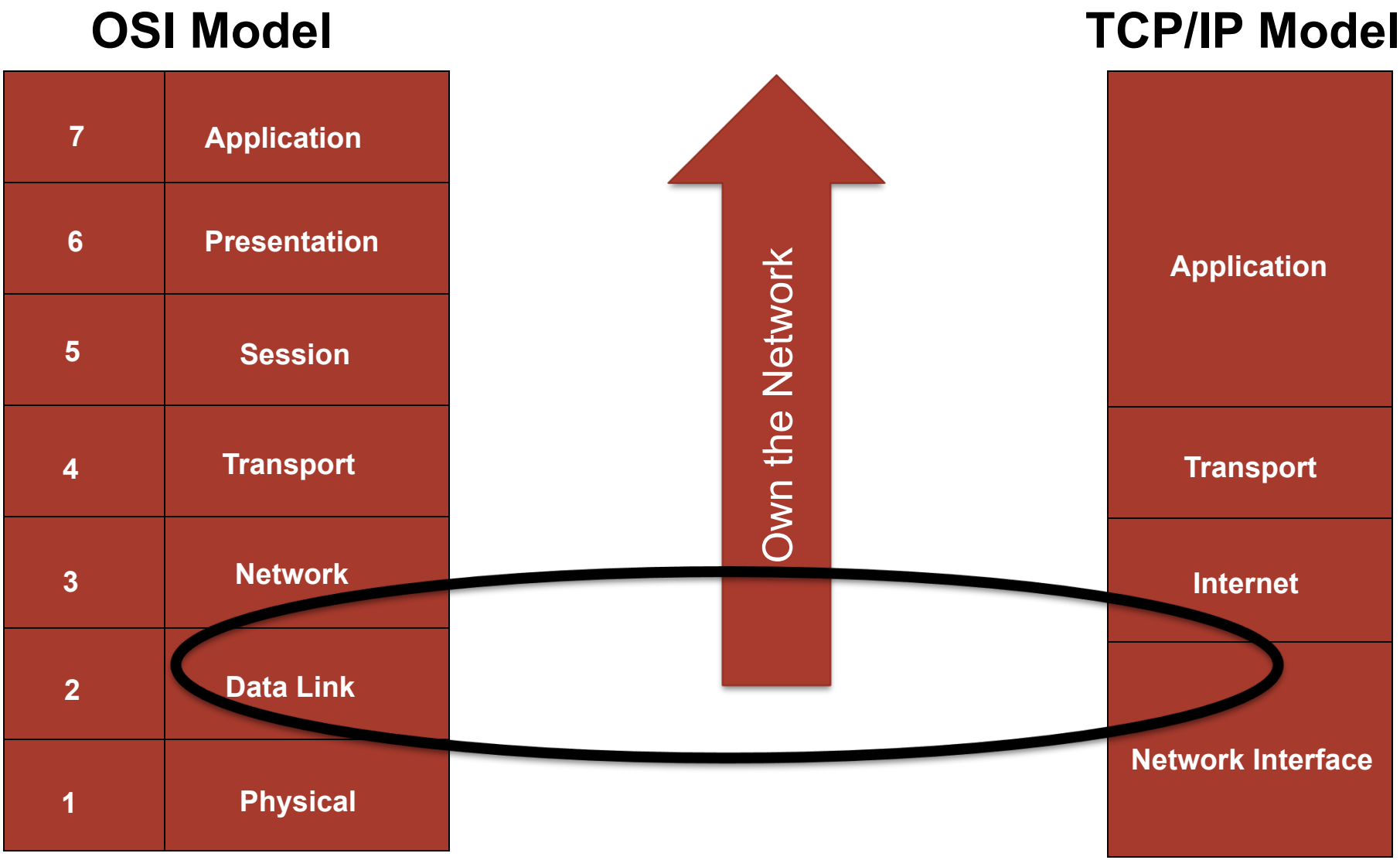
Twisting Layer 2 Protocols

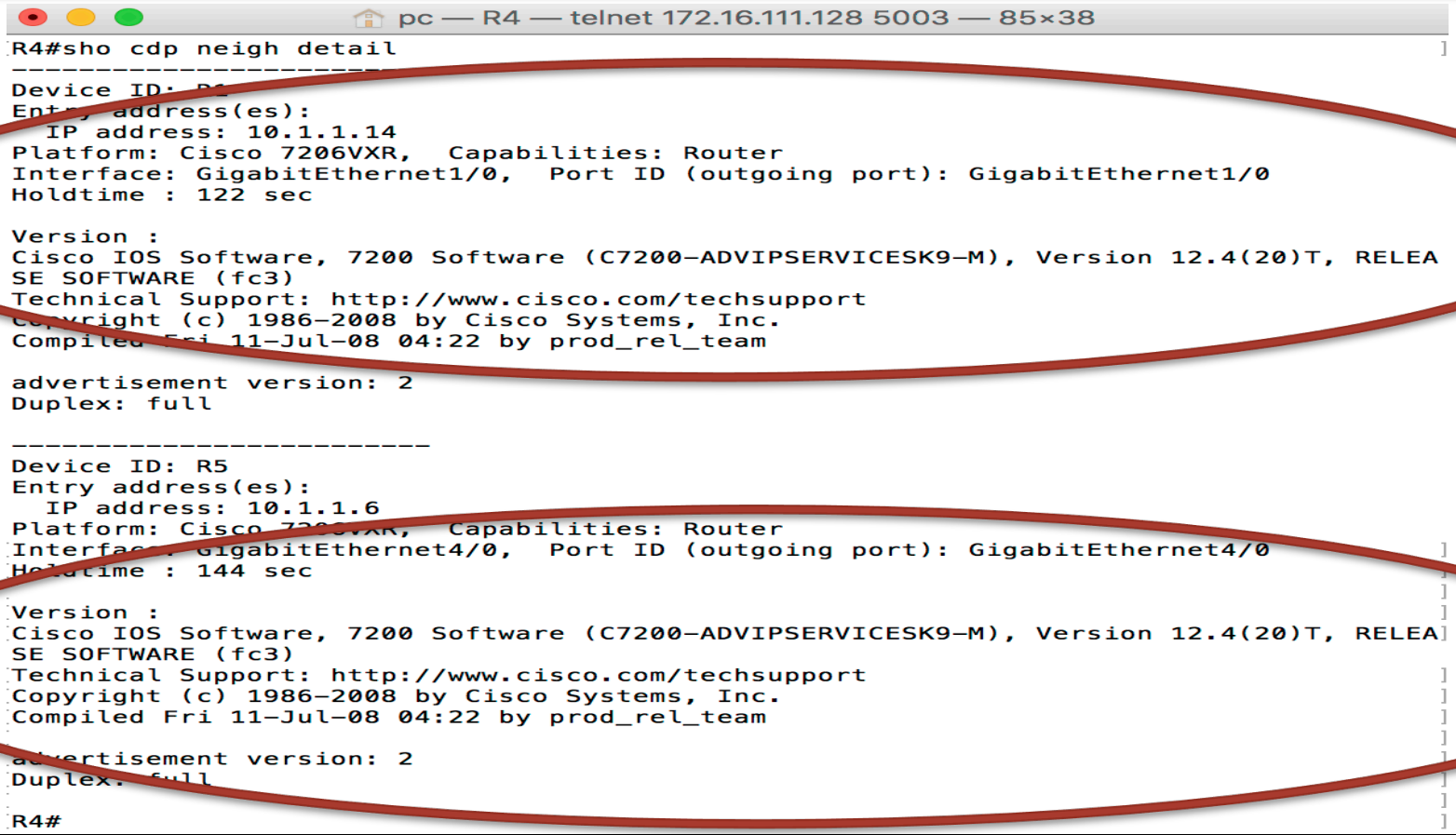
DefCamp 8

Paul Coggin
@PaulCoggin

OSI and TCP/IP Model



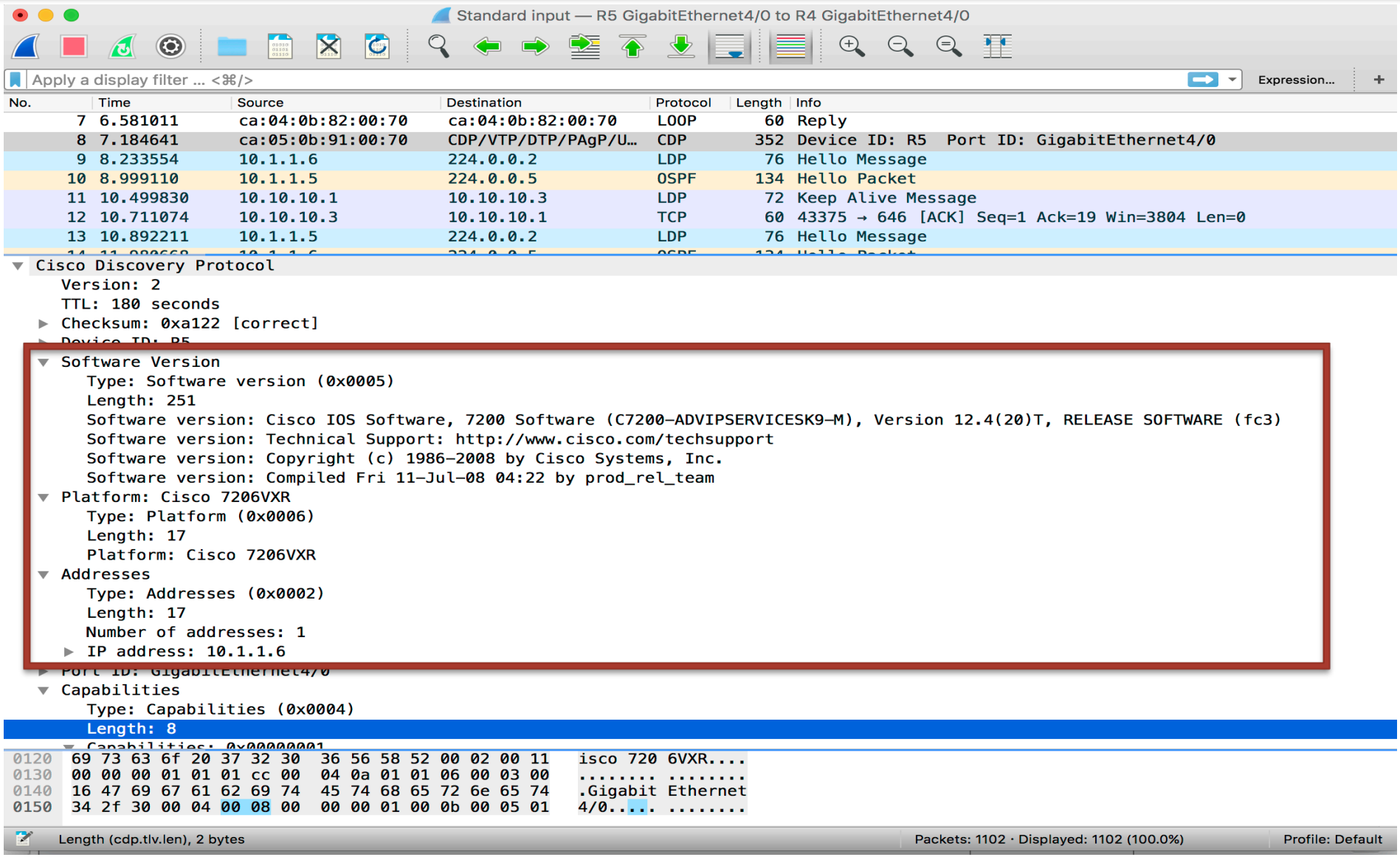
Cisco Discovery Protocol (CDP)



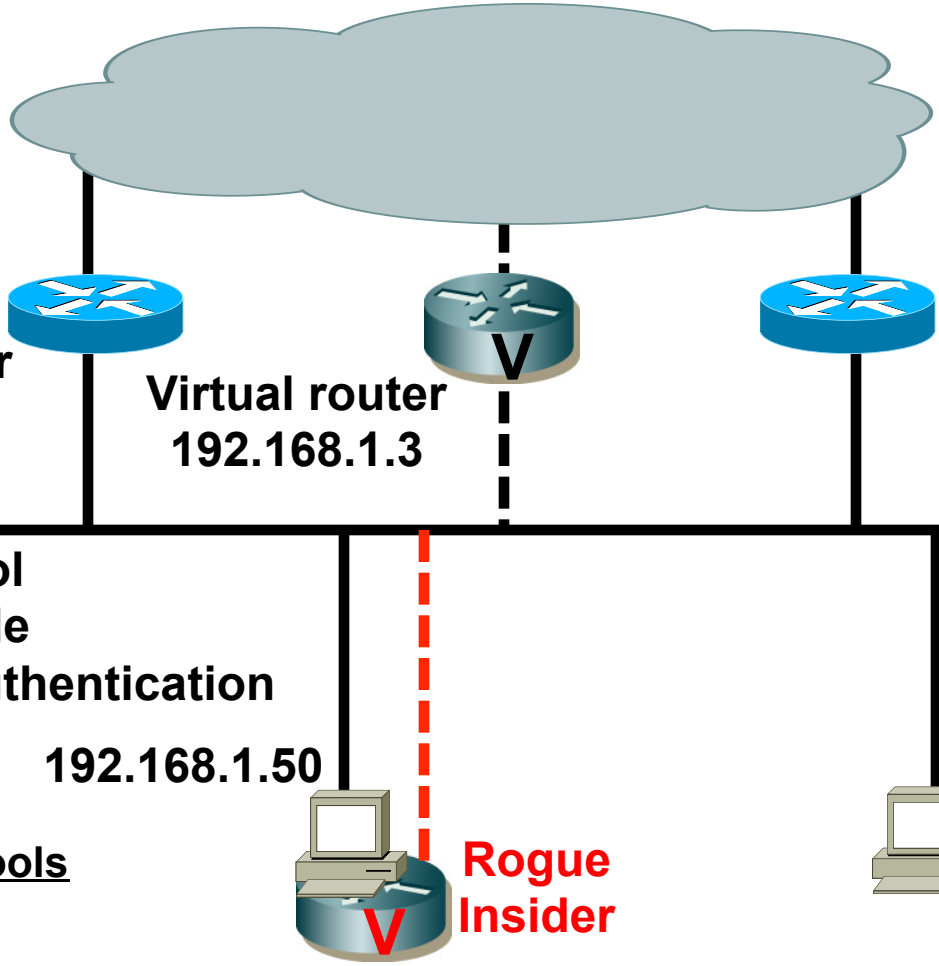
Cisco Discovery Protocol (CDP)

- 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!



First Hop Redundancy Protocols

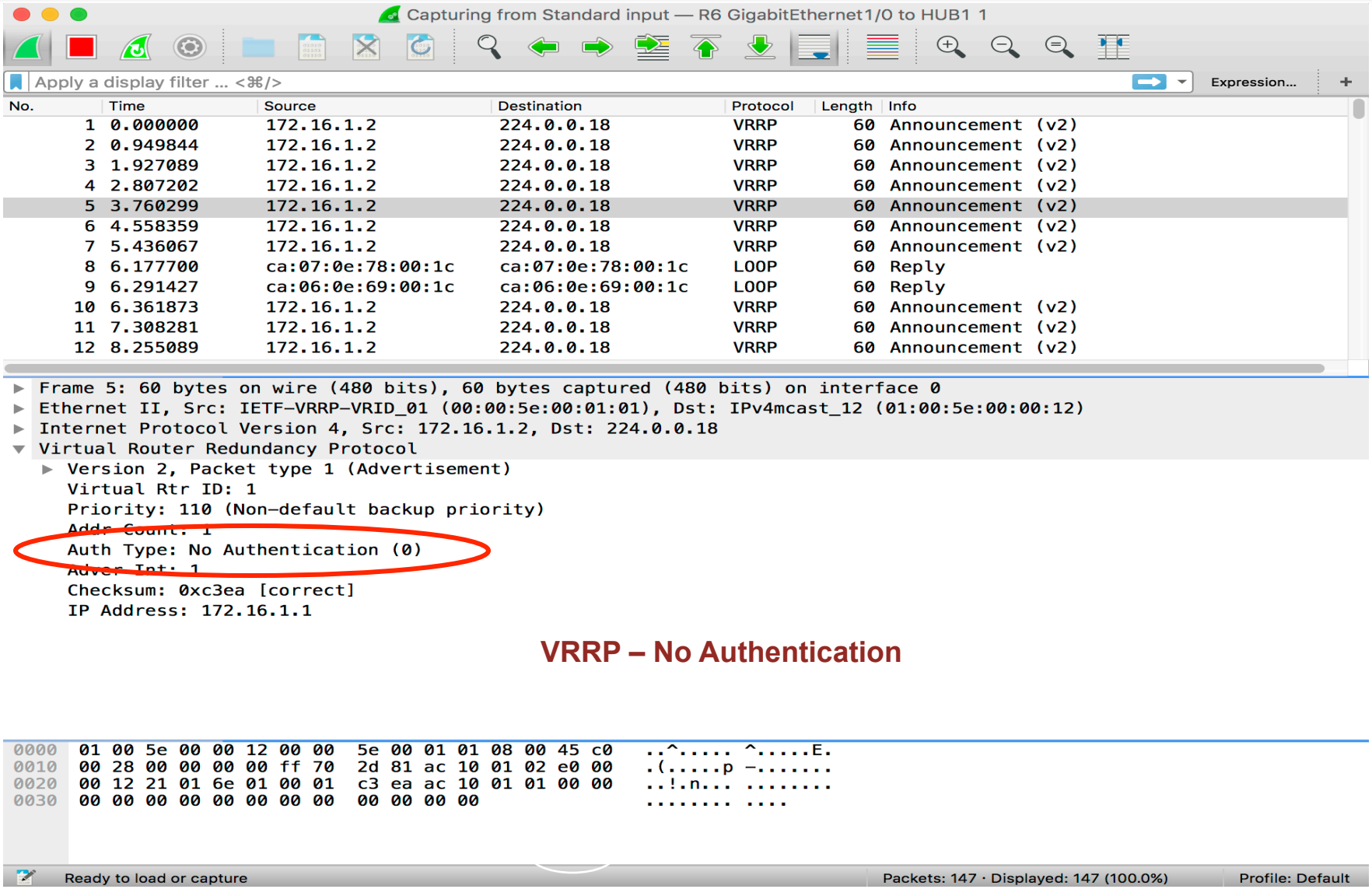


Protocol Hacking Tools

GSN3
SCAPY
Colasoft Packet Builder
Many others…
(Remember to enable IP forwarding)

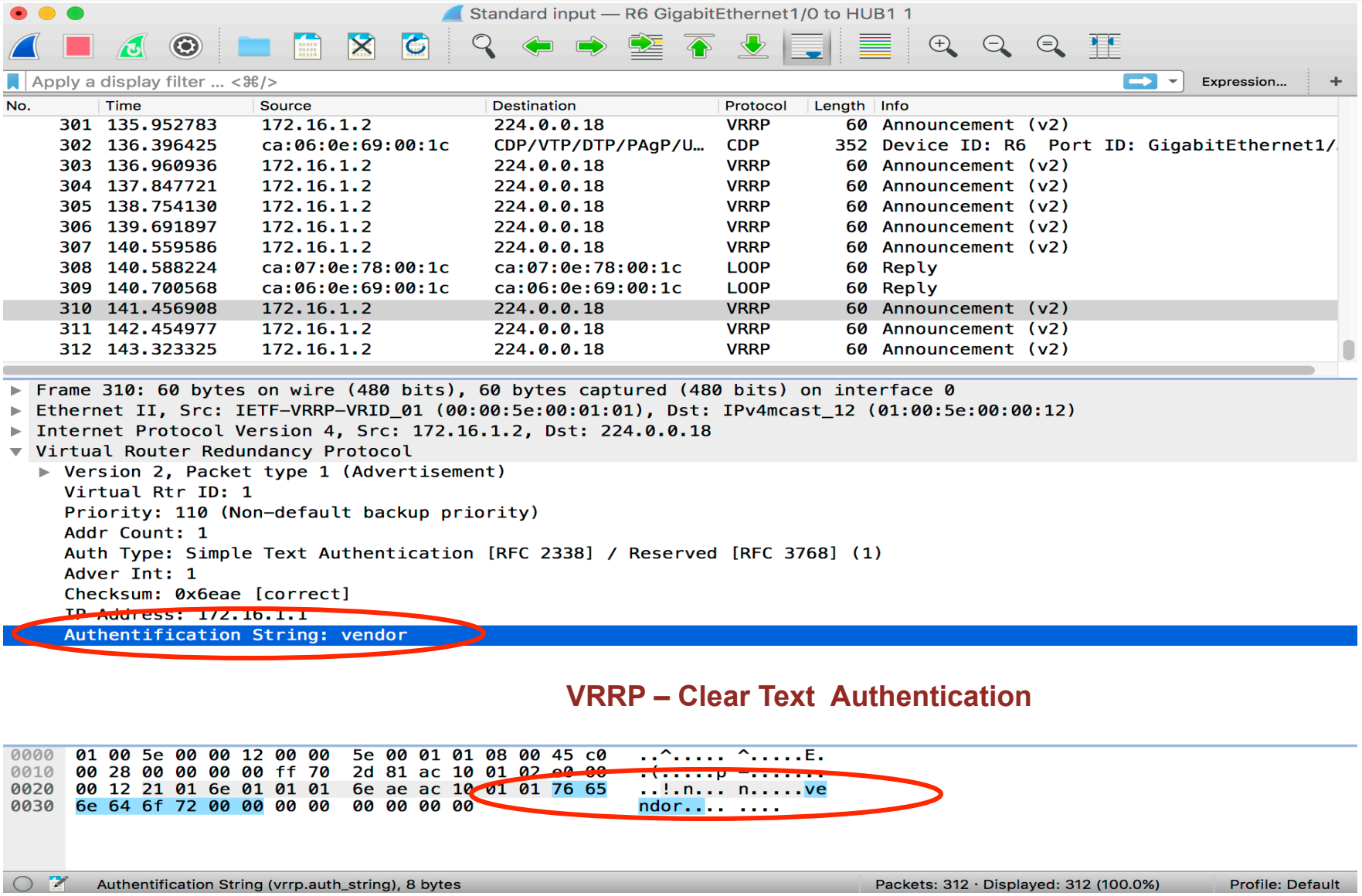
Global Load Balancing Protocol (GLBP)
Hot Standby Router Protocol (HSRP)
Virtual Redundant Router Protocol (VRRP)

VRRP – No Authentication

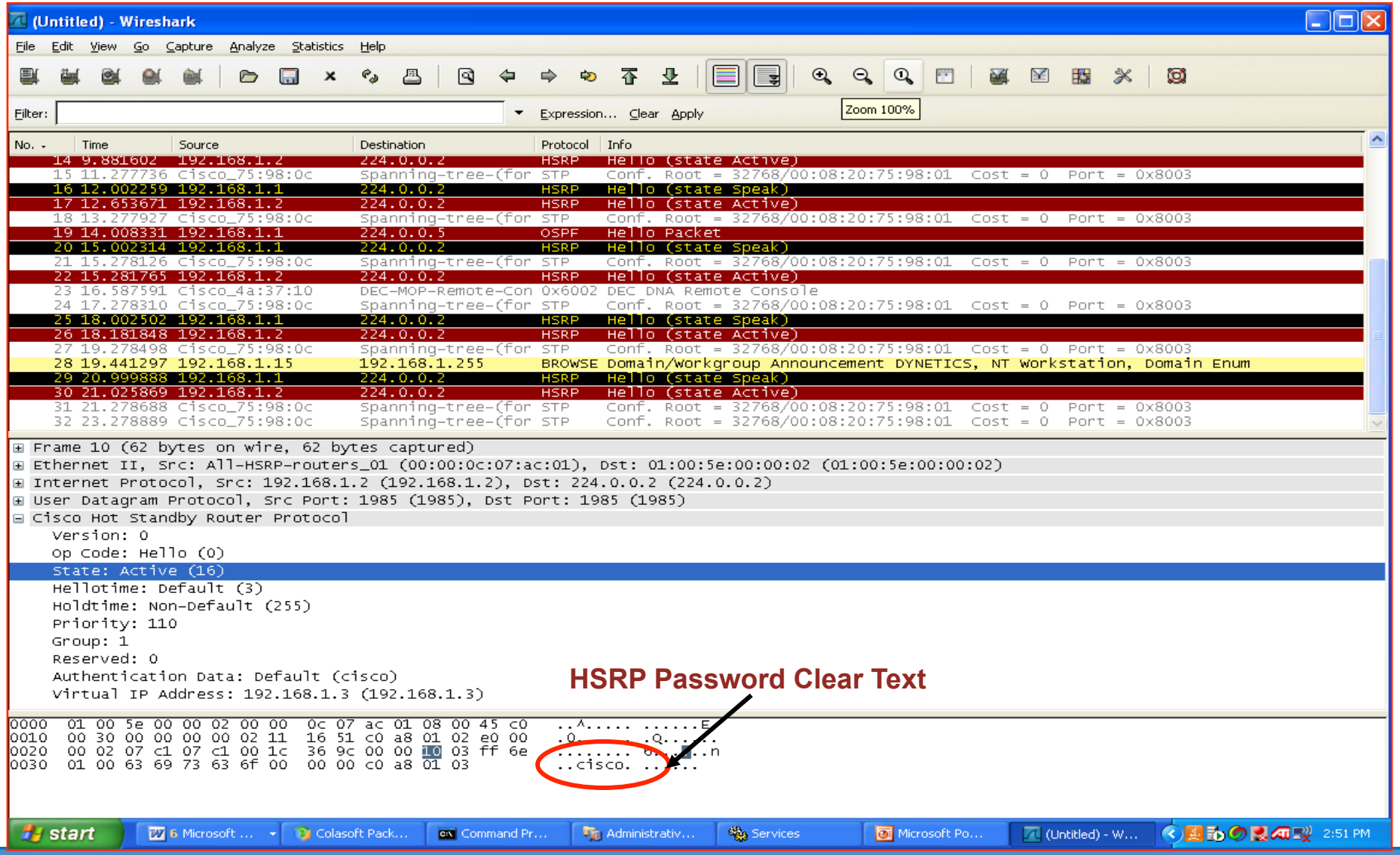


VRRP – No Authentication

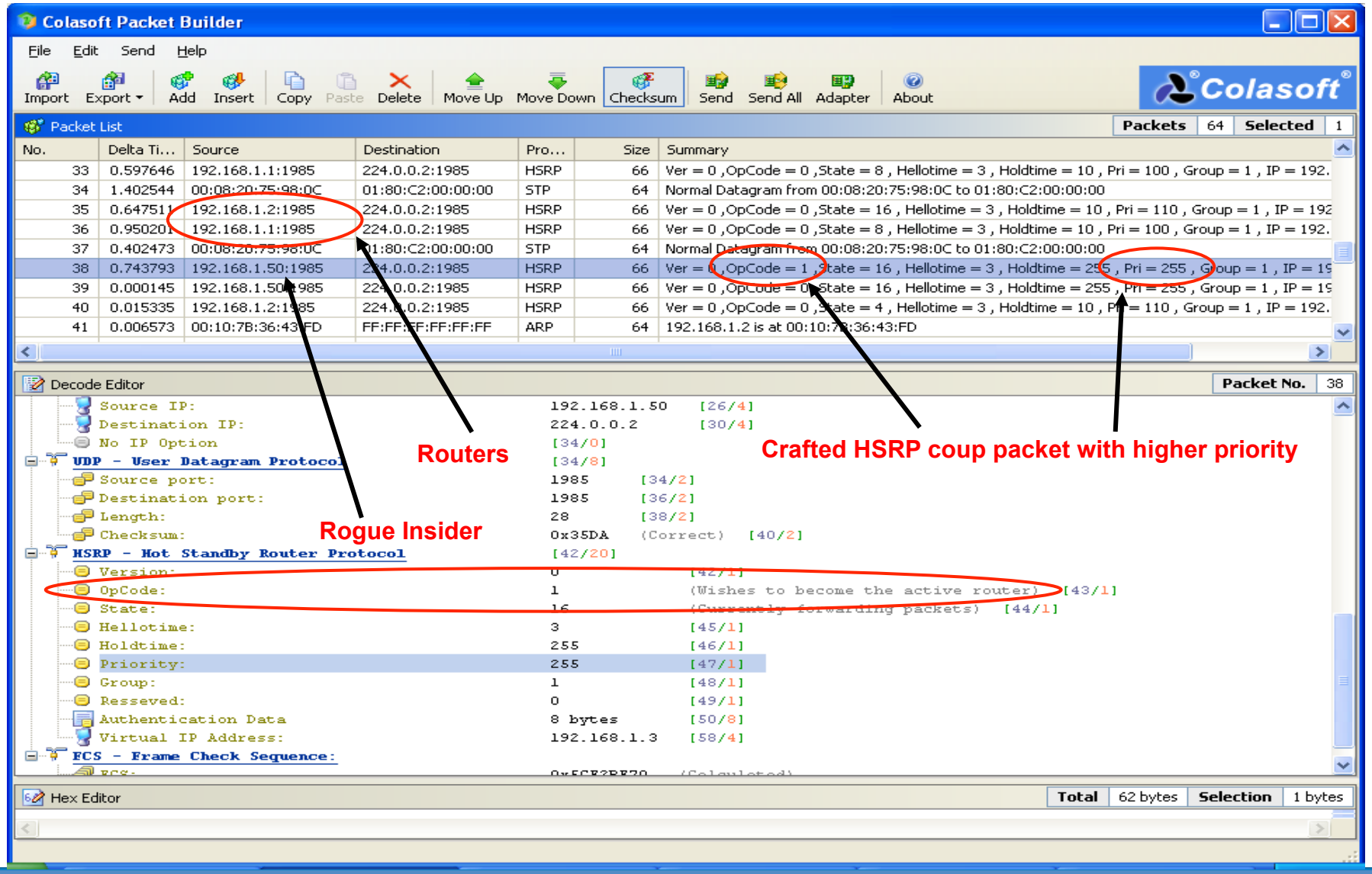
VRRP – Clear Text Authentication



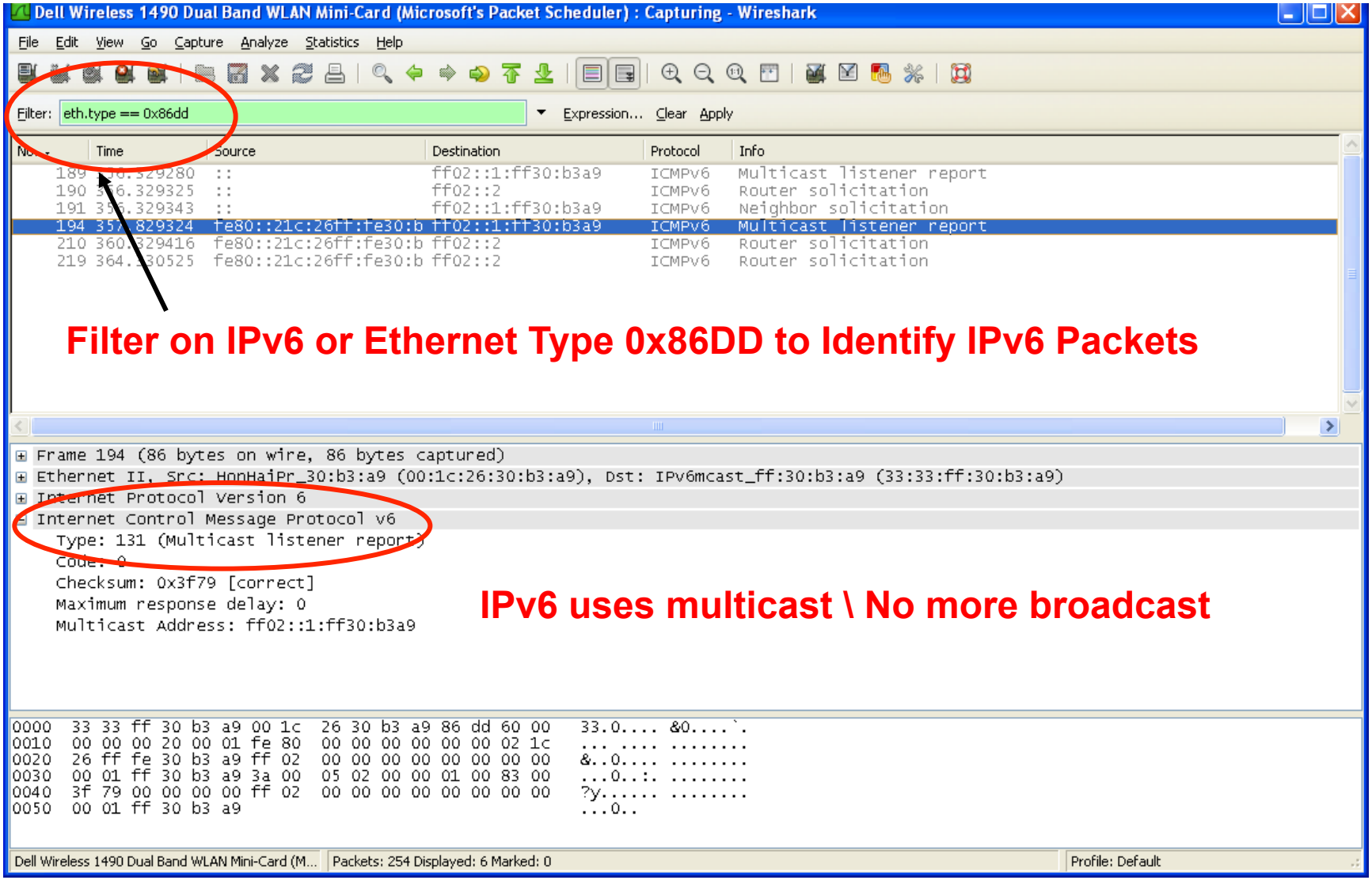
HSRP MITM – Packet Analysis



FHRP – Crafted HSRP Packets



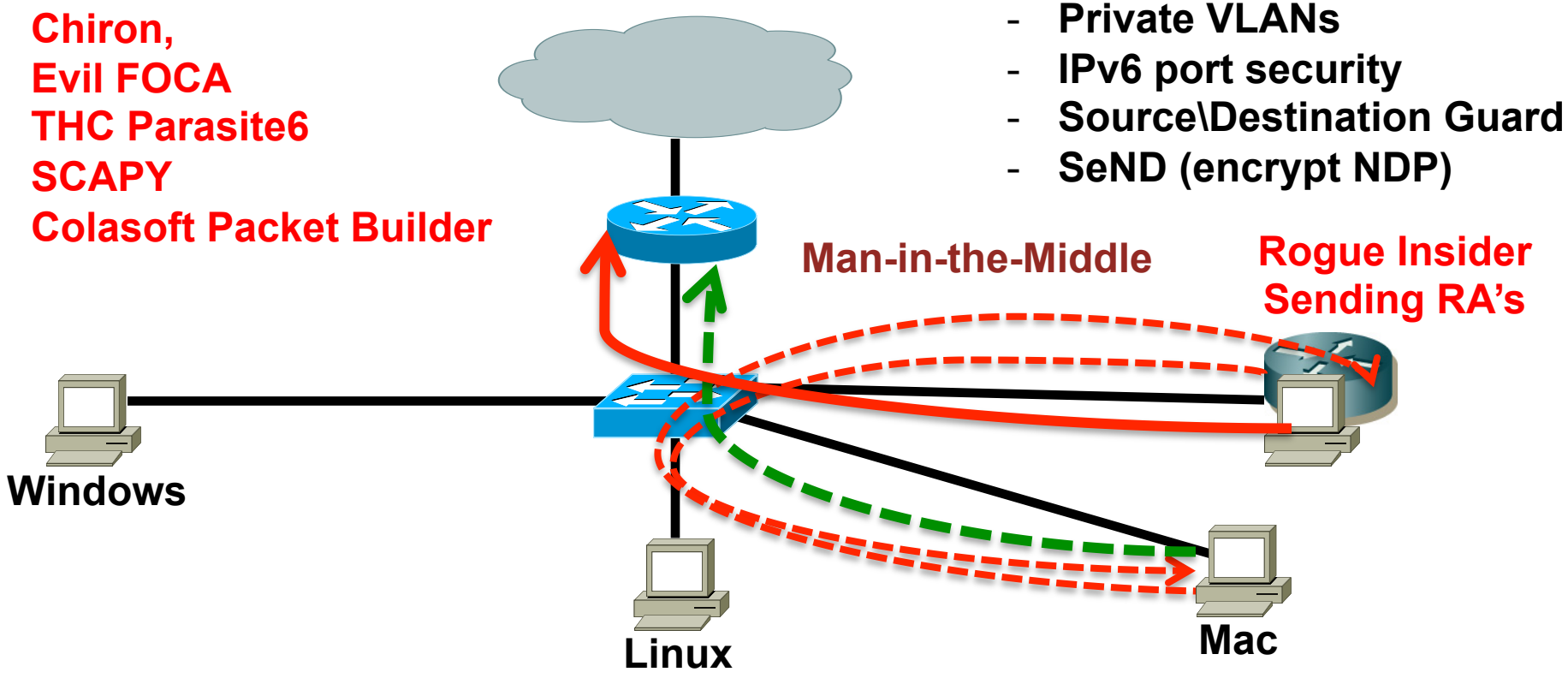
IPv6 Neighbor Discover Protocol



IPv6 SLACC MITM

IPv6 Neighbor Discovery Protocol (NDP)
(Think ARP for IPv6)
IPv6 MITM Tools
- **Chiron,**
- **Evil FOCA**
- **THC Parasite6**
- **SCAPY**
- **Colasoft Packet Builder**

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



Default - Hosts Send ICMPv6 Router Solicitation

IPv6 Network Discovery Spoofing MITM

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

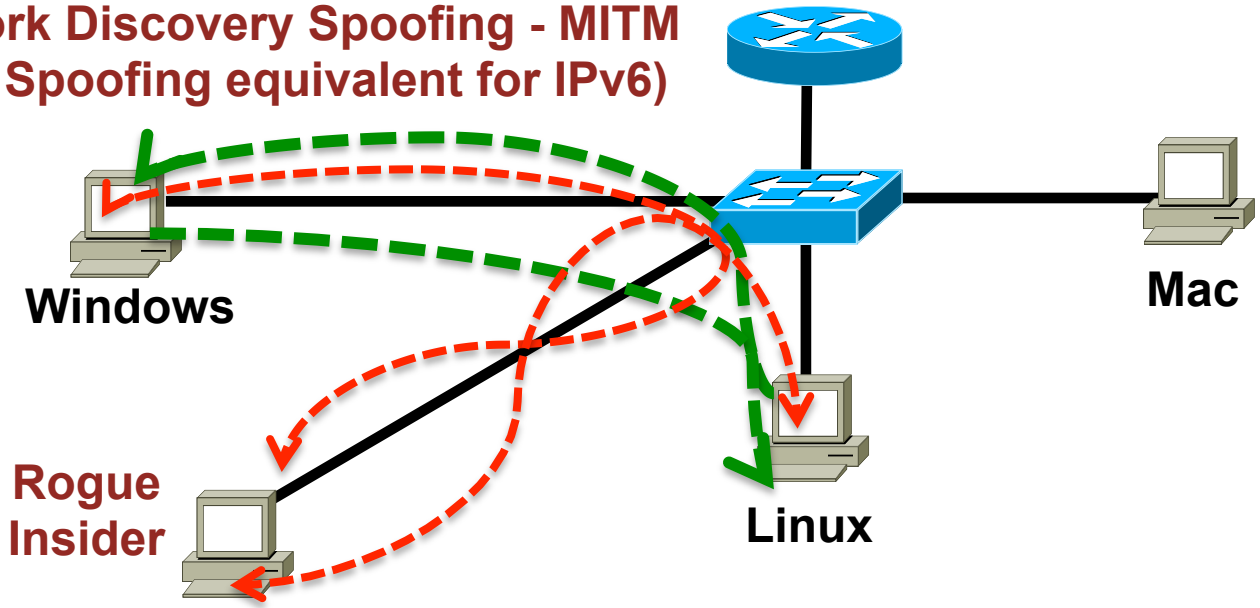
IPv6 MITM Tools

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

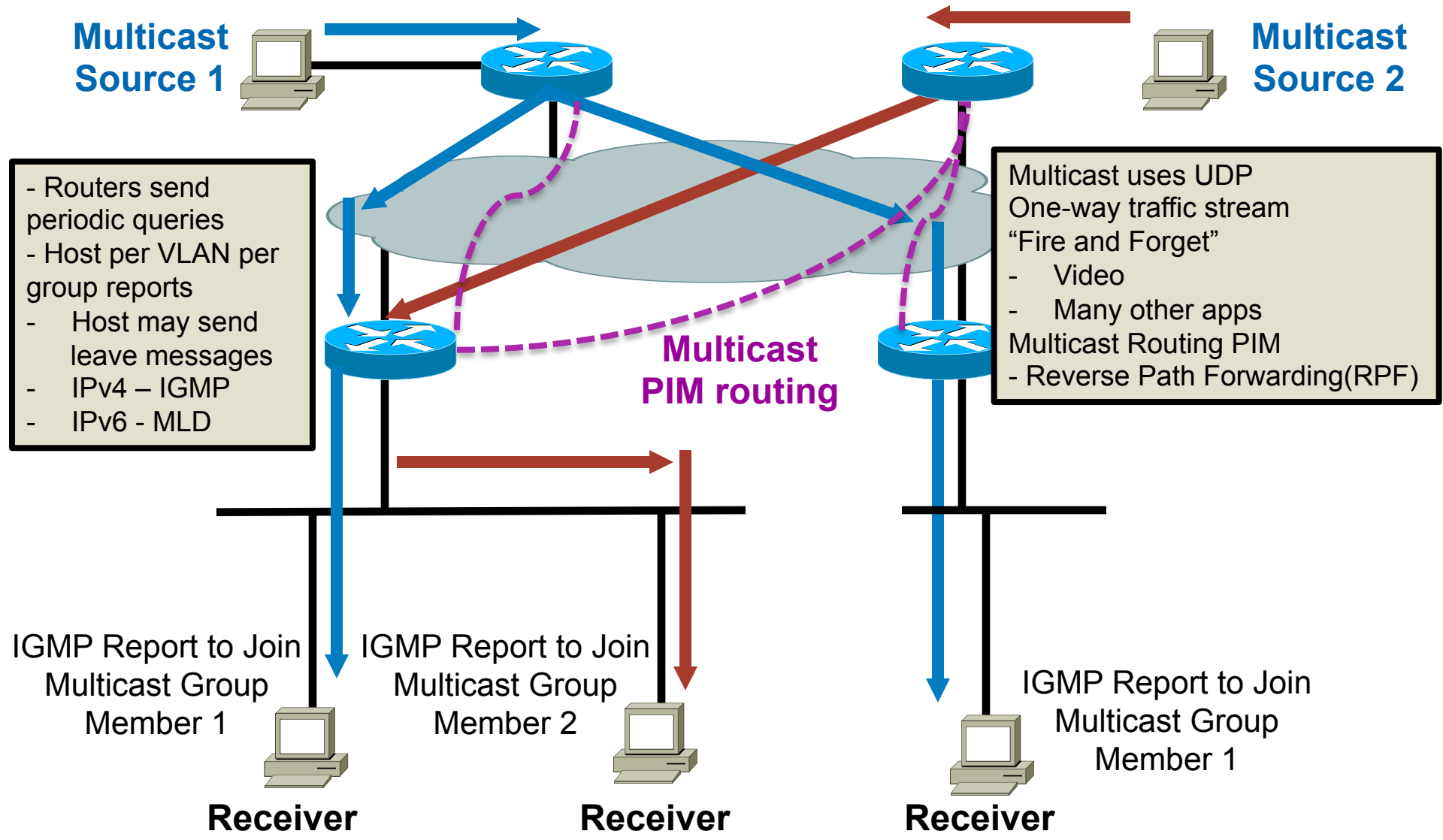
Mitigations

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

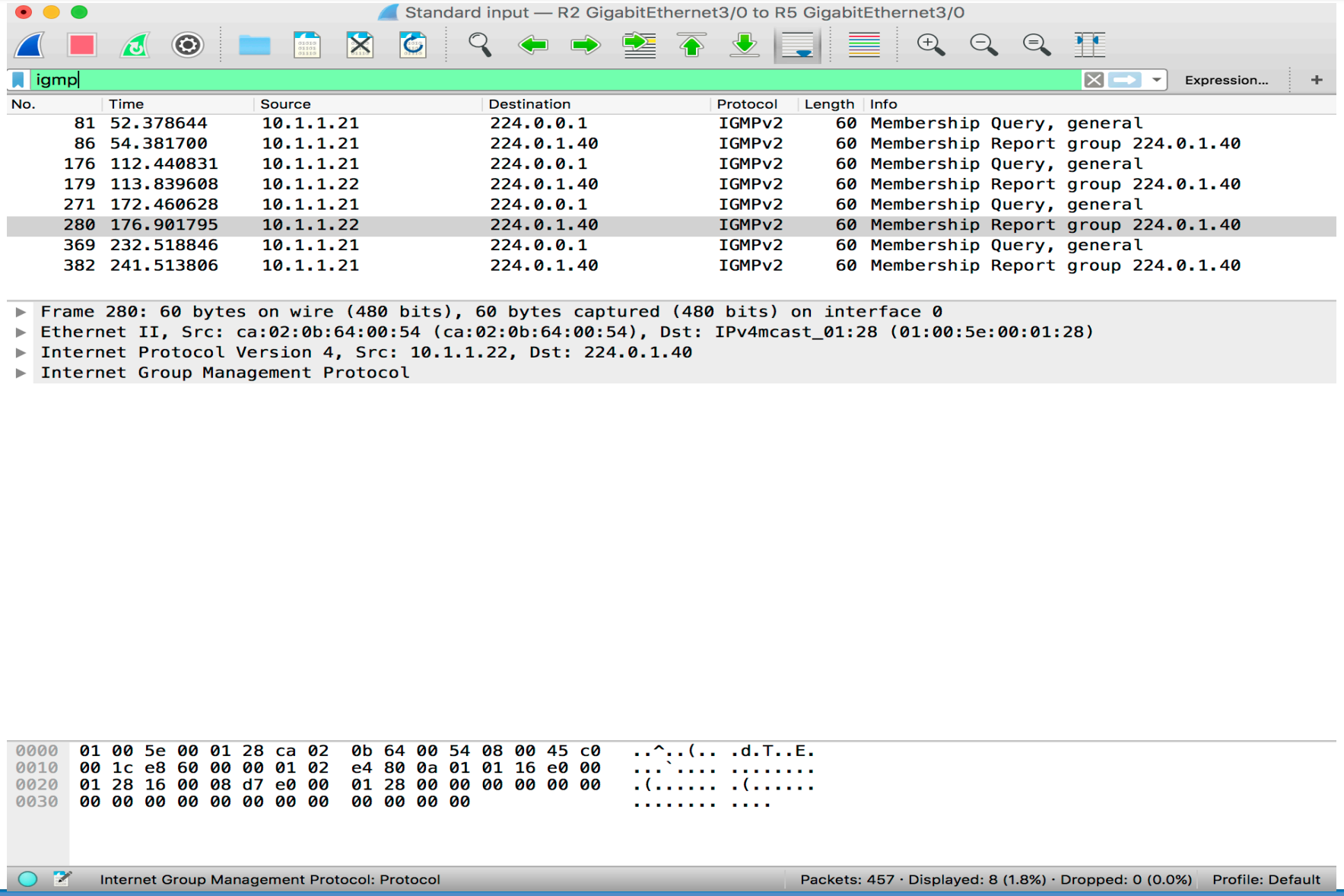
Network Discovery Spoofing - MITM
(ARP Spoofing equivalent for IPv6)



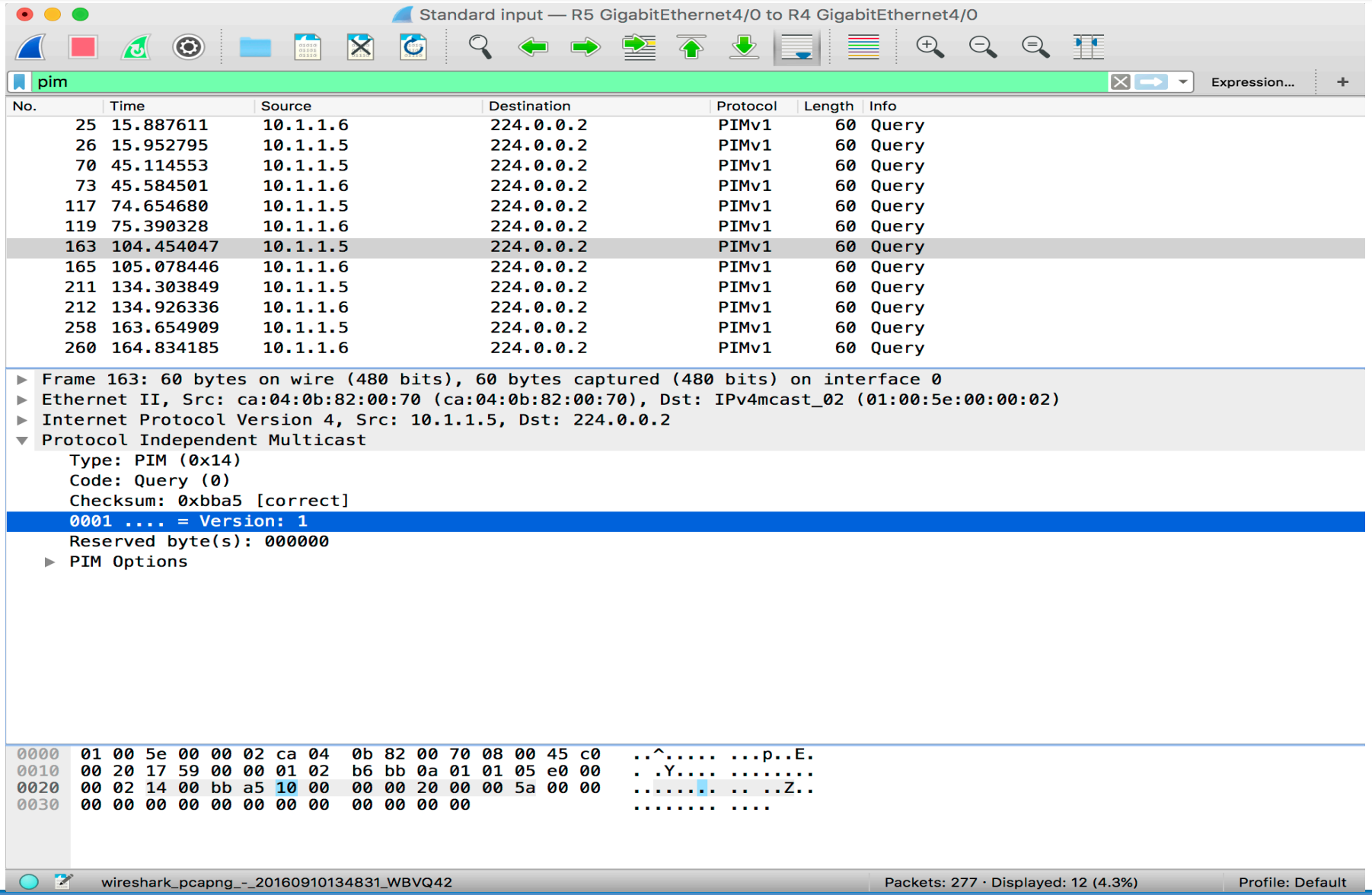
Multicast Overview



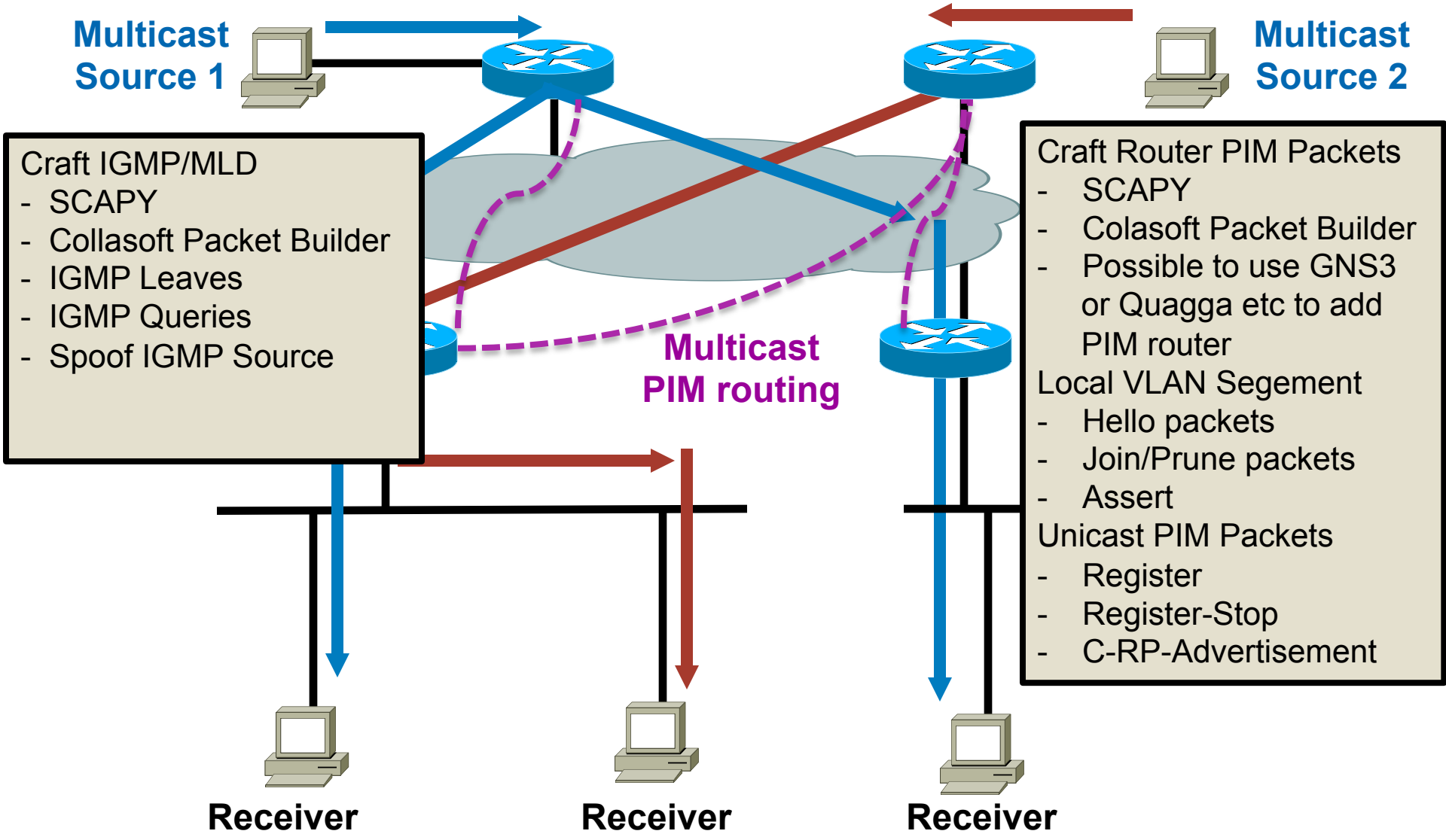
Multicast - IGMP



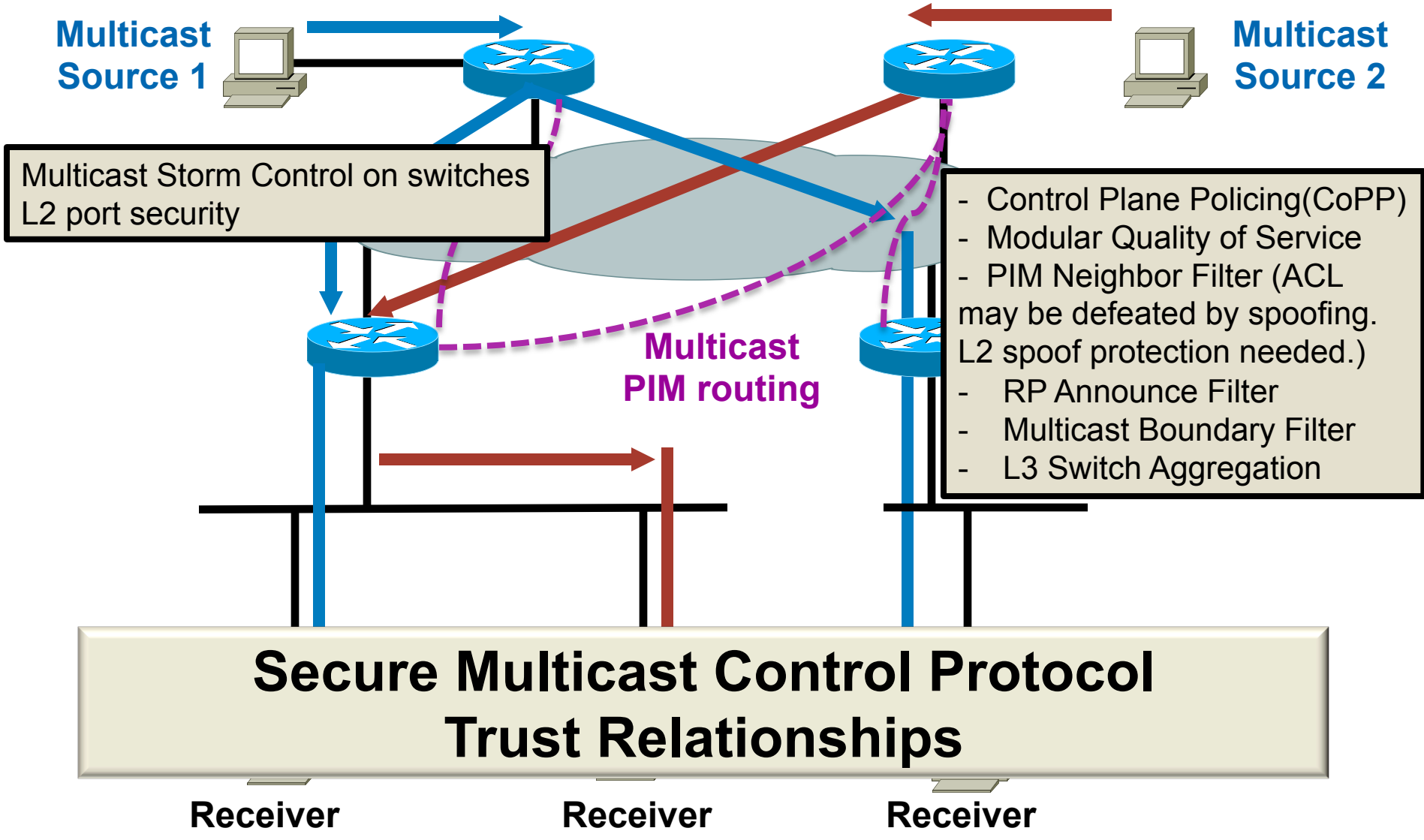
Multicast Routing - PIM



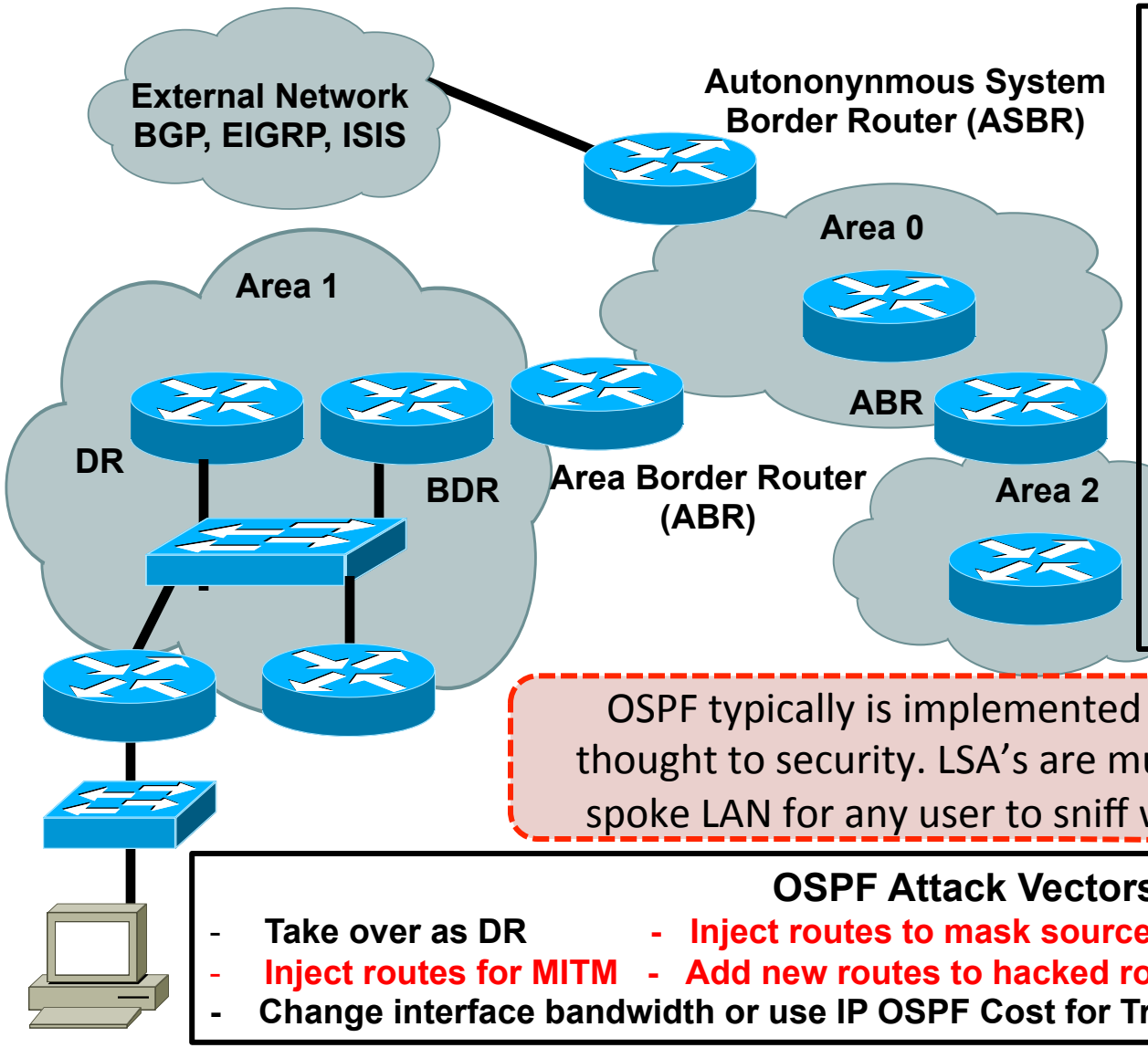
Attacking Multicast



Securing Multicast



Hack the Network via OSPF



OSPF Exploit Tools

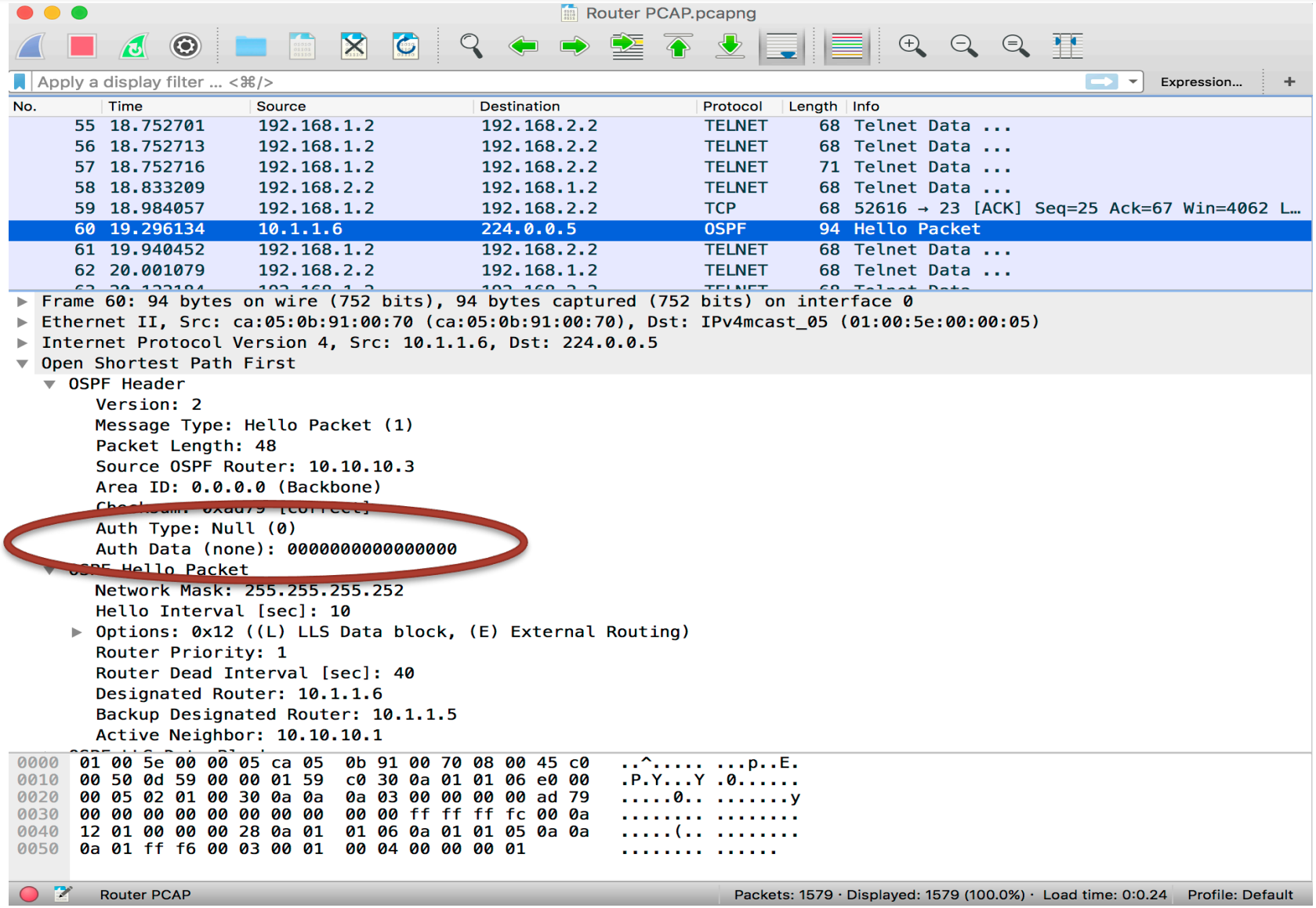
- Quagga
- NRL Core(Network Simulator)
- Nemesis
- Loki
- GSN3\Dynamips
- Buy a router on eBay
- Hack a router and reconfigure
- Code one with Scapy
- IP Sorcery(IP Magic)
- Cain & Able to crack OSPF MD5
- MS RRAS
- NetDude
- Collasoft
- Phenoelit IRPAS

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

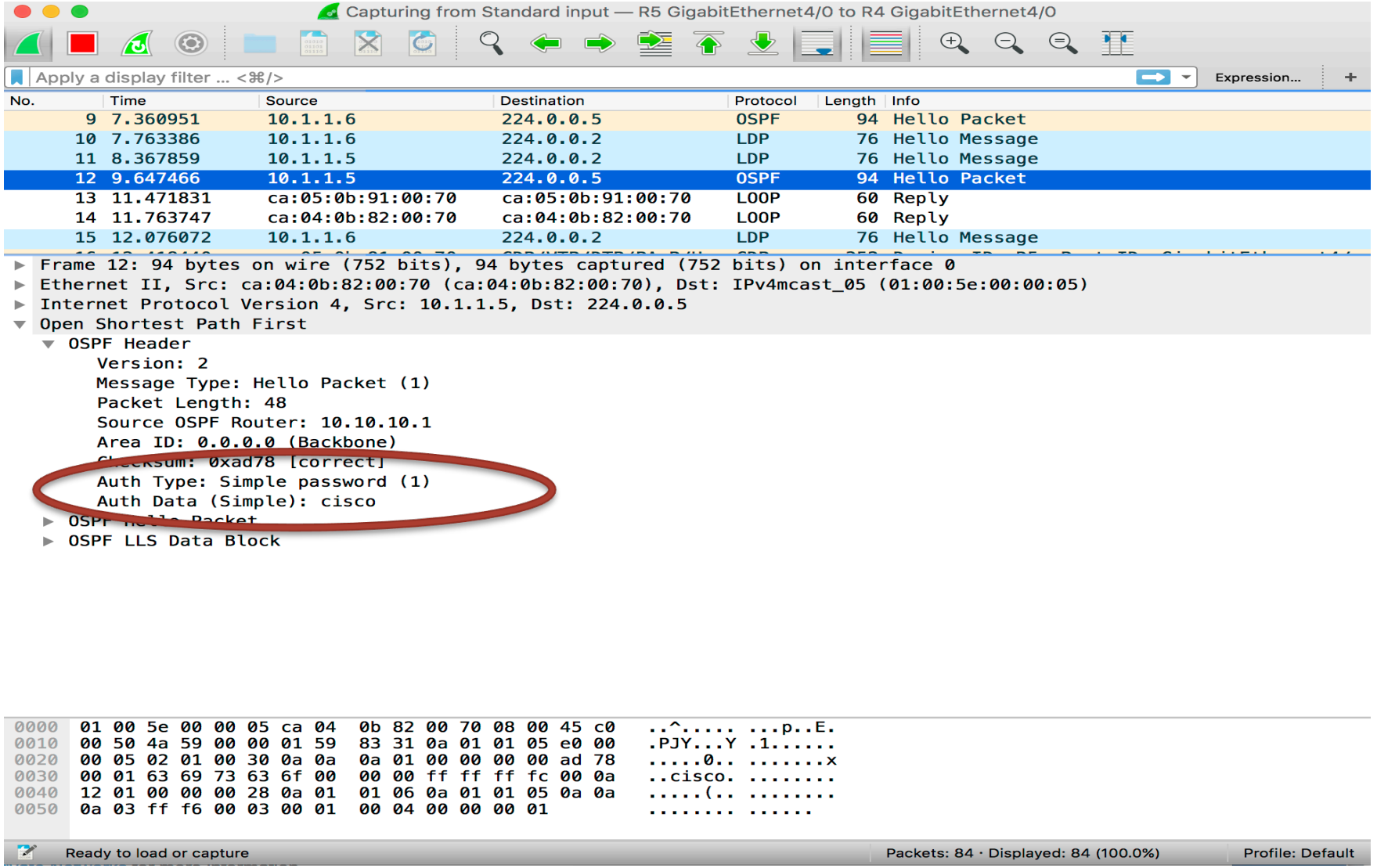
OSPF Attack Vectors

- 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

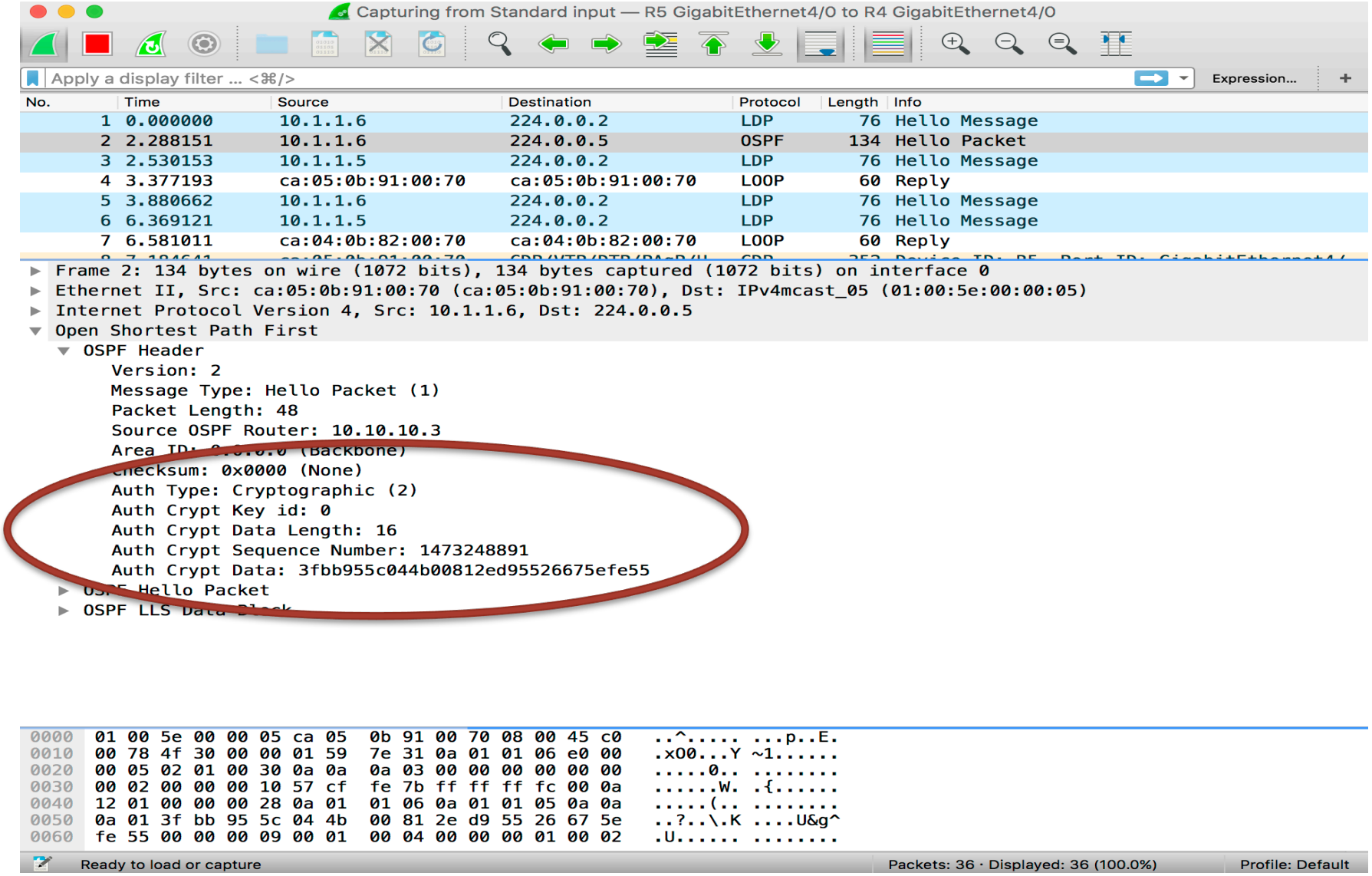
OSPF – No Authentication



OSPF – Clear Text Authentication



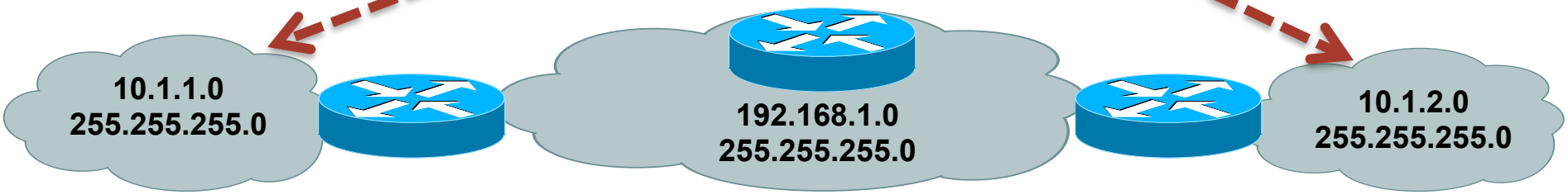
OSPF – MD5 Authentication



EIGRP Overview

- Advanced Distance Vector – “Hybrid”
- No authentication / MD5 Authentication
- Classless \ Classful routing default
- Supports IPv4/6, IPX and Appletalk
- Fast convergence
  - Successor
  - Feasible Successor
- Unequal and equal cost load balancing
- Upgrade replacement for IGRP
- Incremental updates
- EIGRP uses DUAL algorithm
- Cisco proprietary
- 3 Tables similar to OSPF
  - Neighbor table
  - Routing table
  - Topology table
- Summarization at any interface in network

Remember to use “no auto-summary” command to enable classless routing or experience dis-contiguous network issues.

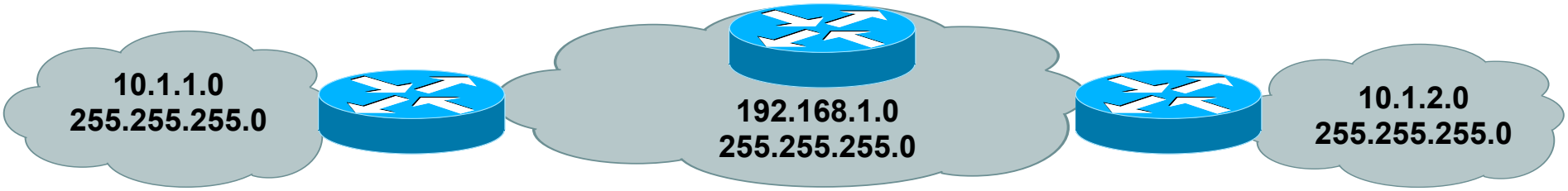


Hack the Network via EIGRP

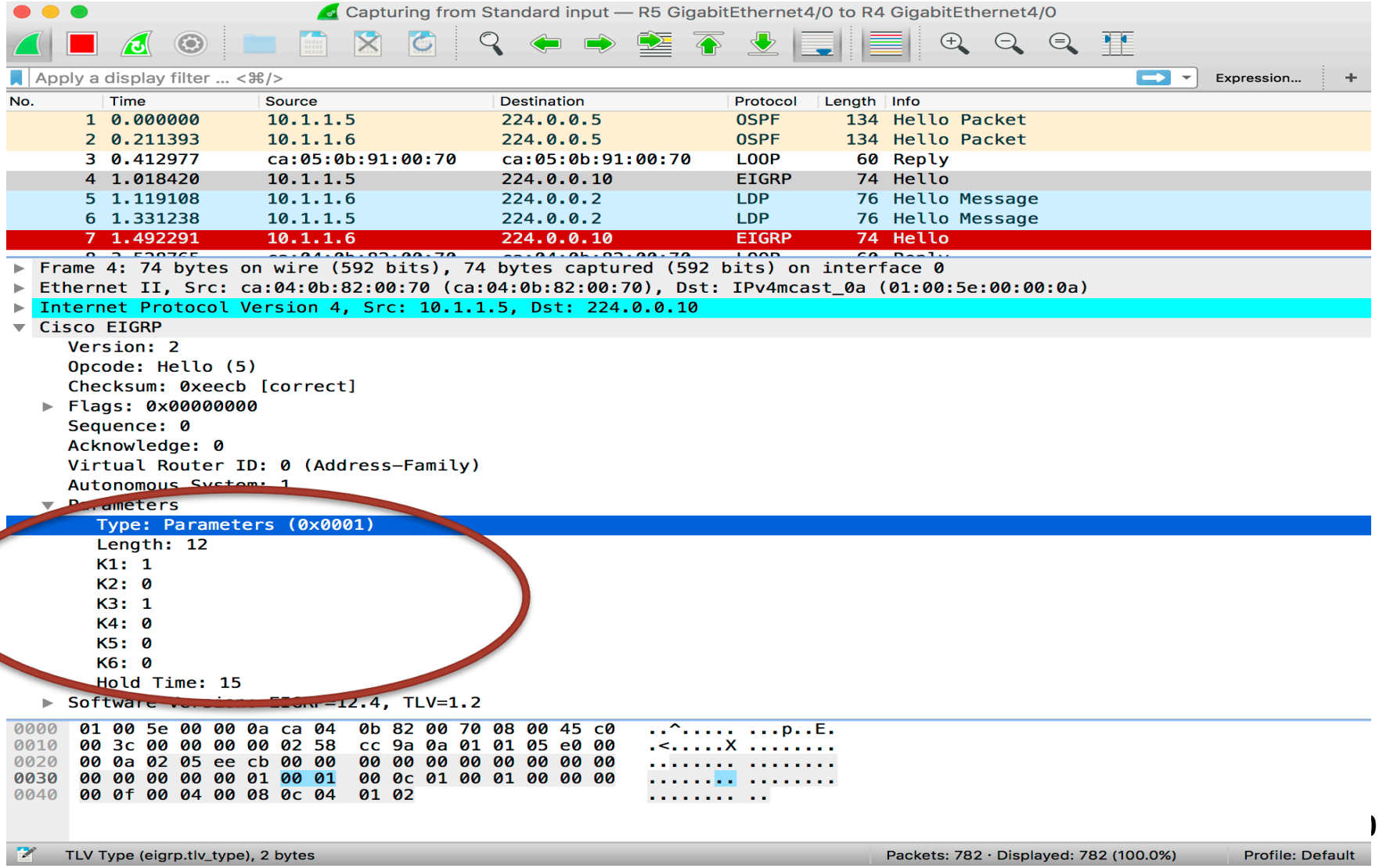
EIGRP Attack Vectors
- Inject routes to mask source of attack
- DoS
- Inject routes for MITM
- Add new routes to hacked router
- Change interface bandwidth for Traffic Engineering on hacked router

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

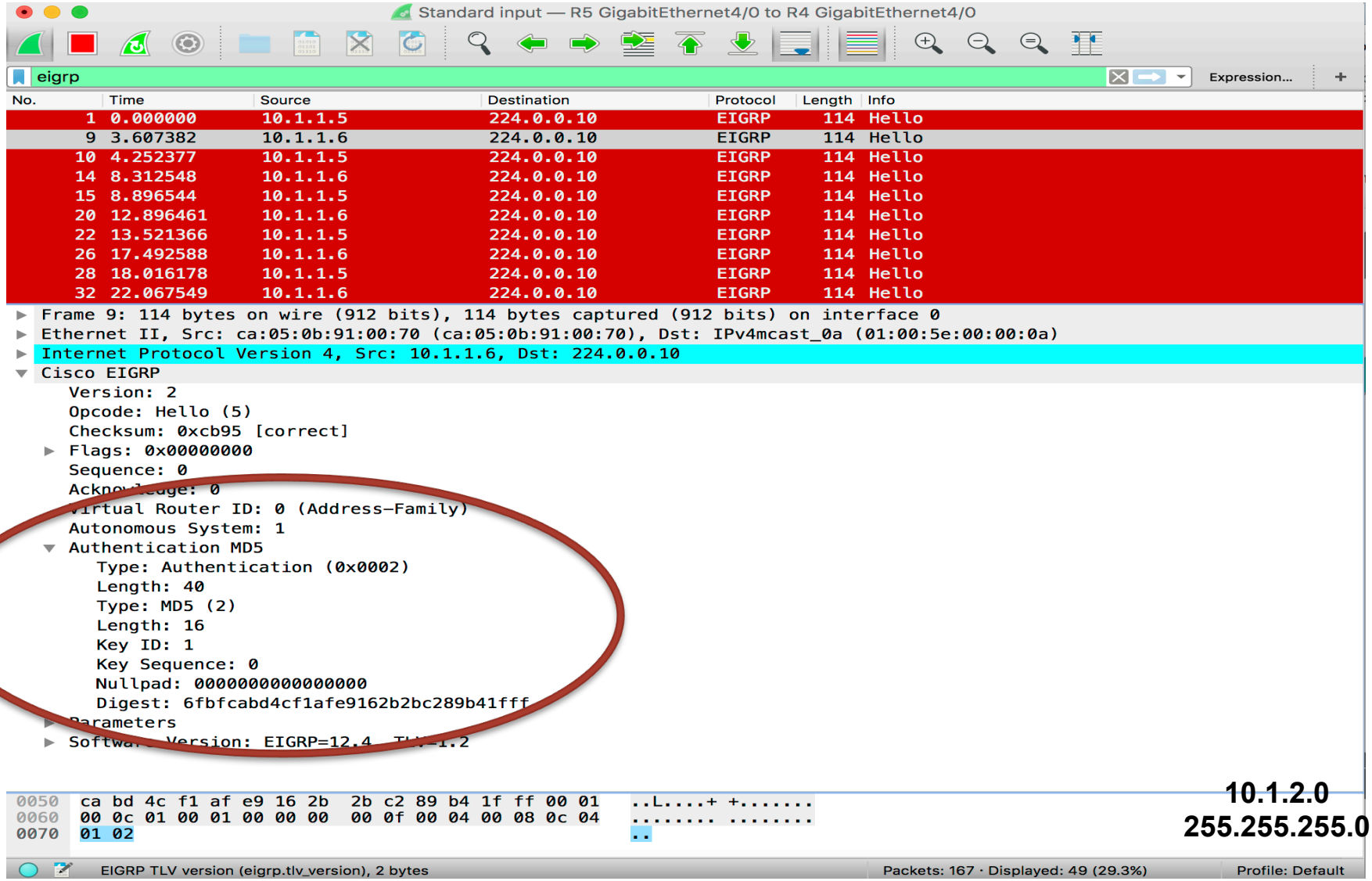
Similar to OSPF, EIGRP typically is implemented without any thought to security. Network administrators should use authentication and configure interfaces to be passive in EIGRP.



EIGRP – No Authentication



EIGRP – MD5 Authentication

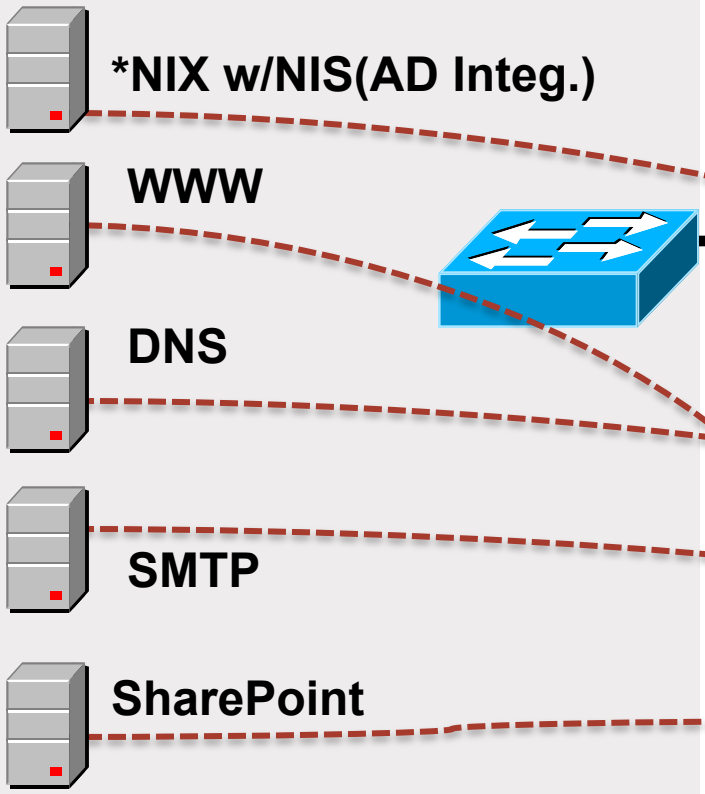


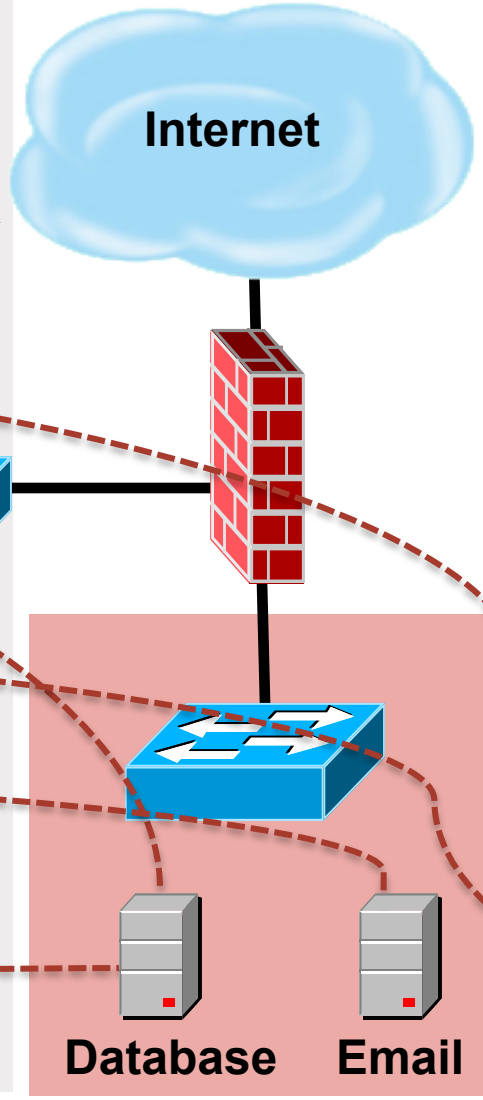
10.1.2.0
255.255.255.0

DMZ Layer 2 Security

DMZ

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

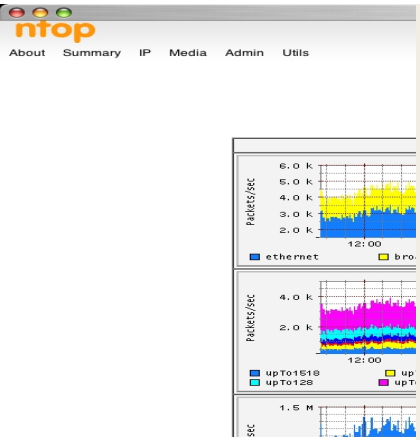


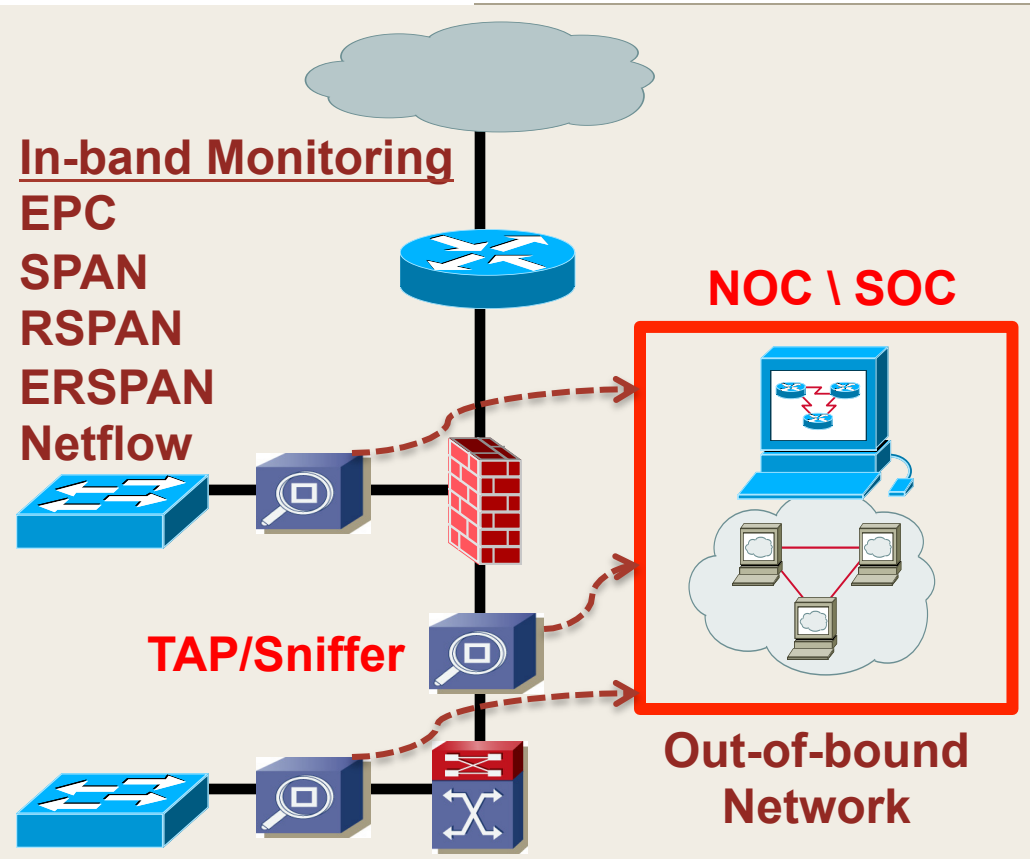


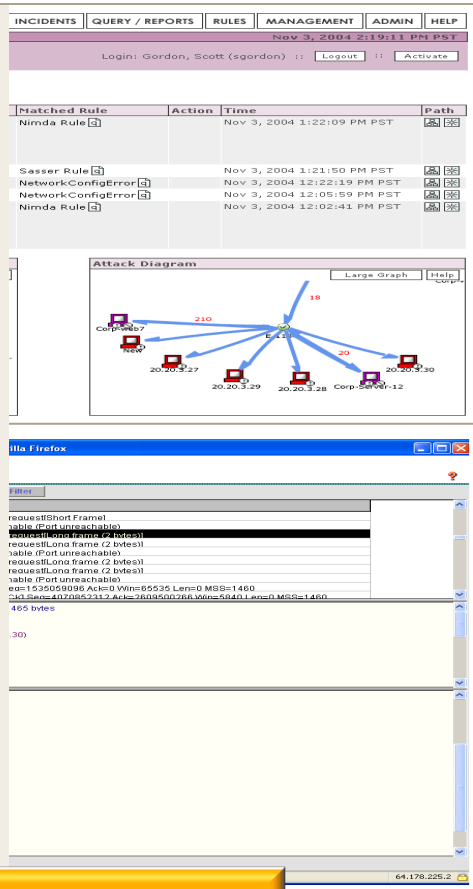
Secure DMZ Trusts

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

Layer 2 – Secure Visualization and Instrumentation







Whitelist the Layer 2 Network Trust Relationships

Whitelist Trusted Information Flows in Monitoring

Secure Control, Management, Data Planes

References

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 PepeInjak - @IOShints, Papers and Resources, http://www.ipspace.net

IPv6 Security, Scott Hogg and Eric Vyncke, Cisco Press

IPv6 Security, Scott Hogg,
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/fhp-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

Questions?

@PaulCoggin