

Exploiting First Hop Protocols to Own the Network

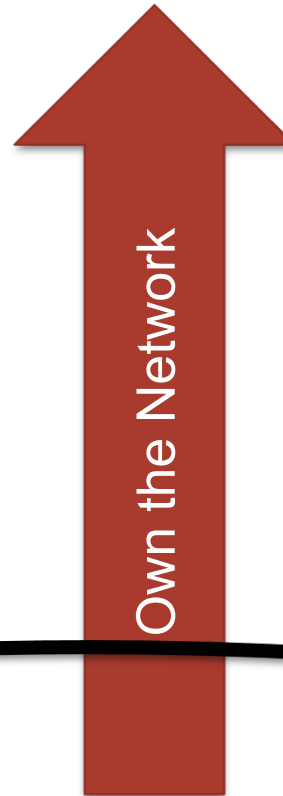
Bsides Vienna 2016

**Paul Coggin
@PaulCoggin**

OSI and TCP/IP Model

OSI Model

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical



TCP/IP Model

Application
Transport
Internet
Network Interface

Cisco Discovery Protocol (CDP)

```
pc — R4 — telnet 172.16.111.128 5003 — 85x38
R4#sho cdp neigh detail
-----
Device ID: R2
Entry address(es):
  IP address: 10.1.1.14
Platform: Cisco 7206VXR, Capabilities: Router
Interface: GigabitEthernet1/0, Port ID (outgoing port): GigabitEthernet1/0
Holdtime : 122 sec

Version :
Cisco IOS Software, 7200 Software (C7200-ADVIPSERVICESK9-M), Version 12.4(20)T, RELEA
SE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 11-Jul-08 04:22 by prod_rel_team

advertisement version: 2
Duplex: full

-----
Device ID: R5
Entry address(es):
  IP address: 10.1.1.6
Platform: Cisco 7206VXR, Capabilities: Router
Interface: GigabitEthernet4/0, Port ID (outgoing port): GigabitEthernet4/0
Holdtime : 144 sec

Version :
Cisco IOS Software, 7200 Software (C7200-ADVIPSERVICESK9-M), Version 12.4(20)T, RELEA
SE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 11-Jul-08 04:22 by prod_rel_team

advertisement version: 2
Duplex: full

R4#
```

Cisco Discovery Protocol (CDP)

- Great tool for mapping out a network during an audit
- Be sure to disable on connections to external networks such as WAN, MetroE
- VoIP phones use CDP (how to secure info leakage on VoIP net??)

Cisco Discovery Protocol (CDP) – Great for Recon!

Standard input — R5 GigabitEthernet4/0 to R4 GigabitEthernet4/0

Apply a display filter ... <⌘/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
7	6.581011	ca:04:0b:82:00:70	ca:04:0b:82:00:70	LOOP	60	Reply
8	7.184641	ca:05:0b:91:00:70	CDP/VTP/DTP/PAGP/U...	CDP	352	Device ID: R5 Port ID: GigabitEthernet4/0
9	8.233554	10.1.1.6	224.0.0.2	LDP	76	Hello Message
10	8.999110	10.1.1.5	224.0.0.5	OSPF	134	Hello Packet
11	10.499830	10.10.10.1	10.10.10.3	LDP	72	Keep Alive Message
12	10.711074	10.10.10.3	10.10.10.1	TCP	60	43375 → 646 [ACK] Seq=1 Ack=19 Win=3804 Len=0
13	10.892211	10.1.1.5	224.0.0.2	LDP	76	Hello Message
14	11.000660	10.1.1.6	224.0.0.5	OSPF	134	Hello Packet

▼ Cisco Discovery Protocol

- Version: 2
- TTL: 180 seconds
- ▶ Checksum: 0xa122 [correct]
- ▶ Device ID: R5
- ▼ Software Version
 - Type: Software version (0x0005)
 - Length: 251
 - Software version: Cisco IOS Software, 7200 Software (C7200-ADVIPSERVICESK9-M), Version 12.4(20)T, RELEASE SOFTWARE (fc3)
 - Software version: Technical Support: <http://www.cisco.com/techsupport>
 - Software version: Copyright (c) 1986-2008 by Cisco Systems, Inc.
 - Software version: Compiled Fri 11-Jul-08 04:22 by prod_rel_team
- ▼ Platform: Cisco 7206VXR
 - Type: Platform (0x0006)
 - Length: 17
 - Platform: Cisco 7206VXR
- ▼ Addresses
 - Type: Addresses (0x0002)
 - Length: 17
 - Number of addresses: 1
 - ▶ IP address: 10.1.1.6
- ▶ Port ID: GigabitEthernet4/0
- ▼ Capabilities
 - Type: Capabilities (0x0004)
 - Length: 8
 - Capabilities: 0x00000001

```
0120 69 73 63 6f 20 37 32 30 36 56 58 52 00 02 00 11 Cisco 720 6VXR....
0130 00 00 00 01 01 01 cc 00 04 0a 01 01 06 00 03 00 .....
0140 16 47 69 67 61 62 69 74 45 74 68 65 72 6e 65 74 .Gigabit Ethernet
0150 34 2f 30 00 04 00 08 00 00 00 01 00 0b 00 05 01 4/0....
```

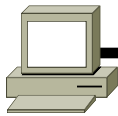
Length (cdp.tlv.len), 2 bytes

Packets: 1102 · Displayed: 1102 (100.0%)

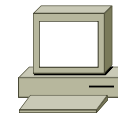
Profile: Default

Multicast Overview

Multicast Source 1



Multicast Source 2



- Routers send periodic queries
- Host per VLAN per group reports
- Host may send leave messages
- IPv4 – IGMP
- IPv6 – MLD

- Multicast uses UDP
- One-way traffic stream
- “Fire and Forget”
- Video
- Many other apps
- Multicast Routing PIM
- Reverse Path Forwarding(RPF)

Multicast PIM routing

IGMP Report to Join
Multicast Group
Member 1

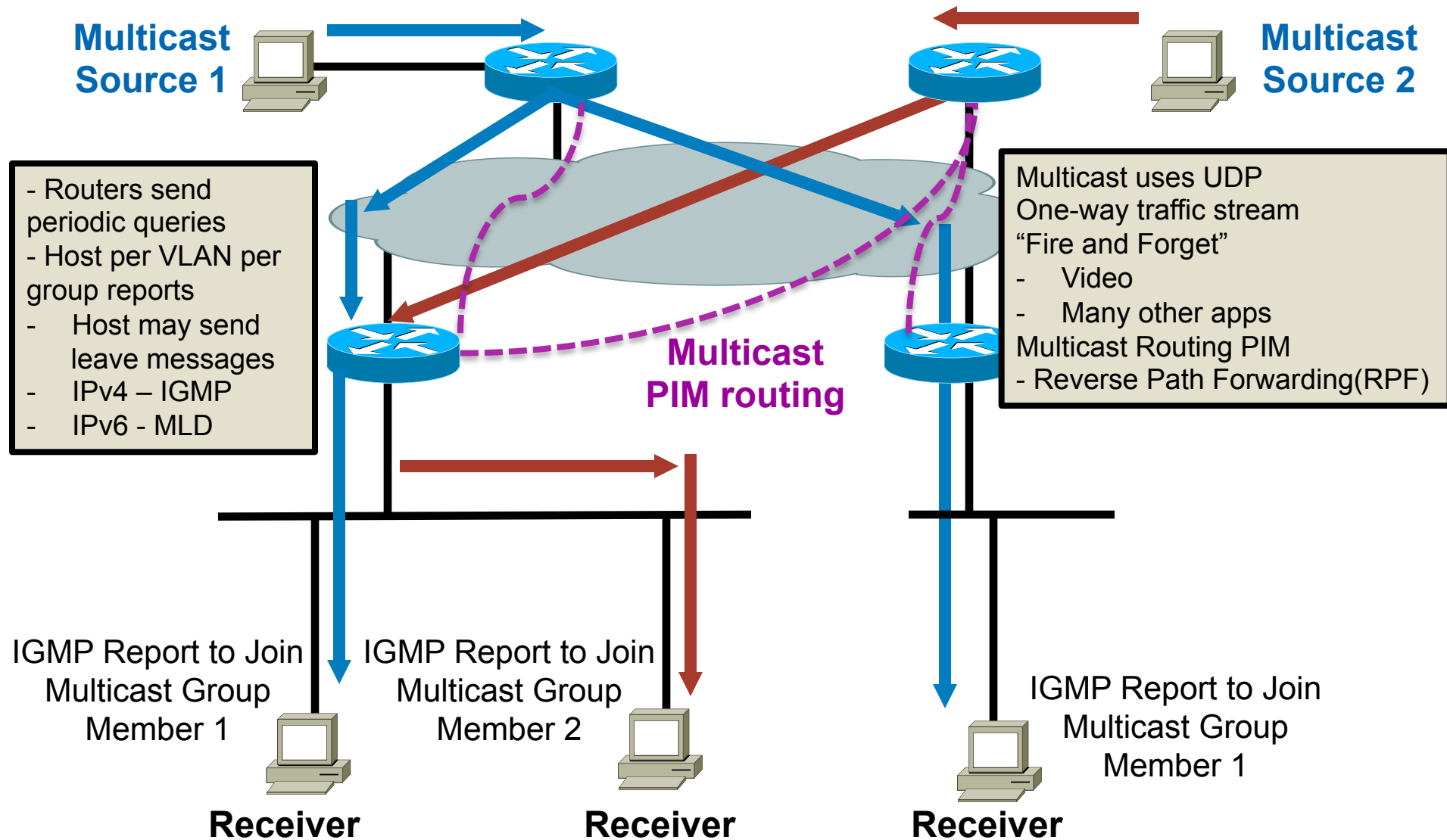
Receiver

IGMP Report to Join
Multicast Group
Member 2

Receiver

IGMP Report to Join
Multicast Group
Member 1

Receiver



Multicast - IGMP

Standard input — R2 GigabitEthernet3/0 to R5 GigabitEthernet3/0

igmp

No.	Time	Source	Destination	Protocol	Length	Info
81	52.378644	10.1.1.21	224.0.0.1	IGMPv2	60	Membership Query, general
86	54.381700	10.1.1.21	224.0.1.40	IGMPv2	60	Membership Report group 224.0.1.40
176	112.440831	10.1.1.21	224.0.0.1	IGMPv2	60	Membership Query, general
179	113.839608	10.1.1.22	224.0.1.40	IGMPv2	60	Membership Report group 224.0.1.40
271	172.460628	10.1.1.21	224.0.0.1	IGMPv2	60	Membership Query, general
280	176.901795	10.1.1.22	224.0.1.40	IGMPv2	60	Membership Report group 224.0.1.40
369	232.518846	10.1.1.21	224.0.0.1	IGMPv2	60	Membership Query, general
382	241.513806	10.1.1.21	224.0.1.40	IGMPv2	60	Membership Report group 224.0.1.40

▶ Frame 280: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

▶ Ethernet II, Src: ca:02:0b:64:00:54 (ca:02:0b:64:00:54), Dst: IPv4mcast_01:28 (01:00:5e:00:01:28)

▶ Internet Protocol Version 4, Src: 10.1.1.22, Dst: 224.0.1.40

▶ Internet Group Management Protocol

```
0000  01 00 5e 00 01 28 ca 02 0b 64 00 54 08 00 45 c0  ..^..(..d.T..E.
0010  00 1c e8 60 00 00 01 02 e4 80 0a 01 01 16 e0 00  ... ..
0020  01 28 16 00 08 d7 e0 00 01 28 00 00 00 00 00 00  .(.....(.....
0030  00 00 00 00 00 00 00 00 00 00 00 00  .....
```

Internet Group Management Protocol: Protocol

Packets: 457 · Displayed: 8 (1.8%) · Dropped: 0 (0.0%) Profile: Default

Multicast Routing - PIM

Standard input — R5 GigabitEthernet4/0 to R4 GigabitEthernet4/0

pim

No.	Time	Source	Destination	Protocol	Length	Info
25	15.887611	10.1.1.6	224.0.0.2	PIMv1	60	Query
26	15.952795	10.1.1.5	224.0.0.2	PIMv1	60	Query
70	45.114553	10.1.1.5	224.0.0.2	PIMv1	60	Query
73	45.584501	10.1.1.6	224.0.0.2	PIMv1	60	Query
117	74.654680	10.1.1.5	224.0.0.2	PIMv1	60	Query
119	75.390328	10.1.1.6	224.0.0.2	PIMv1	60	Query
163	104.454047	10.1.1.5	224.0.0.2	PIMv1	60	Query
165	105.078446	10.1.1.6	224.0.0.2	PIMv1	60	Query
211	134.303849	10.1.1.5	224.0.0.2	PIMv1	60	Query
212	134.926336	10.1.1.6	224.0.0.2	PIMv1	60	Query
258	163.654909	10.1.1.5	224.0.0.2	PIMv1	60	Query
260	164.834185	10.1.1.6	224.0.0.2	PIMv1	60	Query

► Frame 163: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

► Ethernet II, Src: ca:04:0b:82:00:70 (ca:04:0b:82:00:70), Dst: IPv4mcast_02 (01:00:5e:00:00:02)

► Internet Protocol Version 4, Src: 10.1.1.5, Dst: 224.0.0.2

▼ Protocol Independent Multicast

Type: PIM (0x14)

Code: Query (0)

Checksum: 0xbba5 [correct]

0001 = Version: 1

Reserved byte(s): 000000

► PIM Options

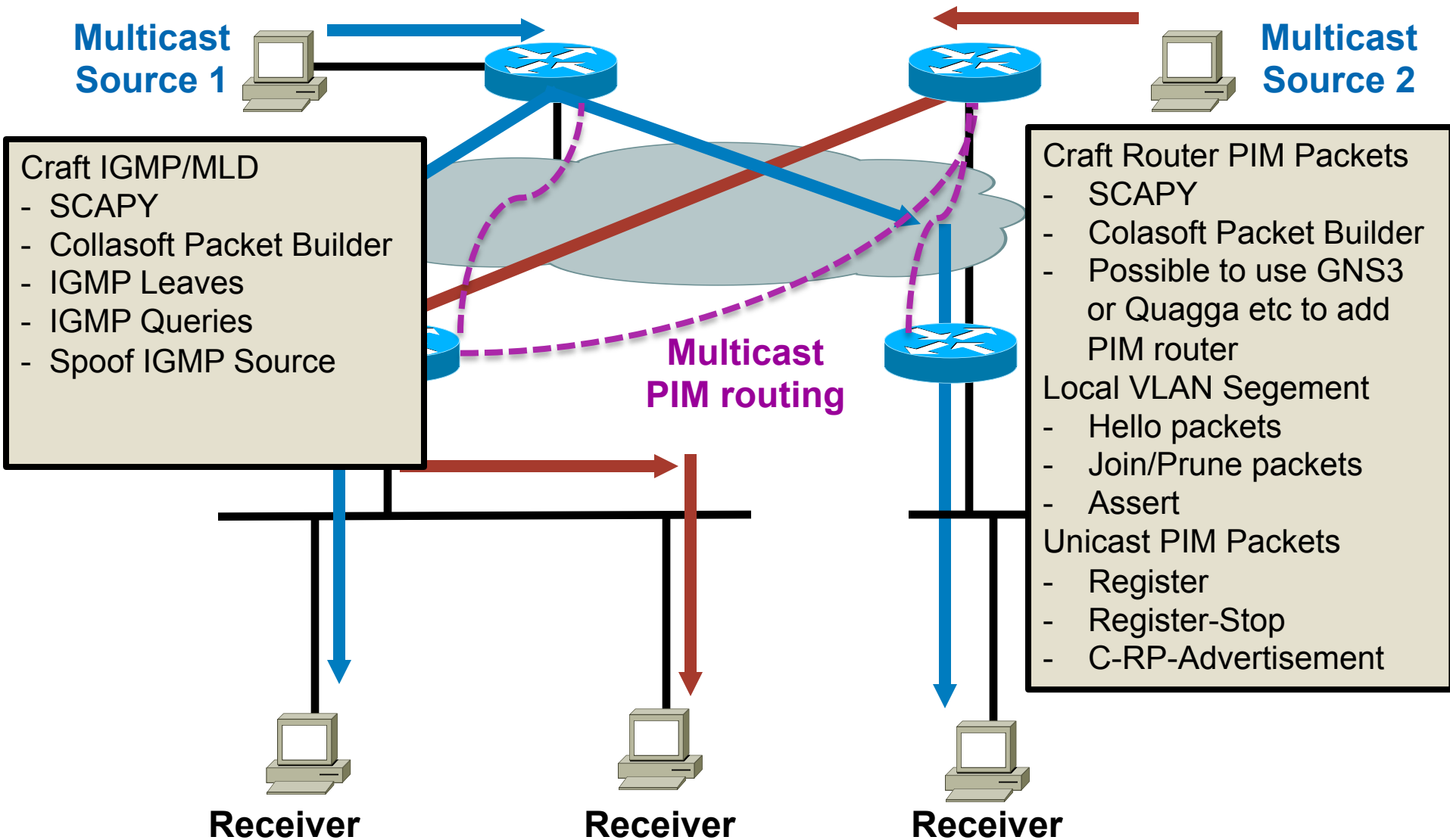
```
0000  01 00 5e 00 00 02 ca 04 0b 82 00 70 08 00 45 c0  ..^.....p..E.
0010  00 20 17 59 00 00 01 02 b6 bb 0a 01 01 05 e0 00  .Y.....
0020  00 02 14 00 bb a5 10 00 00 00 20 00 00 5a 00 00  .....Z..
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

wireshark_pcapng_-_20160910134831_WBVQ42

Packets: 277 · Displayed: 12 (4.3%)

Profile: Default

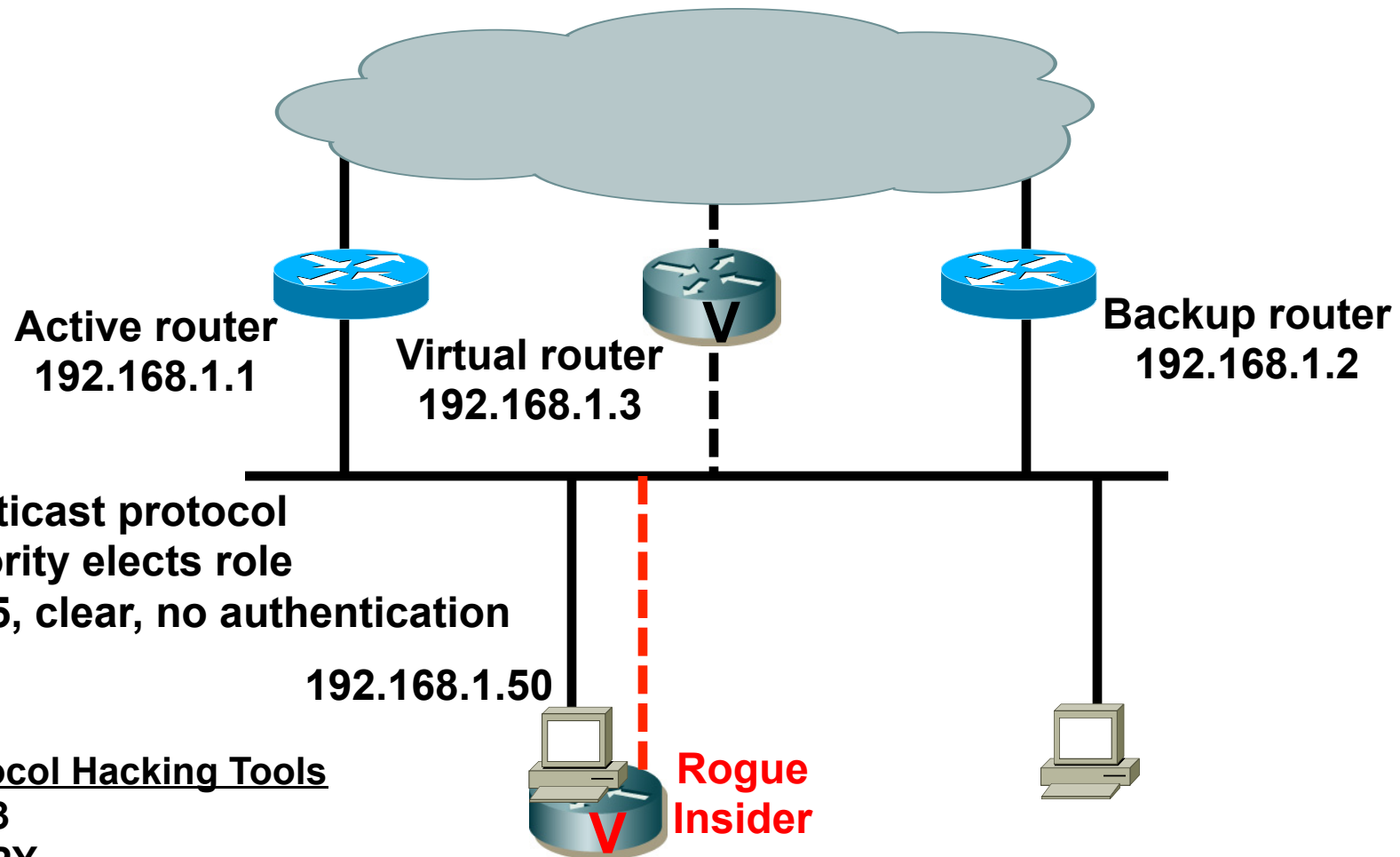
Attacking Multicast



Securing Multicast



First Hop Redundancy Protocols



Protocol Hacking Tools

GNS3

SCAPY

Colasoft Packet Builder

Many others...

(Remember to enable IP forwarding)

Global Load Balancing Protocol (GLBP)

Hot Standby Router Protocol (HSRP)

Virtual Redundant Router Protocol (VRRP)

VRRP – No Authentication

Capturing from Standard input — R6 GigabitEthernet1/0 to HUB1 1

Apply a display filter ... <36/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
2	0.949844	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
3	1.927089	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
4	2.807202	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
5	3.760299	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
6	4.558359	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
7	5.436067	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
8	6.177700	ca:07:0e:78:00:1c	ca:07:0e:78:00:1c	LOOP	60	Reply
9	6.291427	ca:06:0e:69:00:1c	ca:06:0e:69:00:1c	LOOP	60	Reply
10	6.361873	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
11	7.308281	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
12	8.255089	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)

▶ Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

▶ Ethernet II, Src: IETF-VRRP-VRID_01 (00:00:5e:00:01:01), Dst: IPv4mcast_12 (01:00:5e:00:00:12)

▶ Internet Protocol Version 4, Src: 172.16.1.2, Dst: 224.0.0.18

▼ Virtual Router Redundancy Protocol

- ▶ Version 2, Packet type 1 (Advertisement)
 - Virtual Rtr ID: 1
 - Priority: 110 (Non-default backup priority)
 - Addr Count: 1
 - Auth Type: No Authentication (0)**
 - Adver Int: 1
 - Checksum: 0xc3ea [correct]
 - IP Address: 172.16.1.1

VRRP – No Authentication

```
0000 01 00 5e 00 00 12 00 00 5e 00 01 01 08 00 45 c0 ..^....^.....E.
0010 00 28 00 00 00 00 ff 70 2d 81 ac 10 01 02 e0 00 .(.....p-.....
0020 00 12 21 01 6e 01 00 01 c3 ea ac 10 01 01 00 00 ..!.n... ..
0030 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Ready to load or capture Packets: 147 · Displayed: 147 (100.0%) Profile: Default

VRRP – Clear Text Authentication

Standard input — R6 GigabitEthernet1/0 to HUB1 1

Apply a display filter ... <=>/>

No.	Time	Source	Destination	Protocol	Length	Info
301	135.952783	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
302	136.396425	ca:06:0e:69:00:1c	CDP/VTP/DTP/PAgP/U...	CDP	352	Device ID: R6 Port ID: GigabitEthernet1/
303	136.960936	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
304	137.847721	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
305	138.754130	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
306	139.691897	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
307	140.559586	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
308	140.588224	ca:07:0e:78:00:1c	ca:07:0e:78:00:1c	LOOP	60	Reply
309	140.700568	ca:06:0e:69:00:1c	ca:06:0e:69:00:1c	LOOP	60	Reply
310	141.456908	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
311	142.454977	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)
312	143.323325	172.16.1.2	224.0.0.18	VRRP	60	Announcement (v2)

▶ Frame 310: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

▶ Ethernet II, Src: IETF-VRRP-VRID_01 (00:00:5e:00:01:01), Dst: IPv4mcast_12 (01:00:5e:00:00:12)

▶ Internet Protocol Version 4, Src: 172.16.1.2, Dst: 224.0.0.18

▼ Virtual Router Redundancy Protocol

- ▶ Version 2, Packet type 1 (Advertisement)
 - Virtual Rtr ID: 1
 - Priority: 110 (Non-default backup priority)
 - Addr Count: 1
 - Auth Type: Simple Text Authentication [RFC 2338] / Reserved [RFC 3768] (1)
 - Adver Int: 1
 - Checksum: 0x6eae [correct]
 - IP Address: 172.16.1.1
 - Authentication String: vendor

VRRP – Clear Text Authentication

```
0000 01 00 5e 00 00 12 00 00 5e 00 01 01 08 00 45 c0 ..^.....^.....E.
0010 00 28 00 00 00 00 ff 70 2d 81 ac 10 01 02 00 00 ..(.....p.....
0020 00 12 21 01 6e 01 01 01 6e ae ac 10 01 01 76 65 ..!.n...n.....ve
0030 6e 64 6f 72 00 00 00 00 00 00 00 00 00 00 00 ndor....
```

Authentication String (vrrp.auth_string), 8 bytes

Packets: 312 · Displayed: 312 (100.0%)

Profile: Default

HSRP MITM – Packet Analysis

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply Zoom 100%

No.	Time	Source	Destination	Protocol	Info
14	9.881602	192.168.1.2	224.0.0.2	HSRP	Hello (state Active)
15	11.277736	Cisco_75:98:0c	Spanning-tree-(for	STP	Conf. Root = 32768/00:08:20:75:98:01 Cost = 0 Port = 0x8003
16	12.002259	192.168.1.1	224.0.0.2	HSRP	Hello (state Speak)
17	12.653671	192.168.1.2	224.0.0.2	HSRP	Hello (state Active)
18	13.277927	Cisco_75:98:0c	Spanning-tree-(for	STP	Conf. Root = 32768/00:08:20:75:98:01 Cost = 0 Port = 0x8003
19	14.008331	192.168.1.1	224.0.0.5	OSPF	Hello Packet
20	15.002314	192.168.1.1	224.0.0.2	HSRP	Hello (state Speak)
21	15.278126	Cisco_75:98:0c	Spanning-tree-(for	STP	Conf. Root = 32768/00:08:20:75:98:01 Cost = 0 Port = 0x8003
22	15.281765	192.168.1.2	224.0.0.2	HSRP	Hello (state Active)
23	16.587591	Cisco_4a:37:10	DEC-MOP-Remote-Con	0x6002	DEC DNA Remote Console
24	17.278310	Cisco_75:98:0c	Spanning-tree-(for	STP	Conf. Root = 32768/00:08:20:75:98:01 Cost = 0 Port = 0x8003
25	18.002502	192.168.1.1	224.0.0.2	HSRP	Hello (state Speak)
26	18.181848	192.168.1.2	224.0.0.2	HSRP	Hello (state Active)
27	19.278498	Cisco_75:98:0c	Spanning-tree-(for	STP	Conf. Root = 32768/00:08:20:75:98:01 Cost = 0 Port = 0x8003
28	19.441297	192.168.1.15	192.168.1.255	BROWSE	Domain/workgroup Announcement DYNETICS, NT Workstation, Domain Enum
29	20.999888	192.168.1.1	224.0.0.2	HSRP	Hello (state Speak)
30	21.025869	192.168.1.2	224.0.0.2	HSRP	Hello (state Active)
31	21.278688	Cisco_75:98:0c	Spanning-tree-(for	STP	Conf. Root = 32768/00:08:20:75:98:01 Cost = 0 Port = 0x8003
32	23.278889	Cisco_75:98:0c	Spanning-tree-(for	STP	Conf. Root = 32768/00:08:20:75:98:01 Cost = 0 Port = 0x8003

Frame 10 (62 bytes on wire, 62 bytes captured)

Ethernet II, Src: All-HSRP-routers_01 (00:00:0c:07:ac:01), Dst: 01:00:5e:00:00:02 (01:00:5e:00:00:02)

Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 224.0.0.2 (224.0.0.2)

User Datagram Protocol, Src Port: 1985 (1985), Dst Port: 1985 (1985)

Cisco Hot Standby Router Protocol

Version: 0

Op Code: Hello (0)

State: Active (16)

Hello time: Default (3)

Hold time: Non-Default (255)

Priority: 110

Group: 1

Reserved: 0

Authentication Data: Default (cisco)

Virtual IP Address: 192.168.1.3 (192.168.1.3)

HSRP Password Clear Text

0000 01 00 5e 00 00 02 00 00 0c 07 ac 01 08 00 45 c0 ..A.....E

0010 00 30 00 00 00 00 02 11 16 51 c0 a8 01 02 e0 00 ..0.....Q.....

0020 00 02 07 c1 07 c1 00 1c 36 9c 00 00 10 03 ff 6en

0030 01 00 63 69 73 63 6f 00 00 00 c0 a8 01 03 ..cisco.

FHRP – Crafted HSRP Packets

The screenshot displays the Colasoft Packet Builder interface. The top section shows a list of packets, with packet 38 selected. The bottom section shows the detailed decode of packet 38, which is an HSRP (Hot Standby Router Protocol) packet. The decode shows the packet structure, including the Source IP, Destination IP, and the HSRP fields. The HSRP fields are expanded, showing the OpCode, State, Hello time, Hold time, Priority, Group, and Reserved fields. The Priority field is set to 255, which is circled in red. The State field is set to 16, which is also circled in red. The OpCode field is set to 1, which is circled in red. The State field is labeled as "(Currently forwarding packets)". The Priority field is labeled as "(Wishes to become the active router)".

Packet List:

No.	Delta Ti...	Source	Destination	Pro...	Size	Summary
33	0.597646	192.168.1.1:1985	224.0.0.2:1985	HSRP	66	Ver = 0 , OpCode = 0 , State = 8 , Hellotime = 3 , Holdtime = 10 , Pri = 100 , Group = 1 , IP = 192.
34	1.402544	00:08:20:75:98:0C	01:80:C2:00:00:00	STP	64	Normal Datagram from 00:08:20:75:98:0C to 01:80:C2:00:00:00
35	0.647511	192.168.1.2:1985	224.0.0.2:1985	HSRP	66	Ver = 0 , OpCode = 0 , State = 16 , Hellotime = 3 , Holdtime = 10 , Pri = 110 , Group = 1 , IP = 192.
36	0.950201	192.168.1.1:1985	224.0.0.2:1985	HSRP	66	Ver = 0 , OpCode = 0 , State = 8 , Hellotime = 3 , Holdtime = 10 , Pri = 100 , Group = 1 , IP = 192.
37	0.402473	00:08:20:75:98:0C	01:80:C2:00:00:00	STP	64	Normal Datagram from 00:08:20:75:98:0C to 01:80:C2:00:00:00
38	0.743793	192.168.1.50:1985	224.0.0.2:1985	HSRP	66	Ver = 0 , OpCode = 1 , State = 16 , Hellotime = 3 , Holdtime = 255 , Pri = 255 , Group = 1 , IP = 192.
39	0.000145	192.168.1.50:1985	224.0.0.2:1985	HSRP	66	Ver = 0 , OpCode = 0 , State = 16 , Hellotime = 3 , Holdtime = 255 , Pri = 255 , Group = 1 , IP = 192.
40	0.015335	192.168.1.2:1985	224.0.0.2:1985	HSRP	66	Ver = 0 , OpCode = 0 , State = 4 , Hellotime = 3 , Holdtime = 10 , Pri = 110 , Group = 1 , IP = 192.
41	0.006573	00:10:7B:36:43:FD	FF:FF:FF:FF:FF:FF	ARP	64	192.168.1.2 is at 00:10:7B:36:43:FD

Decode Editor (Packet No. 38):

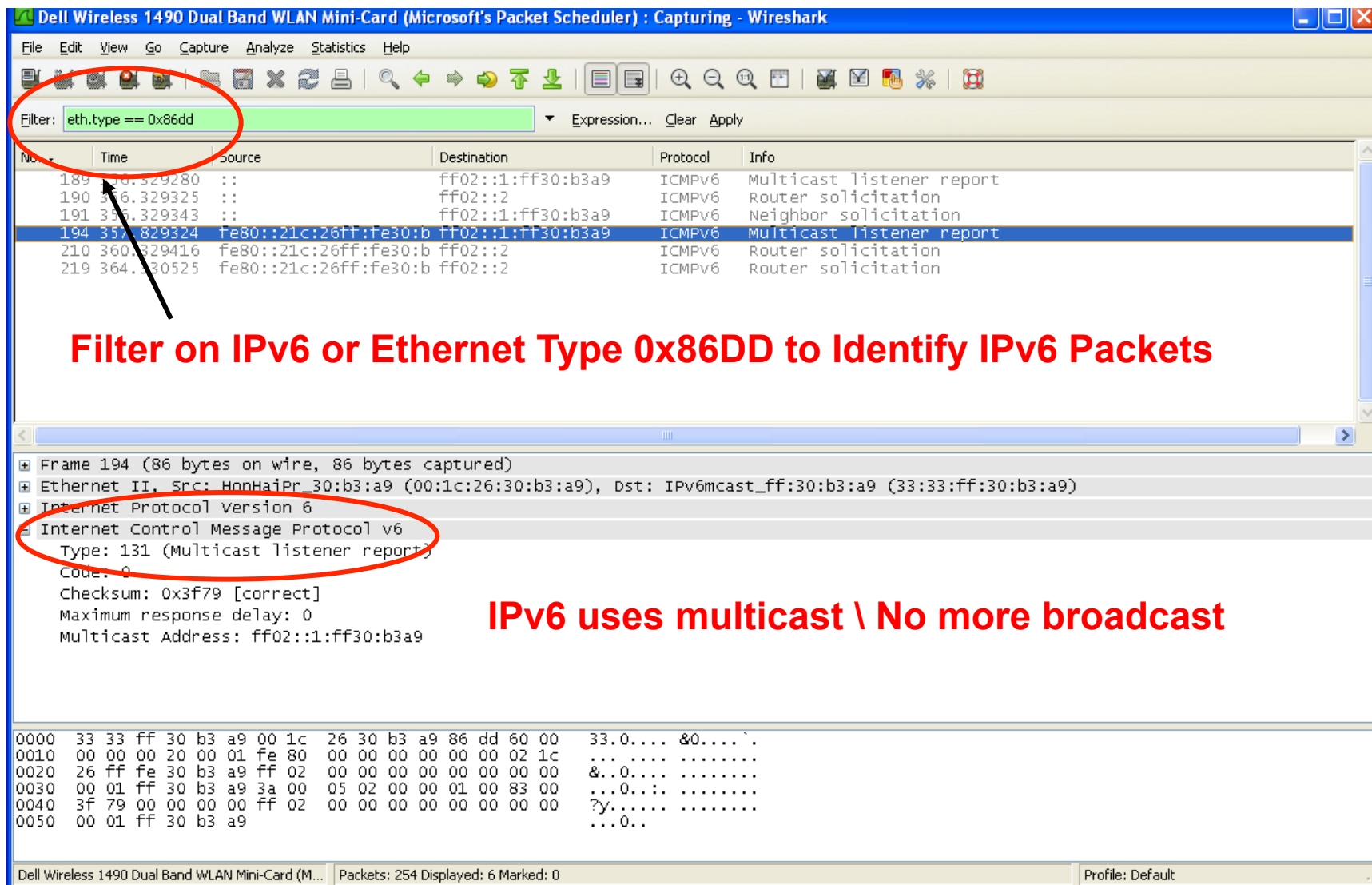
- Source IP: 192.168.1.50 [26/4]
- Destination IP: 224.0.0.2 [30/4]
- No IP Option [34/0]
- UDP - User Datagram Protocol [34/8]
 - Source port: 1985 [34/2]
 - Destination port: 1985 [36/2]
 - Length: 28 [38/2]
 - Checksum: 0x35DA (Correct) [40/2]
- HSRP - Hot Standby Router Protocol [42/20]
 - Version: 0 [42/1]
 - OpCode: 1 (Wishes to become the active router) [43/1]
 - State: 16 (Currently forwarding packets) [44/1]
 - Hello time: 3 [45/1]
 - Hold time: 255 [46/1]
 - Priority: 255 [47/1]
 - Group: 1 [48/1]
 - Reserved: 0 [49/1]
 - Authentication Data: 8 bytes [50/8]
 - Virtual IP Address: 192.168.1.3 [58/4]
- FCS - Frame Check Sequence: 0x5C2B2B20 (Calculated)

Annotations:

- Routers:** Points to the Source IP (192.168.1.50) and Destination IP (224.0.0.2).
- Rogue Insider:** Points to the Source IP (192.168.1.50).
- Crafted HSRP coup packet with higher priority:** Points to the Priority field (255) in the HSRP fields.

Hex Editor: Total 62 bytes, Selection 1 bytes.

IPv6 Neighbor Discover Protocol



Filter: `eth.type == 0x86dd`

No.	Time	Source	Destination	Protocol	Info
189	356.329280	::	ff02::1:ff30:b3a9	ICMPv6	Multicast listener report
190	356.329325	::	ff02::2	ICMPv6	Router solicitation
191	356.329343	::	ff02::1:ff30:b3a9	ICMPv6	Neighbor solicitation
194	357.829324	fe80::21c:26ff:fe30:b	ff02::1:ff30:b3a9	ICMPv6	Multicast listener report
210	360.329416	fe80::21c:26ff:fe30:b	ff02::2	ICMPv6	Router solicitation
219	364.330525	fe80::21c:26ff:fe30:b	ff02::2	ICMPv6	Router solicitation

Filter on IPv6 or Ethernet Type 0x86DD to Identify IPv6 Packets

Frame 194 (86 bytes on wire, 86 bytes captured)

- Ethernet II, Src: HonHaiPr_30:b3:a9 (00:1c:26:30:b3:a9), Dst: IPv6mcast_ff:30:b3:a9 (33:33:ff:30:b3:a9)
- Internet Protocol Version 6
- Internet Control Message Protocol v6
 - Type: 131 (Multicast listener report)
 - Code: 0
 - Checksum: 0x3f79 [correct]
 - Maximum response delay: 0
 - Multicast Address: ff02::1:ff30:b3a9

IPv6 uses multicast \ No more broadcast

```
0000  33 33 ff 30 b3 a9 00 1c 26 30 b3 a9 86 dd 60 00  33.0.... &0....`
0010  00 00 00 20 00 01 fe 80 00 00 00 00 00 02 1c    ...000000021c
0020  26 ff fe 30 b3 a9 ff 02 00 00 00 00 00 00 00 00  &..0....
0030  00 01 ff 30 b3 a9 3a 00 05 02 00 00 01 00 83 00  ?..0....
0040  3f 79 00 00 00 00 ff 02 00 00 00 00 00 00 00 00  ?y.....
0050  00 01 ff 30 b3 a9                                ...0..
```

Dell Wireless 1490 Dual Band WLAN Mini-Card (M... Packets: 254 Displayed: 6 Marked: 0 Profile: Default

IPv6 SLACC MITM

- Chiron,
- Evil FOCA
- THC Parasite6
- SCAPY
- Colasoft Packet Builder

- **RAguard**
- **802.1x**
- **Private VLANs**
- **IPv6 port security**
- **Source\Destination Guard**
- **SeND (encrypt NDP)**



IPv6 Network Discovery Spoofing - MITM

IPv6 Neighbor Discovery Protocol (NDP)
(Think ARP for IPv6)

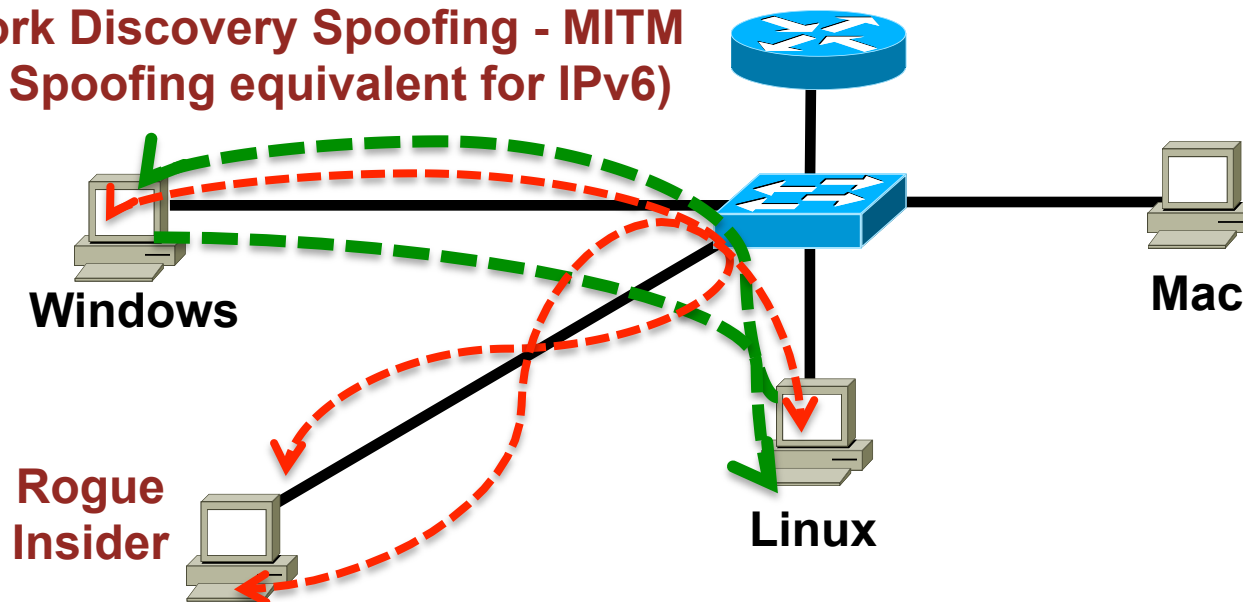
IPv6 MITM Tools

- Chiron
- Evil FOCA
- THC Parasite6
- SCAPY
- Colasoft Packet Builder

Mitigations

- Source\Destination Guard
- 802.1x
- Private VLANs
- IPv6 port security
- NDP Spoofing
- DHCP Snooping
- Source\Destination Guard
- SeND (encrypt NDP)

Network Discovery Spoofing - MITM
(ARP Spoofing equivalent for IPv6)



OSPF – No Authentication

Router PCAP.pcapng

Apply a display filter ... <=>/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
55	18.752701	192.168.1.2	192.168.2.2	TELNET	68	Telnet Data ...
56	18.752713	192.168.1.2	192.168.2.2	TELNET	68	Telnet Data ...
57	18.752716	192.168.1.2	192.168.2.2	TELNET	71	Telnet Data ...
58	18.833209	192.168.2.2	192.168.1.2	TELNET	68	Telnet Data ...
59	18.984057	192.168.1.2	192.168.2.2	TCP	68	52616 → 23 [ACK] Seq=25 Ack=67 Win=4062 L...
60	19.296134	10.1.1.6	224.0.0.5	OSPF	94	Hello Packet
61	19.940452	192.168.1.2	192.168.2.2	TELNET	68	Telnet Data ...
62	20.001079	192.168.2.2	192.168.1.2	TELNET	68	Telnet Data ...
63	20.122184	192.168.1.2	192.168.2.2	TELNET	68	Telnet Data ...

► Frame 60: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0

► Ethernet II, Src: ca:05:0b:91:00:70 (ca:05:0b:91:00:70), Dst: IPv4mcast_05 (01:00:5e:00:00:05)

► Internet Protocol Version 4, Src: 10.1.1.6, Dst: 224.0.0.5

▼ Open Shortest Path First

▼ OSPF Header

Version: 2

Message Type: Hello Packet (1)

Packet Length: 48

Source OSPF Router: 10.10.10.3

Area ID: 0.0.0.0 (Backbone)

Checksum: 0xad79 [correct]

Auth Type: Null (0)

Auth Data (none): 0000000000000000

▼ OSPF Hello Packet

Network Mask: 255.255.255.252

Hello Interval [sec]: 10

► Options: 0x12 ((L) LLS Data block, (E) External Routing)

Router Priority: 1

Router Dead Interval [sec]: 40

Designated Router: 10.1.1.6

Backup Designated Router: 10.1.1.5

Active Neighbor: 10.10.10.1

```
0000 01 00 5e 00 00 05 ca 05 0b 91 00 70 08 00 45 c0 ..^.....p..E.
0010 00 50 0d 59 00 00 01 59 c0 30 0a 01 01 06 e0 00 .P.Y...Y.0.....
0020 00 05 02 01 00 30 0a 0a 0a 03 00 00 00 00 ad 79 .....0.....y
0030 00 00 00 00 00 00 00 00 00 00 ff ff ff fc 00 0a .....
0040 12 01 00 00 00 28 0a 01 01 06 0a 01 01 05 0a 0a .....(.....
0050 0a 01 ff f6 00 03 00 01 00 04 00 00 00 01 .....

```

Router PCAP

Packets: 1579 · Displayed: 1579 (100.0%) · Load time: 0:0.24 Profile: Default

OSPF – Clear Text Authentication

Capturing from Standard input — R5 GigabitEthernet4/0 to R4 GigabitEthernet4/0

Apply a display filter ... <#>/>

No.	Time	Source	Destination	Protocol	Length	Info
9	7.360951	10.1.1.6	224.0.0.5	OSPF	94	Hello Packet
10	7.763386	10.1.1.6	224.0.0.2	LDP	76	Hello Message
11	8.367859	10.1.1.5	224.0.0.2	LDP	76	Hello Message
12	9.647466	10.1.1.5	224.0.0.5	OSPF	94	Hello Packet
13	11.471831	ca:05:0b:91:00:70	ca:05:0b:91:00:70	LOOP	60	Reply
14	11.763747	ca:04:0b:82:00:70	ca:04:0b:82:00:70	LOOP	60	Reply
15	12.076072	10.1.1.6	224.0.0.2	LDP	76	Hello Message

▶ Frame 12: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0

▶ Ethernet II, Src: ca:04:0b:82:00:70 (ca:04:0b:82:00:70), Dst: IPv4mcast_05 (01:00:5e:00:00:05)

▶ Internet Protocol Version 4, Src: 10.1.1.5, Dst: 224.0.0.5

▼ Open Shortest Path First

- ▼ OSPF Header
 - Version: 2
 - Message Type: Hello Packet (1)
 - Packet Length: 48
 - Source OSPF Router: 10.10.10.1
 - Area ID: 0.0.0.0 (Backbone)
 - Checksum: 0xad78 [correct]
 - Auth Type: Simple password (1)
 - Auth Data (Simple): cisco
- ▶ OSPF Hello Packet
- ▶ OSPF LLS Data Block

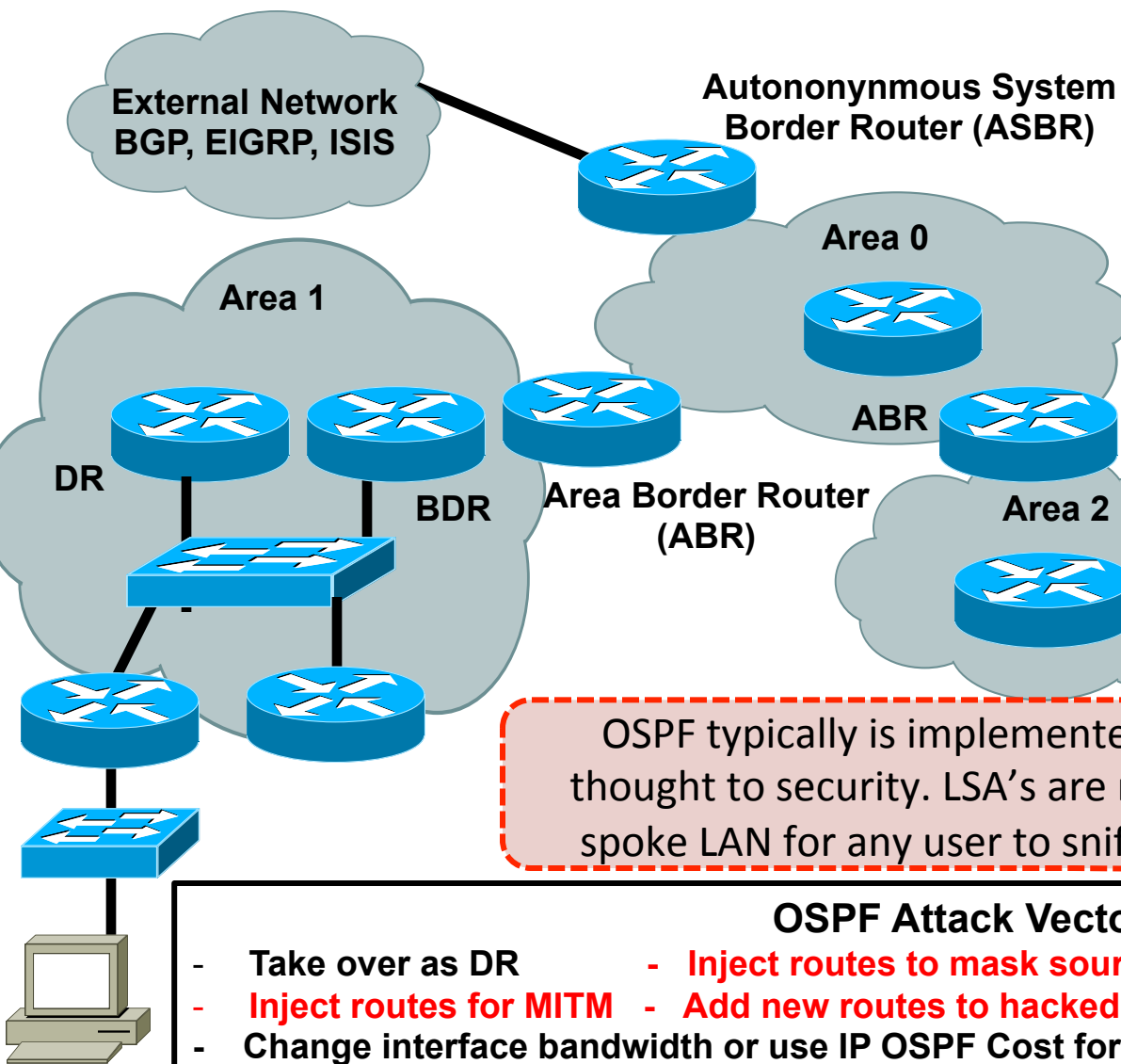
```
0000 01 00 5e 00 00 05 ca 04 0b 82 00 70 08 00 45 c0 ..^.....p..E.
0010 00 50 4a 59 00 00 01 59 83 31 0a 01 01 05 e0 00 .PJY...Y.1.....
0020 00 05 02 01 00 30 0a 0a 0a 01 00 00 00 00 ad 78 .....0.. .....x
0030 00 01 63 69 73 63 6f 00 00 00 ff ff fc 00 0a ..cisco. ....
0040 12 01 00 00 00 28 0a 01 01 06 0a 01 01 05 0a 0a .....(.. .....
0050 0a 03 ff f6 00 03 00 01 00 04 00 00 00 01 ..... .....
```

Ready to load or capture

Packets: 84 · Displayed: 84 (100.0%)

Profile: Default

Hack the Network via OSPF



OSPF Exploit Tools

- Quagga
- NRL Core(Network Simulator)
- Nemesis
- Loki
- GSN3\Dynamips
- Buy a router on eBay
- Hack a router and reconfigure
- Code one with Scapy
- IP Sorcery(IP Magic)
- Cain & Able to crack OSPF MD5
- MS RRAS
- NetDude
- Collasoft
- Phenoelit IRPAS

OSPF typically is implemented without any thought to security. LSA's are multicast on the spoke LAN for any user to sniff without MD5.

OSPF Attack Vectors

- Take over as DR
- Inject routes to mask source of attack
- DoS
- Inject routes for MITM
- Add new routes to hacked router
- Change interface bandwidth or use IP OSPF Cost for Traffic Engineering on hacked router

EIGRP – No Authentication

Capturing from Standard input — R5 GigabitEthernet4/0 to R4 GigabitEthernet4/0

Apply a display filter ... <#>/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.1.5	224.0.0.5	OSPF	134	Hello Packet
2	0.211393	10.1.1.6	224.0.0.5	OSPF	134	Hello Packet
3	0.412977	ca:05:0b:91:00:70	ca:05:0b:91:00:70	LOOP	60	Reply
4	1.018420	10.1.1.5	224.0.0.10	EIGRP	74	Hello
5	1.119108	10.1.1.6	224.0.0.2	LDP	76	Hello Message
6	1.331238	10.1.1.5	224.0.0.2	LDP	76	Hello Message
7	1.492291	10.1.1.6	224.0.0.10	EIGRP	74	Hello

Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: ca:04:0b:82:00:70 (ca:04:0b:82:00:70), Dst: IPv4mcast_0a (01:00:5e:00:00:0a)

Internet Protocol Version 4, Src: 10.1.1.5, Dst: 224.0.0.10

Cisco EIGRP

- Version: 2
- Opcode: Hello (5)
- Checksum: 0xeecb [correct]
- Flags: 0x00000000
- Sequence: 0
- Acknowledge: 0
- Virtual Router ID: 0 (Address-Family)
- Autonomous System: 1
- Parameters
 - Type: Parameters (0x0001)
 - Length: 12
 - K1: 1
 - K2: 0
 - K3: 1
 - K4: 0
 - K5: 0
 - K6: 0
 - Hold Time: 15
- Software Version: EIGRP=12.4, TLV=1.2

```
0000  01 00 5e 00 00 0a ca 04 0b 82 00 70 08 00 45 c0  ..^....p..E.
0010  00 3c 00 00 00 00 02 58 cc 9a 0a 01 01 05 e0 00  <.....X.....
0020  00 0a 02 05 ee cb 00 00 00 00 00 00 00 00 00 00  .....
0030  00 00 00 00 00 01 00 01 00 0c 01 00 01 00 00 00  .....
0040  00 0f 00 04 00 08 0c 04 01 02
```

TLV Type (eigrp.tlv_type), 2 bytes

Packets: 782 · Displayed: 782 (100.0%)

Profile: Default

Hack the Network via EIGRP

EIGRP Attack Vectors

- Inject routes to mask source of attack
- DoS
- Inject routes for MITM
- Add new routes to hacked router
- Change interface bandwidth for Traffic Engineering on hacked router

EIGRP Exploit Tools

- GSN3\Dynamips
- Buy a router on eBay
- Hack a router and reconfigure
- Phenoelit IRPAS

Similar to OSPF, EIGRP typically is implemented without any thought to security. Network administrators should use authentication and configure interfaces to be passive in EIGRP.

10.1.1.0
255.255.255.0



192.168.1.0
255.255.255.0

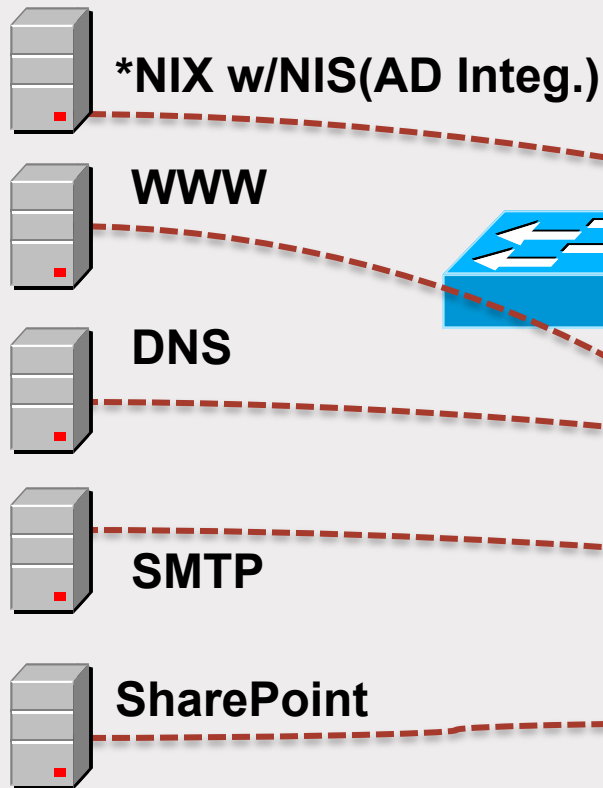


10.1.2.0
255.255.255.0

DMZ Layer 2 Security

DMZ

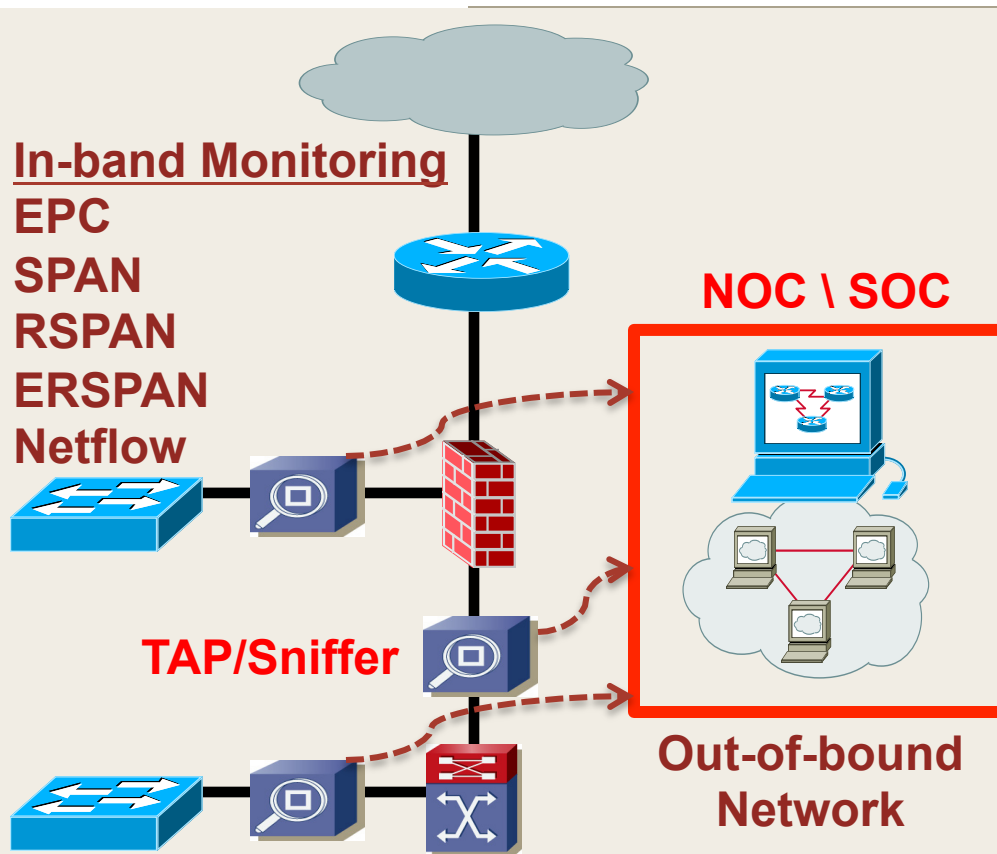
- Typically single VLAN
- Open trusts Inside VLAN
- DMZ to Internal AD integ.
- Pivot from DMZ to Internal network



Secure DMZ Trusts

- PVLAN
- VACL
- Separate Virtual or Physical Int w/ ACL's
- Develop a network traffic matrix to define required network traffic flows

The screenshot displays the ntop web interface. At the top, there is a navigation bar with links: About, Summary, IP, Media, Admin, and Utils. The main content area is divided into two columns. The left column contains a sidebar with a search bar and a list of hosts. The right column contains two line graphs showing network traffic over time. The top graph is labeled 'Packets/sec' and shows traffic for 'ethernet' (blue) and 'bro' (yellow). The bottom graph is also labeled 'Packets/sec' and shows traffic for 'up T01E10' (blue), 'up T0120' (cyan), and 'up T' (magenta). Below the graphs, there is a table titled 'Traffic U' with columns for 'Host', 'Domain', and 'IP Address'. The table lists various hosts, including 'host254', 'host078-144', 'host005-160', 'host019-154', 'host017-148', 'host081-144', 'host016-148', 'host067-144', 'host153-147', 'host095-144', 'host019-146', 'host014-148', 'freebsd.computerhouseprato.com', 'freebsd.giovannelli.com', 'host012-144', and 'host023-146'. Each host entry is accompanied by a small icon representing the host's status or type.



Login: Gordon, Scott (sgordon) :: [Logout](#) :: [Activate](#)

The diagram is titled "Attack Diagram". It features a central node labeled "E-11" with a value of "210" above it. This central node is connected to several other nodes, each with a value and a label:

- Top right: Node with value "10" and label "Large Graph" (with a "Help" link).
- Top left: Node with value "210" and label "Corpora-7".
- Bottom left: Node with value "20" and label "NEW".
- Bottom left: Node with value "20" and label "20.20.32.27".
- Bottom center: Node with value "20" and label "20.20.32.29".
- Bottom center: Node with value "20" and label "20.20.32.28".
- Bottom right: Node with value "20" and label "Corp-S&W-12".
- Bottom right: Node with value "20" and label "20.20.32.30".

Arrows indicate the direction of the connections, generally pointing from the central node "E-11" towards the peripheral nodes.

illa Firefox

[illegible]

64.178.225.2

Whitelist the Layer 2 Network Trust Relationships

Whitelist Trusted Information Flows in Monitoring

Secure Control, Management, Data Planes

References

Developing IP Multicast Networks, Vol 1 – Beau Williamson

LAN Switch Security – What Hackers Know About Your Switches, Eric Vyncke, Christopher Paggen, Cisco Press

Enno Rey - [@Enno_Insinuator](#), [@WEareTROOPERS](#), ERNW Papers and Resources ,[www.ernw.de](#), [www.insinuator.net](#)

Ivan Pepelnjak - [@IOShints](#), Papers and Resources, [http://www.ipspace.net](#)

IPv6 Security, Scott Hogg and Eric Vyncke, Cisco Press

[http://www.gtri.com/wp-content/uploads/2014/10/IPv6-Hacker-Halted-The-Hacker-Code-Angels-vs-Demons.pdf](#)

The Practice of Network Security Monitoring, Ricard Bejtlich, No Starch Press

Router Security Strategies Securing IP Network Traffic Planes, Gregg Schudel, David J. Smith, Cisco Press

[https://www.cisco.com/go/safe](#)

[http://docwiki.cisco.com/wiki/FHS](#)

[http://www.netoptics.com/blog/01-07-2011/sample-pcap-files](#)

[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/12-4/fhrp-12-4-book.html](#)

[http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook/sec_chap8.html](#)

[http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/best/practices/recommendations.html](#)

[http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook/sec_chap8.html](#)

[http://www.cisco.com/web/about/security/intelligence/ipv6_first_hop.html](#)

[http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html](#)

[http://monkey.org/~dugsong/dsniff/](#)

[https://www.yersinia.net](#)

[https://www.nsa.gov/ia/_files/factsheets/Factsheet-Cisco%20Port%20Security.pdf](#)

[http://iase.disa.mil/stigs/net_perimeter/network-infrastructure/Pages/index.aspx](#)

[http://www.cisco.com/c/en/us/about/security-center/multicast-toolkit.html](#)

Questions?

@PaulCoggin

OSPF – MD5 Authentication

Capturing from Standard input — R5 GigabitEthernet4/0 to R4 GigabitEthernet4/0

Apply a display filter ... <%%/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.1.6	224.0.0.2	LDP	76	Hello Message
2	2.288151	10.1.1.6	224.0.0.5	OSPF	134	Hello Packet
3	2.530153	10.1.1.5	224.0.0.2	LDP	76	Hello Message
4	3.377193	ca:05:0b:91:00:70	ca:05:0b:91:00:70	LOOP	60	Reply
5	3.880662	10.1.1.6	224.0.0.2	LDP	76	Hello Message
6	6.369121	10.1.1.5	224.0.0.2	LDP	76	Hello Message
7	6.581011	ca:04:0b:82:00:70	ca:04:0b:82:00:70	LOOP	60	Reply

▶ Frame 2: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0

▶ Ethernet II, Src: ca:05:0b:91:00:70 (ca:05:0b:91:00:70), Dst: IPv4mcast_05 (01:00:5e:00:00:05)

▶ Internet Protocol Version 4, Src: 10.1.1.6, Dst: 224.0.0.5

▼ Open Shortest Path First

- ▼ OSPF Header
 - Version: 2
 - Message Type: Hello Packet (1)
 - Packet Length: 48
 - Source OSPF Router: 10.10.10.3
 - Area ID: 0.0.0.0 (Backbone)
 - Checksum: 0x0000 (None)
 - Auth Type: Cryptographic (2)
 - Auth Crypt Key id: 0
 - Auth Crypt Data Length: 16
 - Auth Crypt Sequence Number: 1473248891
 - Auth Crypt Data: 3fbb955c044b00812ed95526675efe55
- ▶ OSPF Hello Packet
- ▶ OSPF LLS Data Block

```
0000 01 00 5e 00 00 05 ca 05 0b 91 00 70 08 00 45 c0 ..^.....p..E.
0010 00 78 4f 30 00 00 01 59 7e 31 0a 01 01 06 e0 00 .x00...Y~1.....
0020 00 05 02 01 00 30 0a 0a 0a 03 00 00 00 00 00 .....0.....
0030 00 02 00 00 00 10 57 cf fe 7b ff ff ff fc 00 0a .....W.{.....
0040 12 01 00 00 00 28 0a 01 01 06 0a 01 01 05 0a 0a .....(.....
0050 0a 01 3f bb 95 5c 04 4b 00 81 2e d9 55 26 67 5e ...?...\K....U&g^
0060 fe 55 00 00 00 09 00 01 00 04 00 00 00 01 00 02 .U.....
```



Ready to load or capture

Packets: 36 · Displayed: 36 (100.0%)

Profile: Default

EIGRP – MD5 Authentication

Standard input — R5 GigabitEthernet4/0 to R4 GigabitEthernet4/0

eigrp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.1.5	224.0.0.10	EIGRP	114	Hello
9	3.607382	10.1.1.6	224.0.0.10	EIGRP	114	Hello
10	4.252377	10.1.1.5	224.0.0.10	EIGRP	114	Hello
14	8.312548	10.1.1.6	224.0.0.10	EIGRP	114	Hello
15	8.896544	10.1.1.5	224.0.0.10	EIGRP	114	Hello
20	12.896461	10.1.1.6	224.0.0.10	EIGRP	114	Hello
22	13.521366	10.1.1.5	224.0.0.10	EIGRP	114	Hello
26	17.492588	10.1.1.6	224.0.0.10	EIGRP	114	Hello
28	18.016178	10.1.1.5	224.0.0.10	EIGRP	114	Hello
32	22.067549	10.1.1.6	224.0.0.10	EIGRP	114	Hello

▶ Frame 9: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0

▶ Ethernet II, Src: ca:05:0b:91:00:70 (ca:05:0b:91:00:70), Dst: IPv4mcast_0a (01:00:5e:00:00:0a)

▶ Internet Protocol Version 4, Src: 10.1.1.6, Dst: 224.0.0.10

▼ Cisco EIGRP

- Version: 2
- Opcode: Hello (5)
- Checksum: 0xcb95 [correct]
- Flags: 0x00000000
- Sequence: 0
- Acknowledge: 0
- Virtual Router ID: 0 (Address-Family)
- Autonomous System: 1
- Authentication MD5
 - Type: Authentication (0x0002)
 - Length: 40
 - Type: MD5 (2)
 - Length: 16
 - Key ID: 1
 - Key Sequence: 0
 - Nullpad: 0000000000000000
 - Digest: 6fbfcabd4cf1afe9162b2bc289b41fff
- Parameters
- Software Version: EIGRP=12.4 TLV=1.2

0050 ca bd 4c f1 af e9 16 2b 2b c2 89 b4 1f ff 00 01 ..L....+ +.....
0060 00 0c 01 00 01 00 00 00 00 0f 00 04 00 08 0c 04
0070 01 02 ..

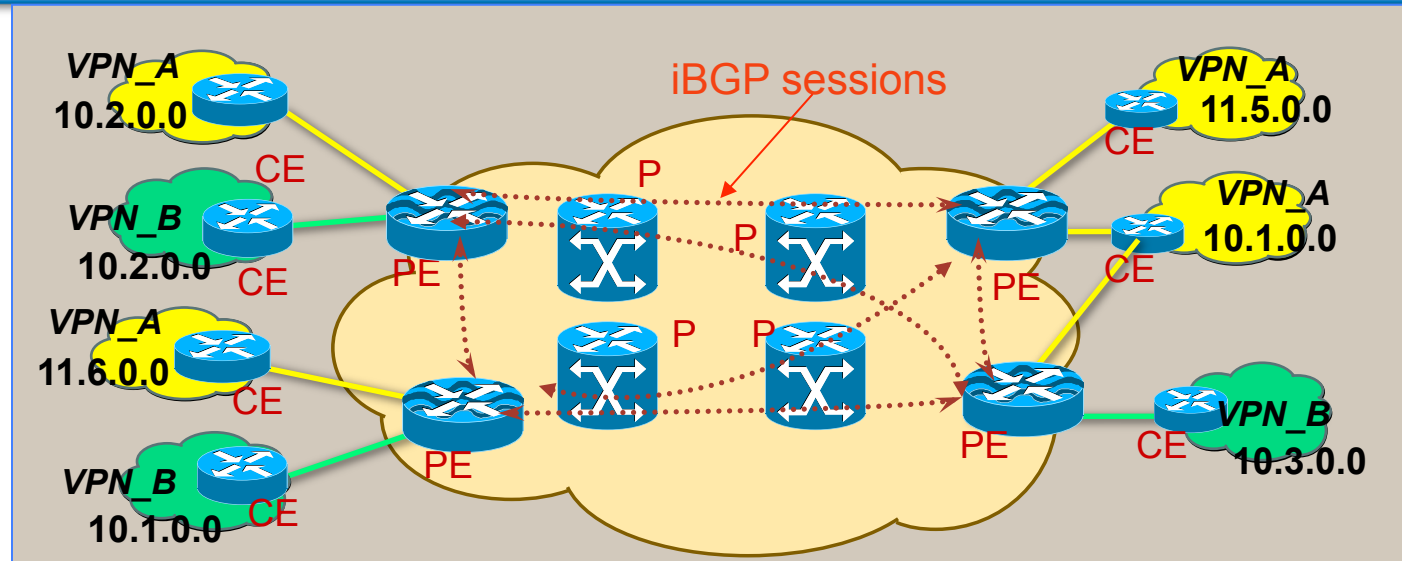
EIGRP TLV version (eigrp.tlv_version), 2 bytes

Packets: 167 · Displayed: 49 (29.3%)

Profile: Default

10.1.2.0
255.255.255.0

MPLS Architecture Overview



- P Routers (LSRs) are in the Core of the MPLS Cloud
- PE Routers (Edge LSRs or LERs) Use MPLS with the Core and Plain IP with CE Routers
- P and PE Routers Share a Common IGP
- PE Routers are MP-iBGP Fully-meshed

Service provider may accidentally or intentionally misconfigure VPN's
Utilize IPSEC VPN over MPLS VPN to insure security

MPLS Label PCAP - Service Provider Core

CPE to CPE Telnet over Service Provider MPLS VPN

No.	Time	Source	Destination	Protocol	Length	Info
25	13.704914	10.1.1.6	224.0.0.2	LDP	76	Hello Message
26	13.987283	10.1.1.5	224.0.0.5	OSPF		
27	14.379748	192.168.1.2	192.168.2.2	TELNET		
28	14.420133	192.168.2.2	192.168.1.2	TELNET		
29	14.612199	192.168.1.2	192.168.2.2	TELNET		
30	14.662586	192.168.2.2	192.168.1.2	TELNET		
31	14.755023	192.168.1.2	192.168.2.2	TELNET	68	Telnet Data ...
32	14.813915	192.168.2.2	192.168.1.2	TELNET	68	Telnet Data ...
33	14.954802	192.168.1.2	192.168.2.2	TELNET	68	Telnet Data ...

Frame 32: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
Ethernet II, Src: 08:00:27:00:00:00, Dst: 08:00:27:00:00:00, Protocol: Telnet (0x00000000)

MultiProtocol Label Switching Header, Label: 16, Exp: 6, S: 0, TTL: 253
0000 0000 0000 0001 0000 = MPLS Label: 16
..... 110. = MPLS Experimental Bits: 6
..... 0 = MPLS Bottom Of Label Stack: 0
..... 1111 1101 = MPLS TTL: 253

MultiProtocol Label Switching Header, Label: 25, Exp: 6, S: 1, TTL: 254
0000 0000 0000 0001 1001 = MPLS Label: 25
..... 110. = MPLS Experimental Bits: 6
..... 1 = MPLS Bottom Of Label Stack: 1
..... 1111 1110 = MPLS TTL: 254

Internet Protocol Version 4, Src: 192.168.2.2, Dst: 192.168.1.2
Transmission Control Protocol, Src Port: 23 (23), Dst Port: 35676 (35676), Seq: 10, Ack: 8, Len: 1
Telnet

32-bit MPLS Label Format

- Label : 20-bit
- EXP : 3-bit
- Bottom-of-Stack : 1-bit
- TTL : 8-bit

Router PCAP

Packets: 1579 · Displayed: 1579 (100.0%) · Load time: 0:0.25 · Profile: Default

Telnet Username \ Password – Clear Text Encapsulated in MPLS VPN

Router PCAP.pcapng

tcp.stream eq 2

No.	Time	Source	Destination	Protocol	Length	Info
46	18.531077	192.168.1.2	192.168.2.2	TCP	68	52616 → 23 [SYN] Seq=0 Win=4128 Len=0 MSS...
47	18.591464	192.168.2.2	192.168.1.2	TCP	68	23 → 52616 [SYN, ACK] Seq=0 Ack=1 Win=412...
48	18.631724	192.168.1.2	192.168.2.2	TCP	68	52616 → 23 [ACK] Seq=1 Ack=1 Win=4128 Len...
49	18.631735	192.168.1.2	192.168.2.2	TELNET	71	Telnet Data ...
50	18.641907	192.168.1.2	192.168.2.2	TCP	68	[TCP Dup ACK 48#1] 52616 → 23 [ACK] Seq=1...
51	18.692276	192.168.2.2	192.168.1.2	TELNET	74	Telnet Data ...
52	18.692307	192.168.2.2	192.168.1.2	TELNET	104	Telnet Data ...
53	18.712380	192.168.2.2	192.168.1.2	TELNET	68	Telnet Data ...
54	18.712408	192.168.2.2	192.168.1.2	TELNET	68	Telnet Data ...

Frame 49: 71 bytes on wire (568 bits) 71 bytes captured (568 bits) on interface 0

Ethernet II, Src: ca:04:0b:82:00:70 (ca:04:0b:82:00:70), Dst: ca:05:0b:91:00:70 (ca:05:0b:91:00:70)

MultiProtocol Label Switching Header, Label: 16, Exp: 6, S: 0, TTL: 253

MultiProtocol Label Switching Header, Label: 28, Exp: 6, S: 1, TTL: 254

Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.2.2

Transmission Control Protocol, Src Port: 52616, Dst Port: 23

Telnet

Wireshark · Follow TCP Stream (tcp.stream eq 2) · Router PCAP

```
.....!.....  
User Access Verification  
Username: ..!...!.....P.....ccisiscoco  
Password: sanfran  
R7>  
R7>
```

20 client pkt(s), 17 server pkt(s), 17 turns.

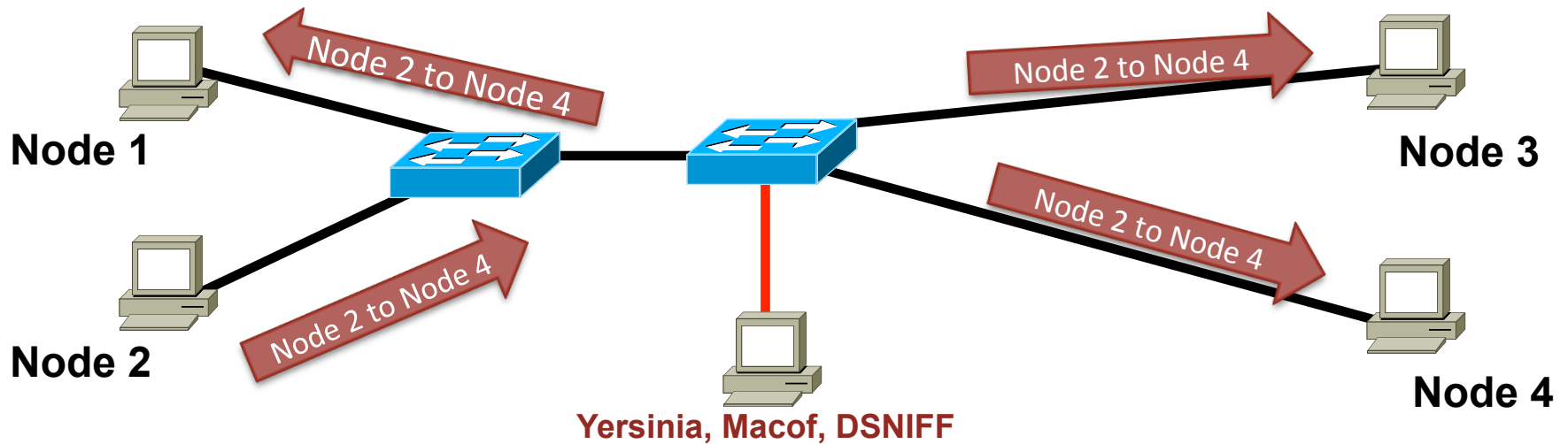
Router PCAP

Packets: 1579 · Displayed: 57 (3.6%) · Load time: 0:0.40 · Profile: Default

0000
0010
0020
0030
0040

A Separate Overlay Encrypted VPN is Required to Secure Your Traffic

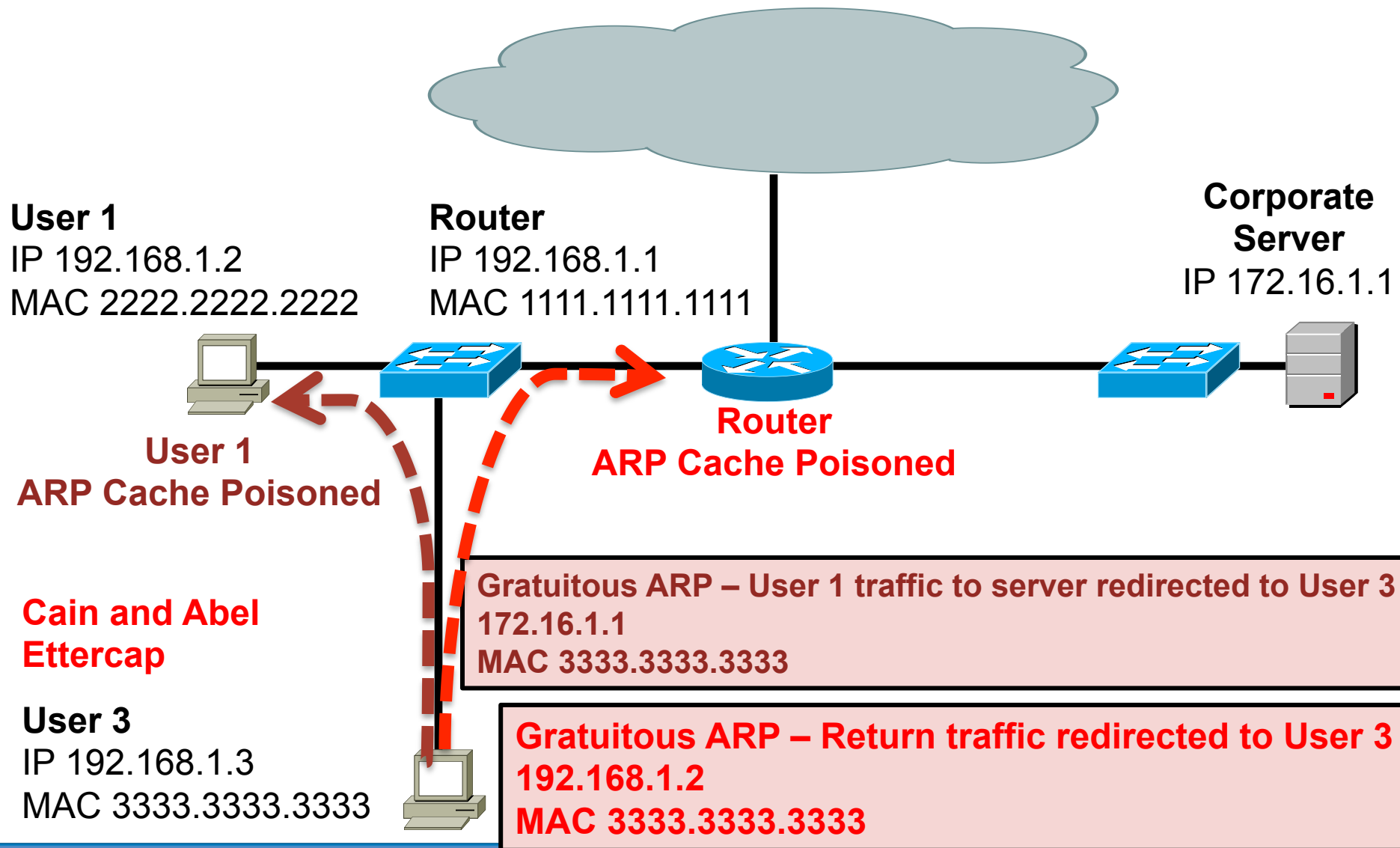
CAM Table Overflow Attack



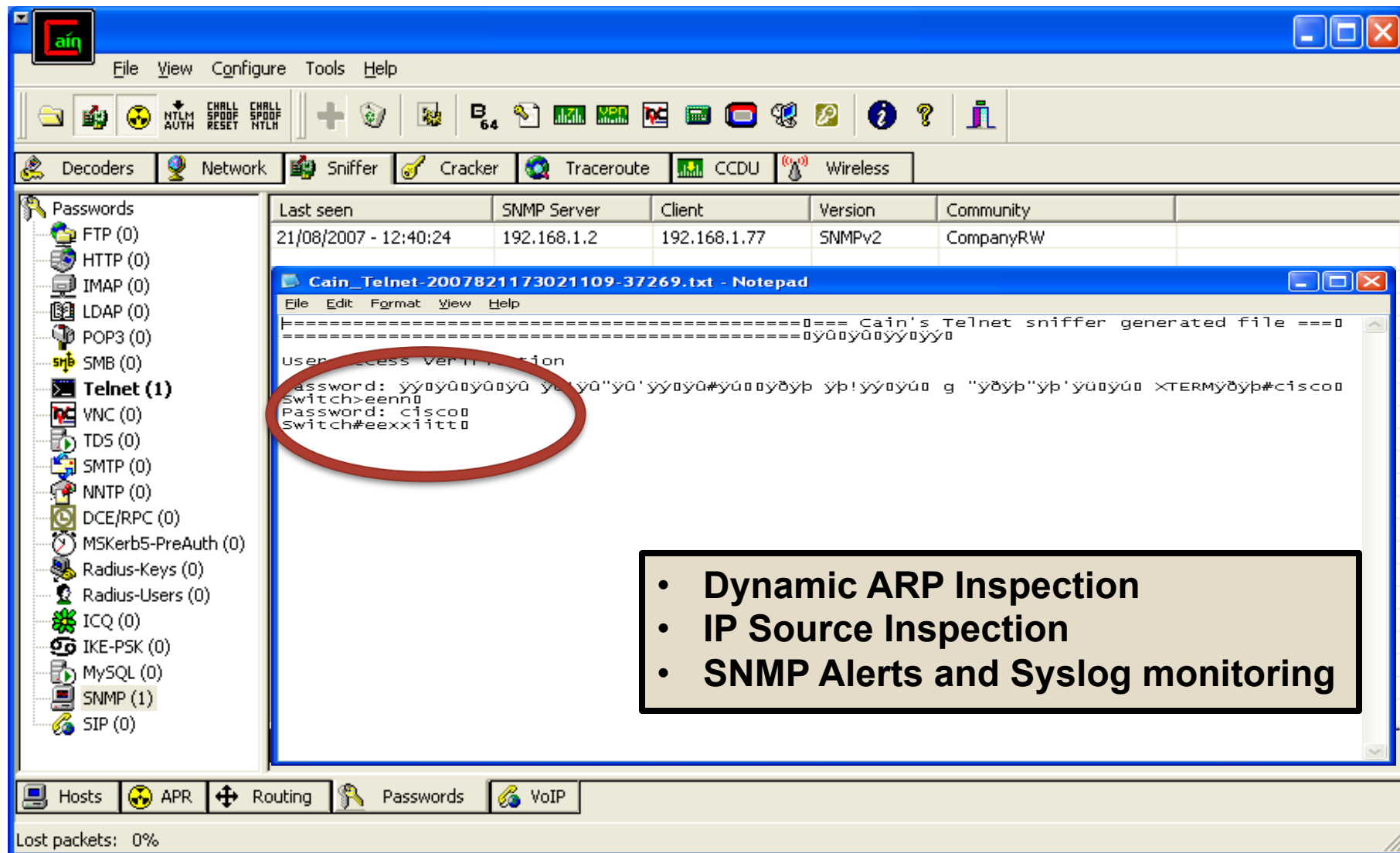
Switch CAM table exploited resulting in switch VLAN operating like a shared Ethernet hub
Attack may cause multiple switches to fallback to shared Ethernet behavior

Implement port security to limit MACs per interface, SNMP Traps

ARP Poisoning



ARP Poisoning



The screenshot displays the Cain & Abel network sniffer interface. On the left, a tree view shows various protocols, with 'Telnet (1)' selected. The main window shows a table of network activity. A Notepad window titled 'Cain_Telnet-2007821173021109-37269.txt' is open, displaying a Telnet session log. A red circle highlights the login attempt details.

Last seen	SNMP Server	Client	Version	Community
21/08/2007 - 12:40:24	192.168.1.2	192.168.1.77	SNMPv2	CompanyRW

```
===== Cain's Telnet sniffer generated file =====  
=====0y00y00yy0yy0  
User access verification  
Password: y0y00y00y0 y0 y0"y0'y0y0#y00y00y0 y0!y0y00 g "y0y0"y0'y00y00 xTERMy0y0#cisco0  
Switch>eenno  
Password: cisco0  
Switch#eexxiitt0
```

- Dynamic ARP Inspection
- IP Source Inspection
- SNMP Alerts and Syslog monitoring

Rogue DHCP Server

Unauthorized DHCP Server

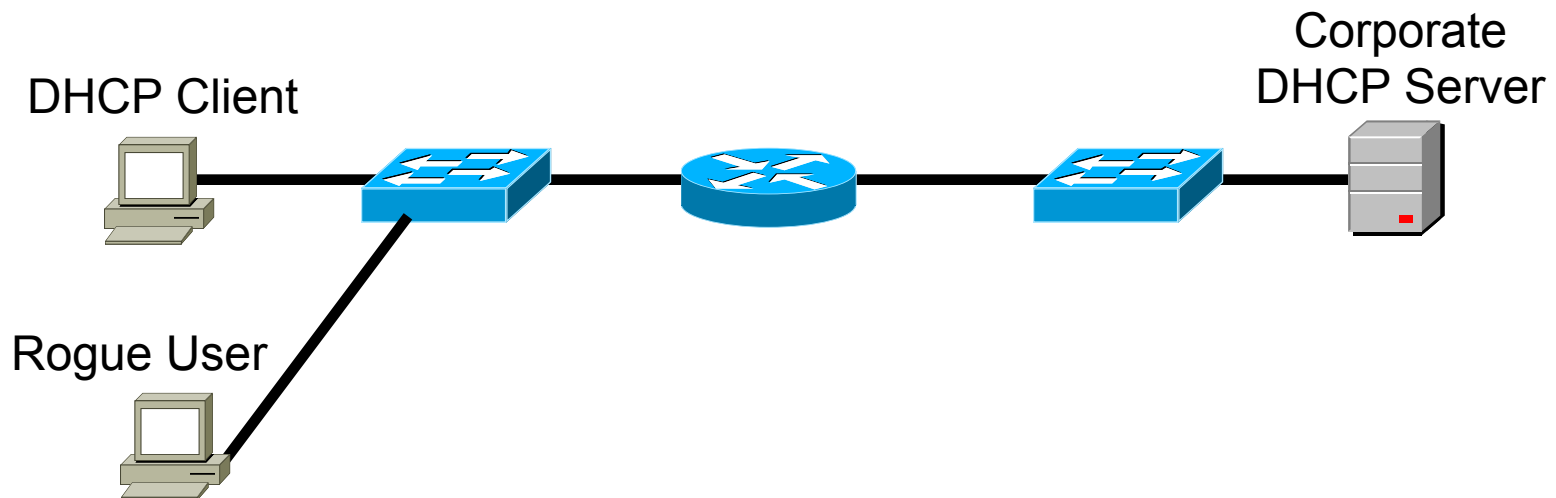
- Allocates bad DNS server or default gateway

Denial of service by exhausting the leases in the DHCP scope

- Tools – Yersinia, Gobbler

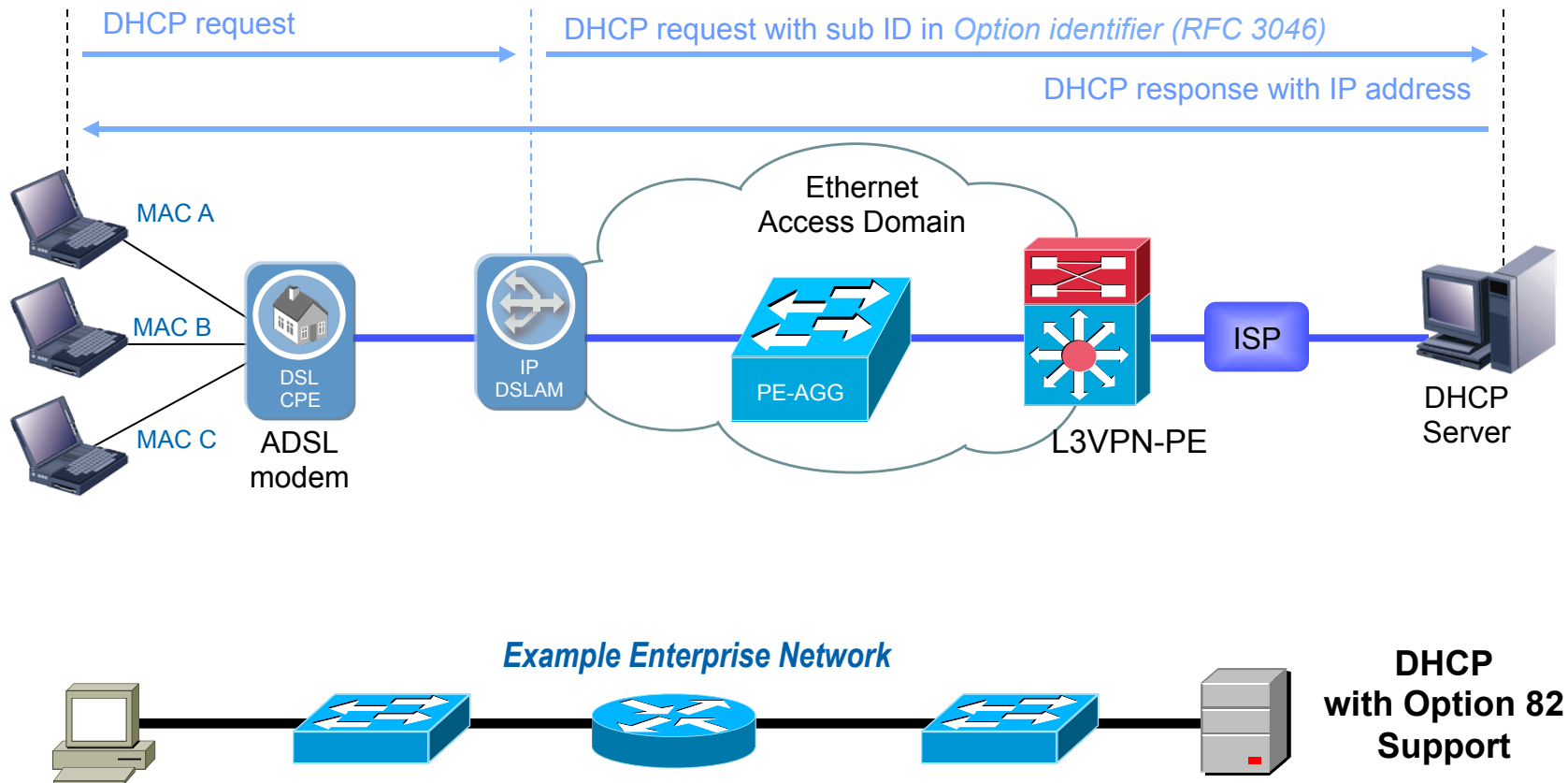
Mitigation

- Limit MAC addresses per interface
- VACL's to block DHCP UDP 68
- DHCP snooping Trusted\Untrusted (mitigates client hardware address change)



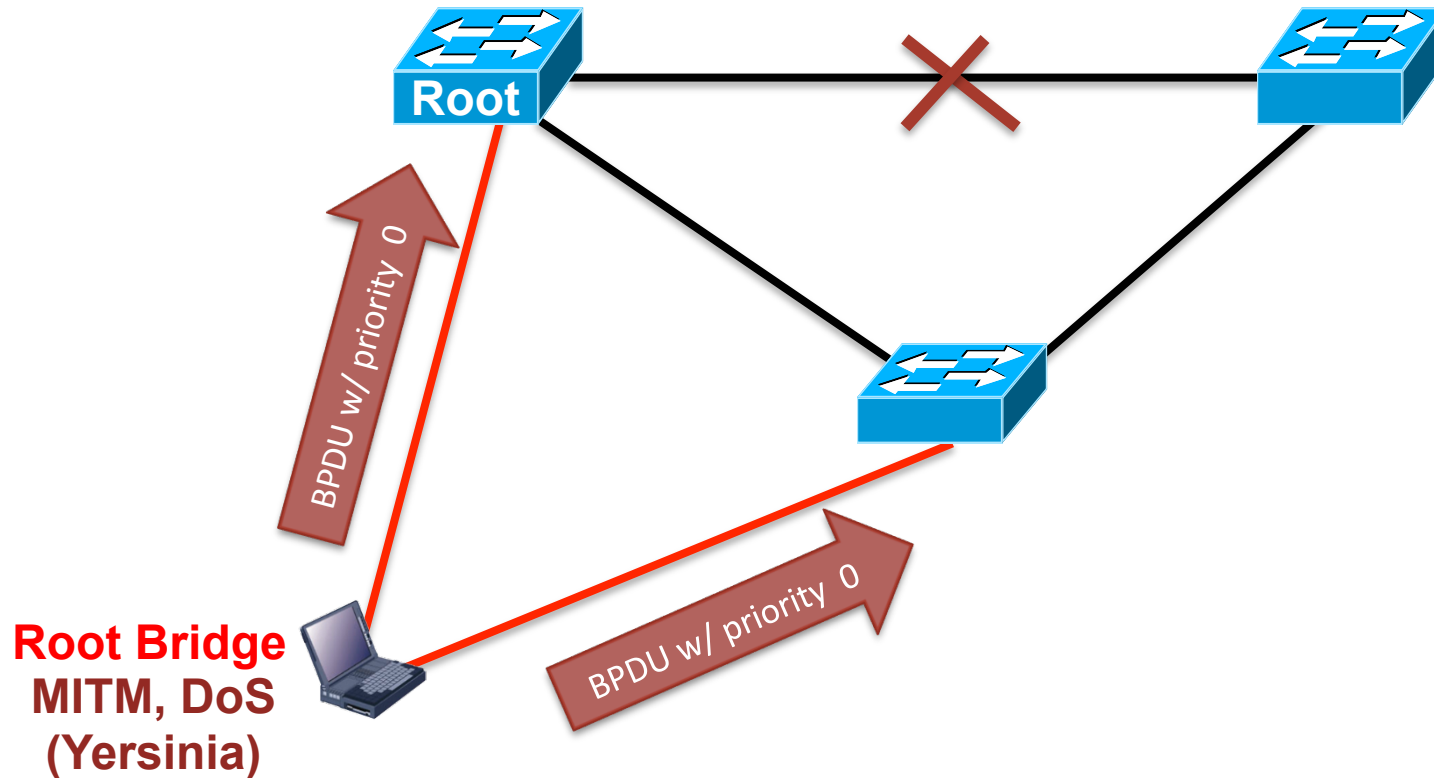
Lawful Intercept

Identify Physical Source of Traffic



DHCP Option 82 provides the DSLAM and Switch Name and the Physical Interface That Requested a DHCP IP Address

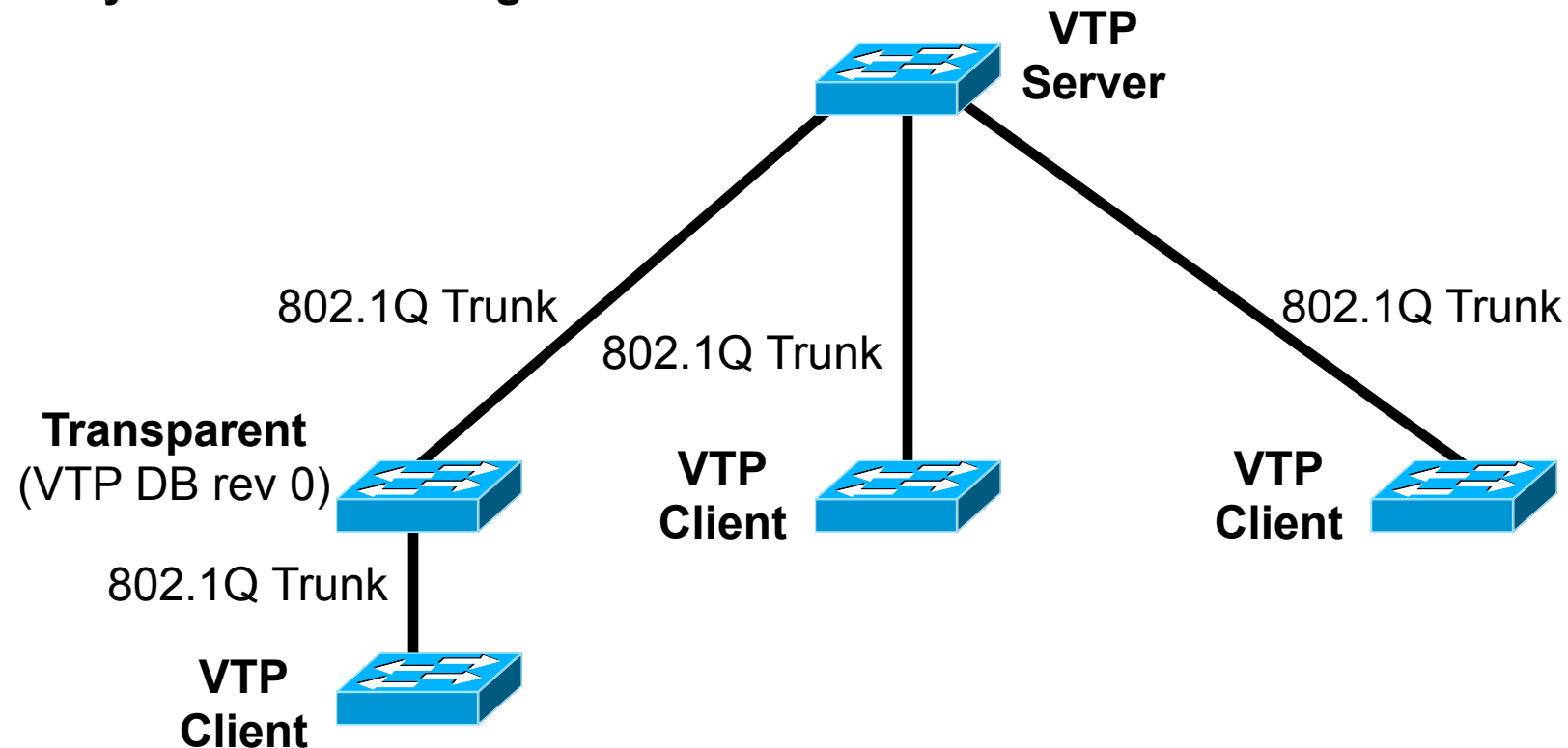
Spanning Tree Protocol – Attack



Implement Root Guard, BPDU Guard, Syslog, SNMPv3 Alerts

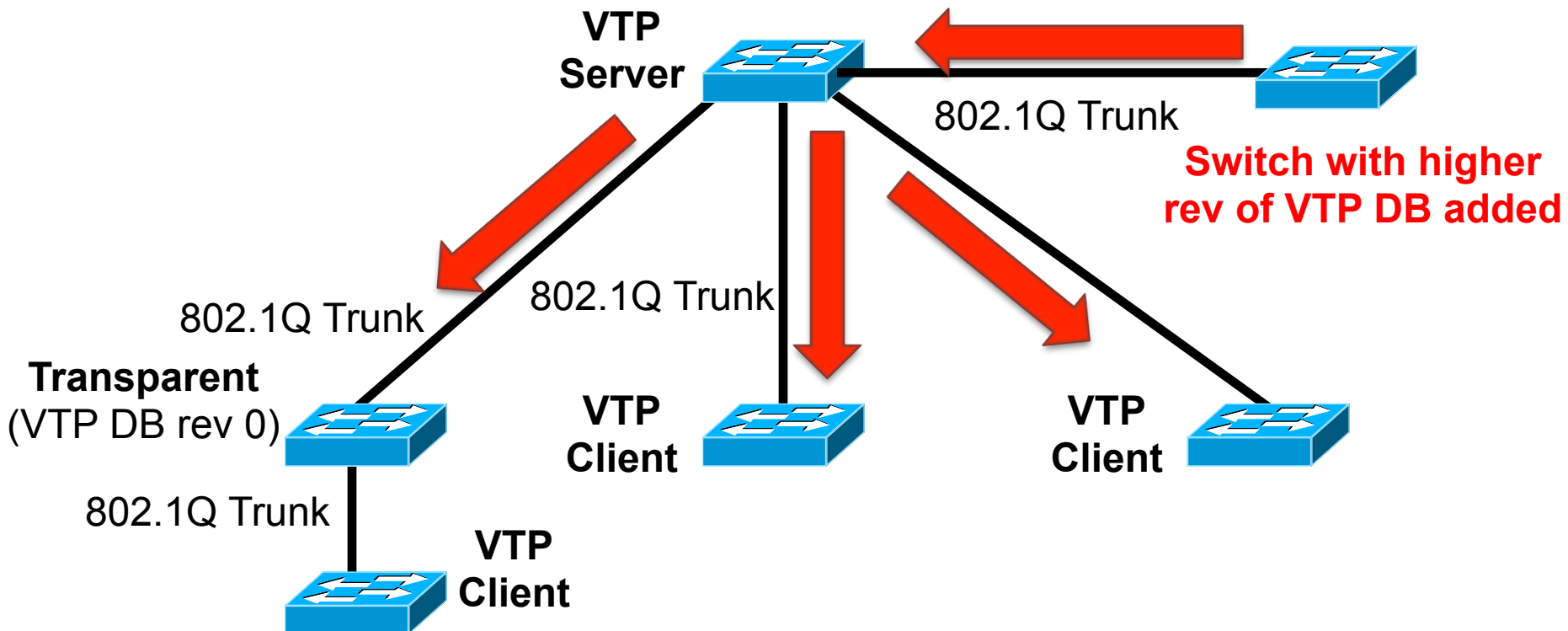
VLAN Trunking Protocol (VTP)

- VLANs are added\removed on VTP Server
- VLAN modifications propagated to VTP Clients
- Common VTP Domain name and password
- Same Native VLAN on Trunk
- Sync to latest changes

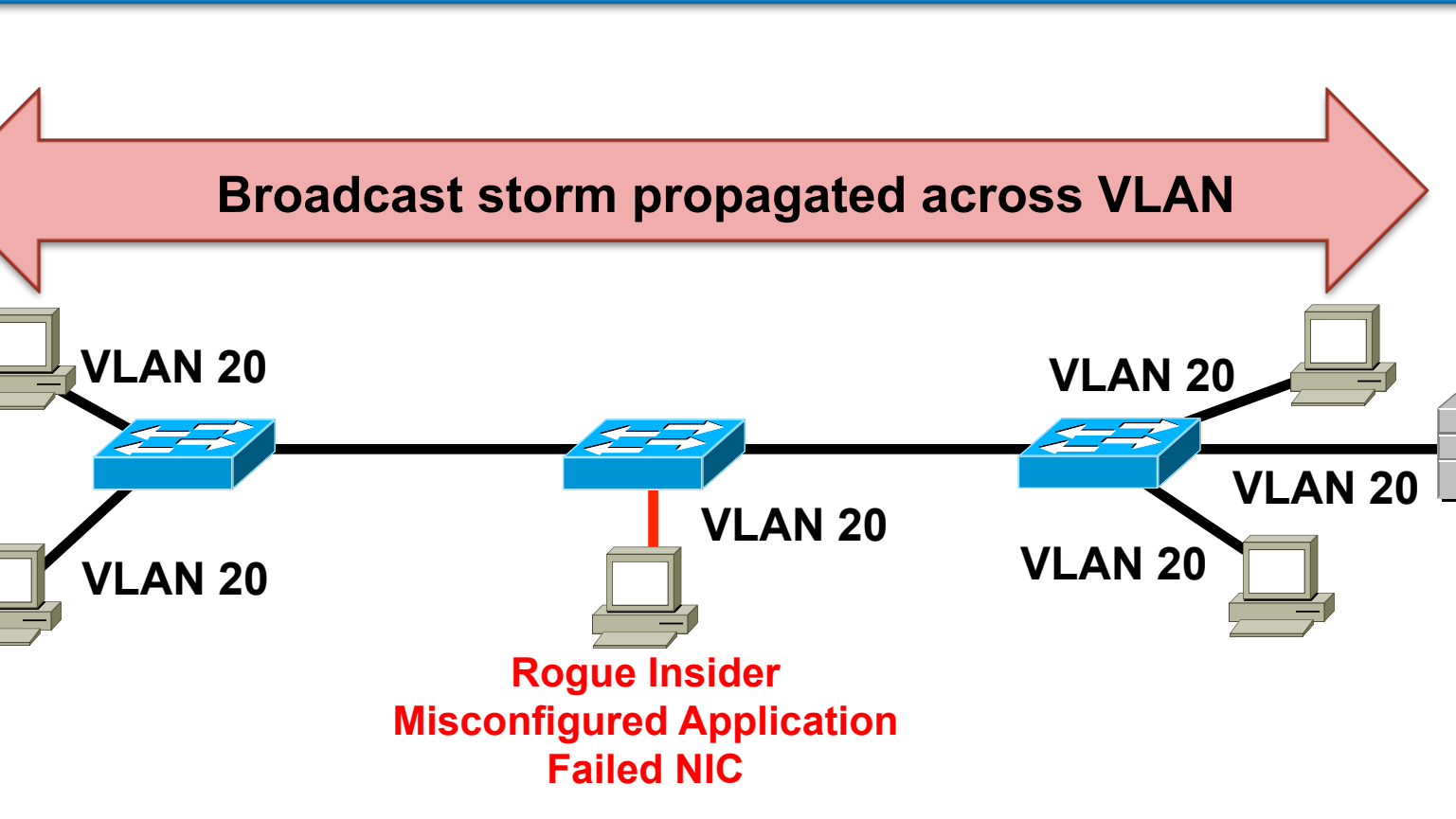


VLAN Trunking Protocol (VTP) - Security

- Existing network running default VTP settings
- **Switches sync to higher rev VTP DB resulting in VLAN config being lost!!**
- Everyone has a current VLAN.DAT backup right??
- **Configure a password for VTP Domain (NOT Cisco....SanFran....)**
- **Delete VLAN.DAT before connecting a new switch**
- **Change the native VLAN to something other than 1**



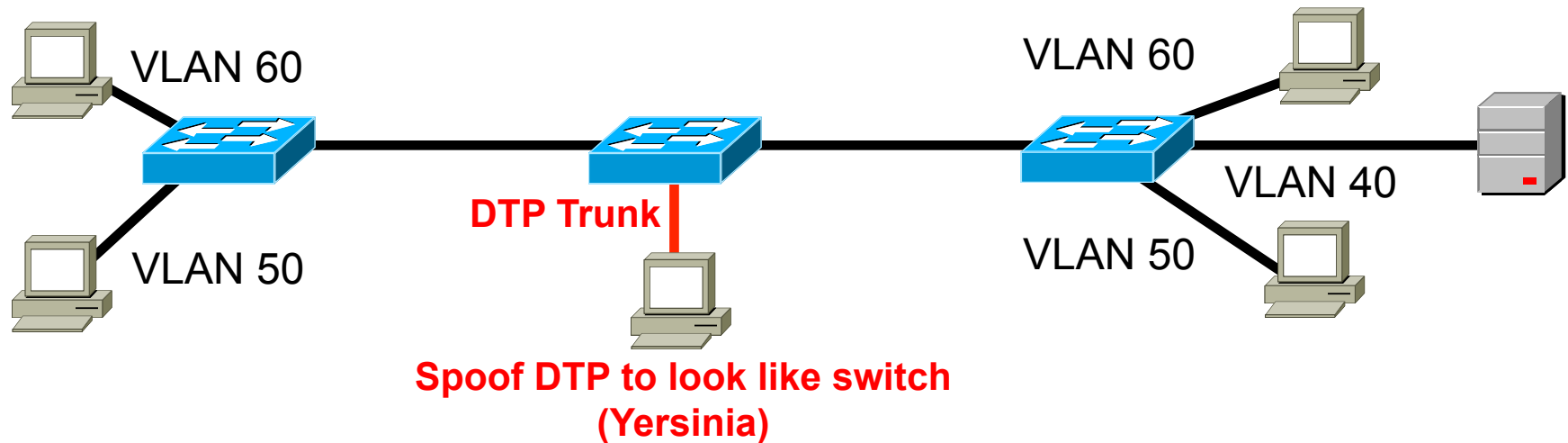
Broadcast Storms



Traffic Storm Control limits unicast, multicast, broadcast traffic to a % of port BW

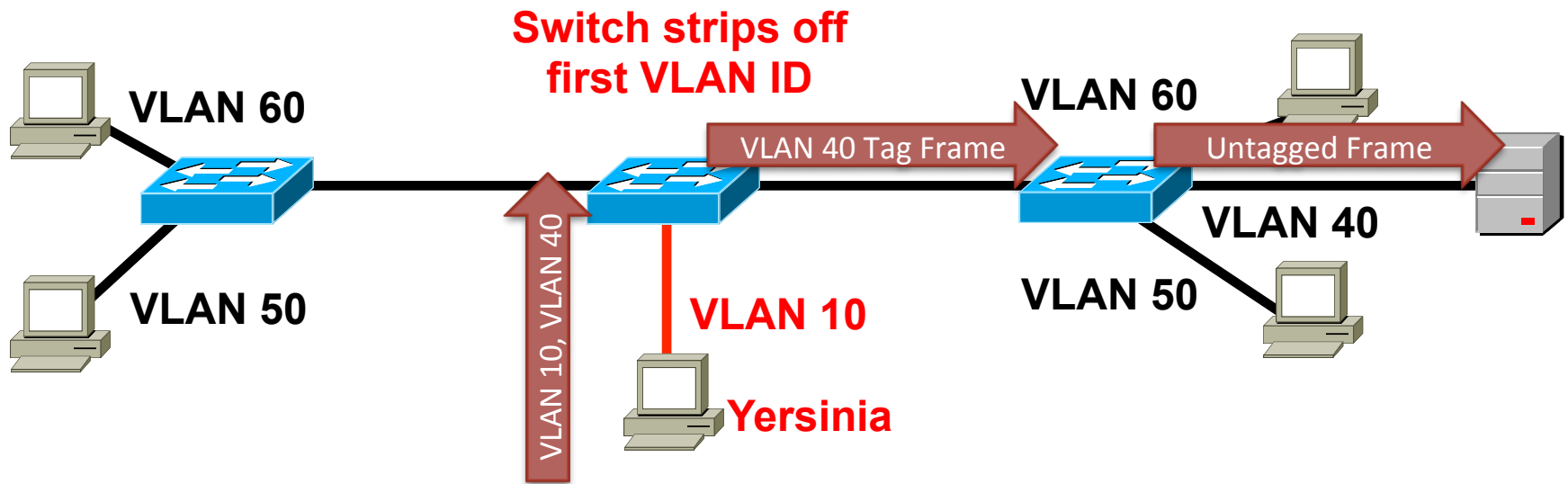
- Not enabled on interfaces by default (add to template configuration for port security)
- Traffic that exceeds configured threshold will be dropped
- Violations can be configured to be **shutdown** or send a **SNMP Trap(recommend v3)**

VLAN Hopping – Dynamic Trunking Protocol



- Dynamic Trunk Protocol (DTP) Modes : Auto, On, Off, Desirable, Non-negotiate
- IP Phones, Wireless Access Points
- All VLANs are trunked by default
- Native VLAN (untagged); Default **Native VLAN 1** and required by DTP
- Yersinia or other packet crafting tools
- Disable trunking on interfaces where not in use
- Specify VLANs to be allowed on trunk interfaces
- Do not use Native VLAN **1**

VLAN Hopping – Double VLAN Tag



- No two-way communication. Frames sent to target with no response to sender.
- Craft Frames with double encapsulated frames
- VLAN trunking is not required in this scenario
- **Disable AUTO/DYNAMIC NEGOTIATION!**
- **Don't use native VLAN 1. Use tagged mode for native VLAN x on trunks**
- **Disable interfaces not in use**