- VRRP is the standardised solution for redundant gateways
- RFC 2338



VRRP security

- Hellos sent to 224.0.0.18, ttl 255
- IP protocol 112 is assigned by IANA
- The priority value for the VRRP router that owns the IP address(es) associated with the virtual router MUST be 255 (decimal)

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

VRRP security

- The protocol should ensure after Master election that no state transition is triggered by any Backup router of equal or lower preference as long as the Master continues to function properly
- Exception is that the router that owns the IP address(es) associated with the virtual router always pre-empts independent of the setting of this flag.

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

VRRP security

The VRRP specification makes it much harder to launch an hijacking attack