Becoming a Hacker

Breaking Networks

Chris McCoy
cmm@cisco.com
ASIG

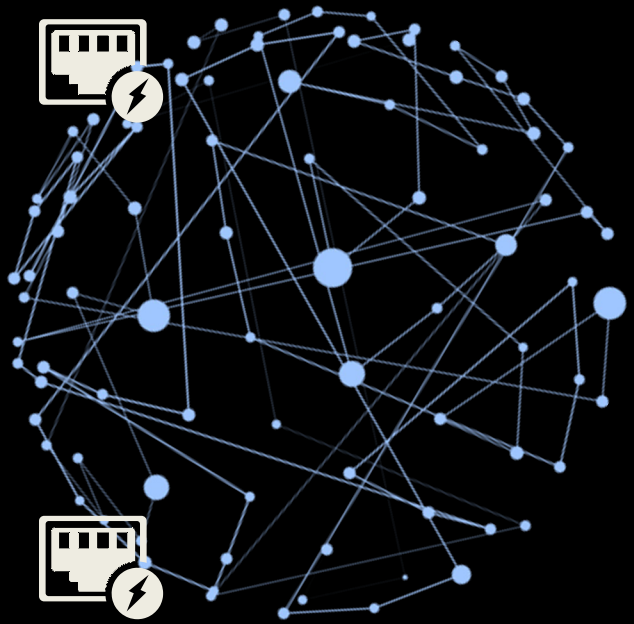
Everett Stiles
evstiles@cisco.com
ASIG

Nicholas Weigand
nweigand@cisco.com
ASIG

Agenda

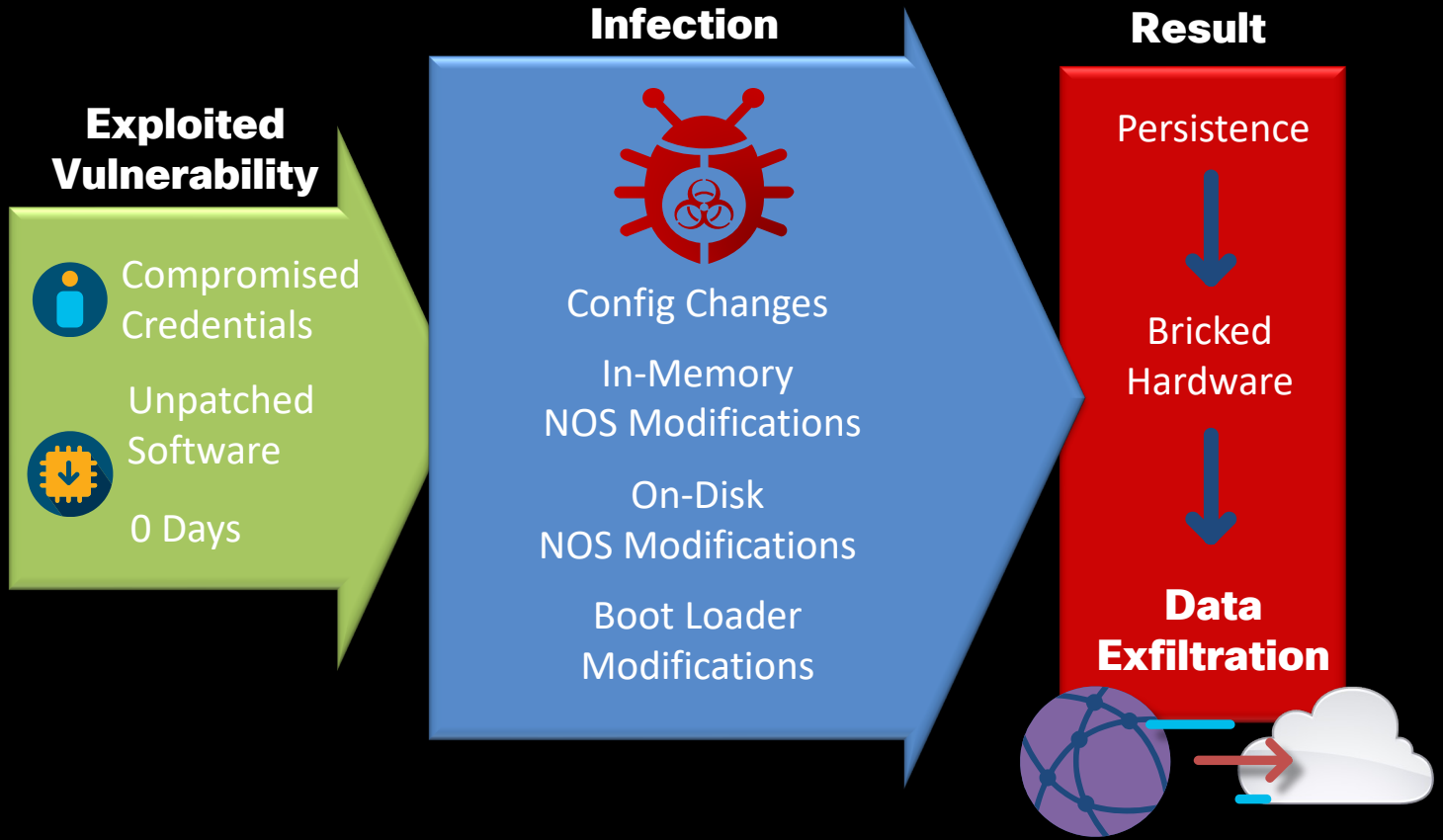
- Why hack networks?
- ARP and ICMP Redirects
- First Hop Redundancy Protocols
- Routing Protocols
- Management Protocols
- Denial of Service Attacks using DNS & NTP Amplification
- Tools for packet decoding
- The “Swiss-Army-Knife” of packet crafting - Scapy!
- Use newly acquired skills to break into a router

Why Hack Network Devices?

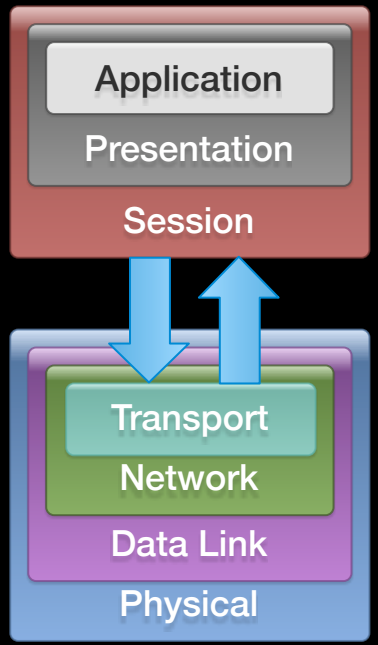


- Core of the Network
- May not be monitored as closely as hosts
- Longer system life cycle
- No malware detection
- Antiquated protocols - configurations tend to stay static
- Routers and switches have features such as port mirroring, tunneling, and lawful intercept to infiltrate and exfiltrate data
- Some devices even have built-in analysis tools such as Wireshark

Steps to Owning a Network

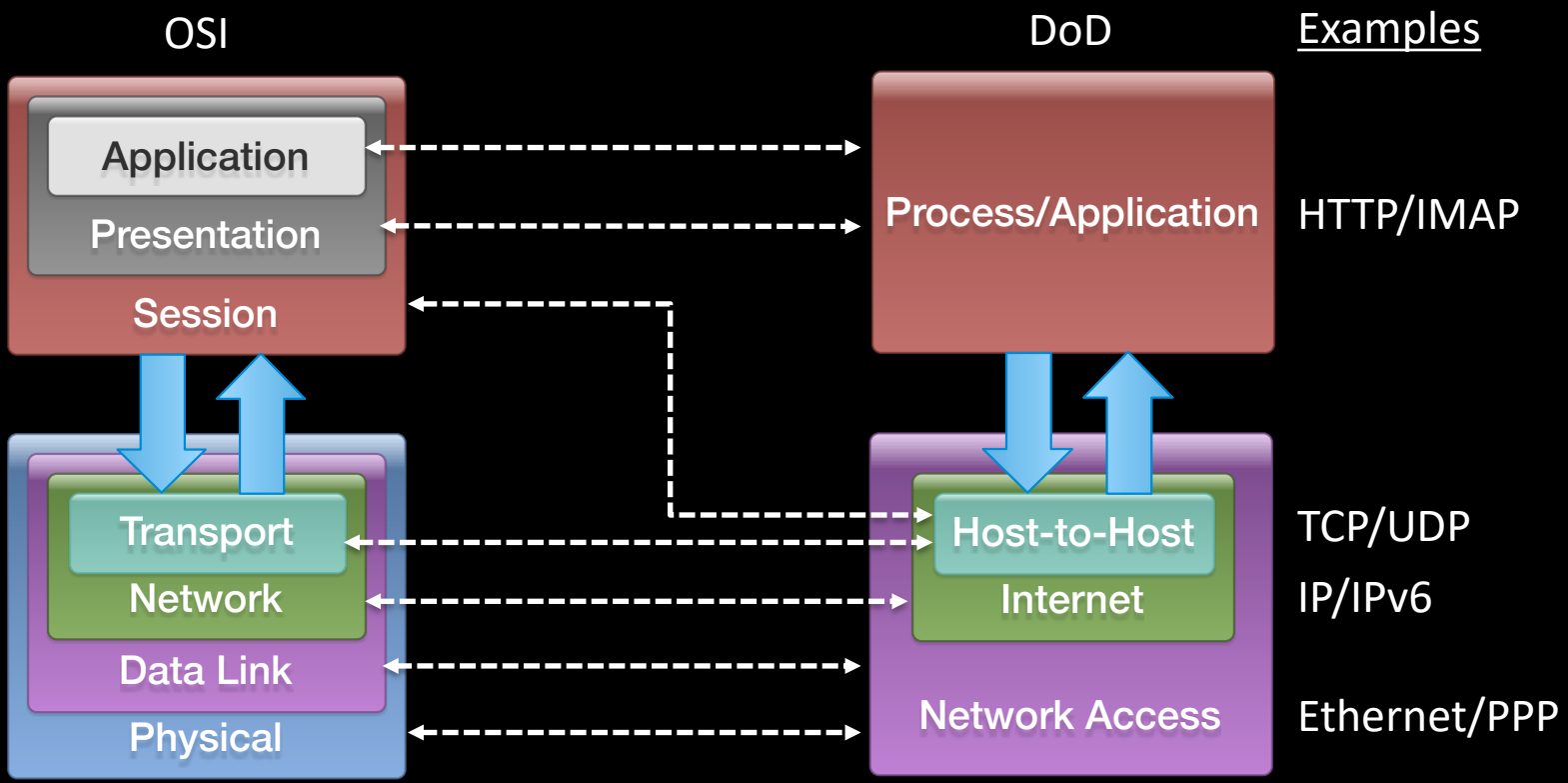


Layers of the Internet (OSI Model)

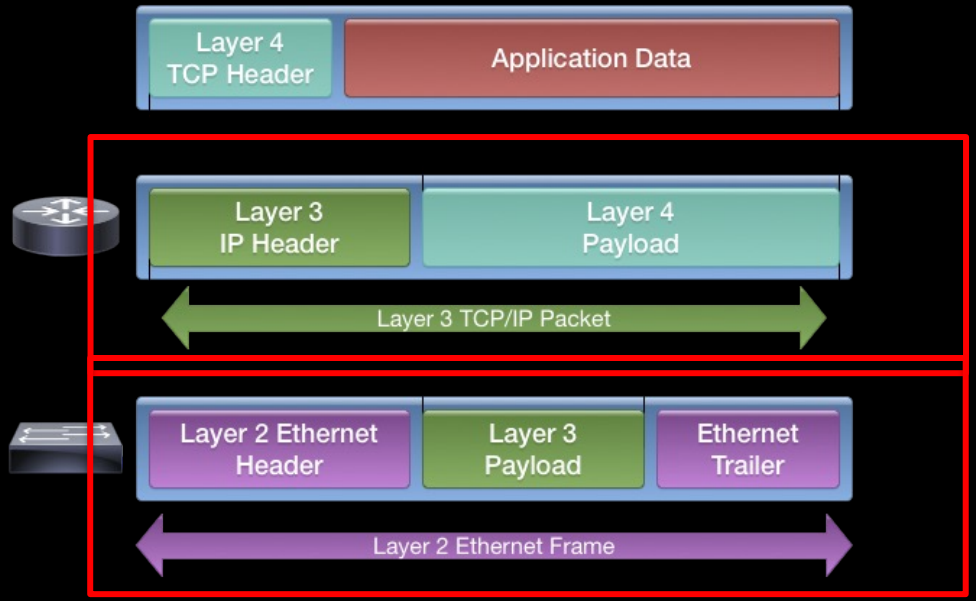


- Protocol: Formal rules of communication
- Internet Protocol suite is standardized by the Internet Engineering Task Force (IETF)
- These protocols are arranged in layers (“stack”) to make it easier to replace one without affecting the other layers below or above
- Units of data have different names depending on the layer of OSI currently referenced

OSI vs. DoD Internet Model



Defining Terms

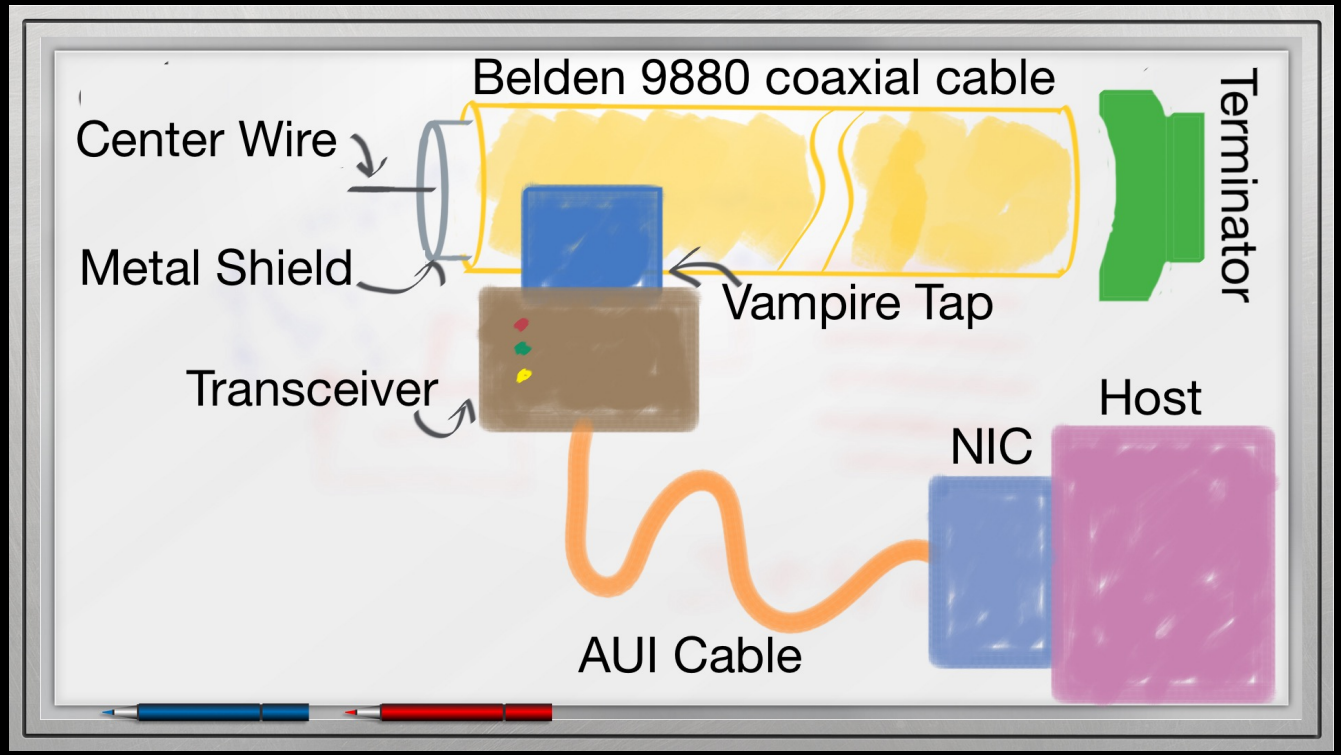


- Layer 3 Routers and Layer 2 Switches make forwarding decisions on how to handle units of data known as Packets and Frames
  - **Packets** are **Layer 3** encapsulated units of data
  - **Frames** are **Layer 2** encapsulated units of data

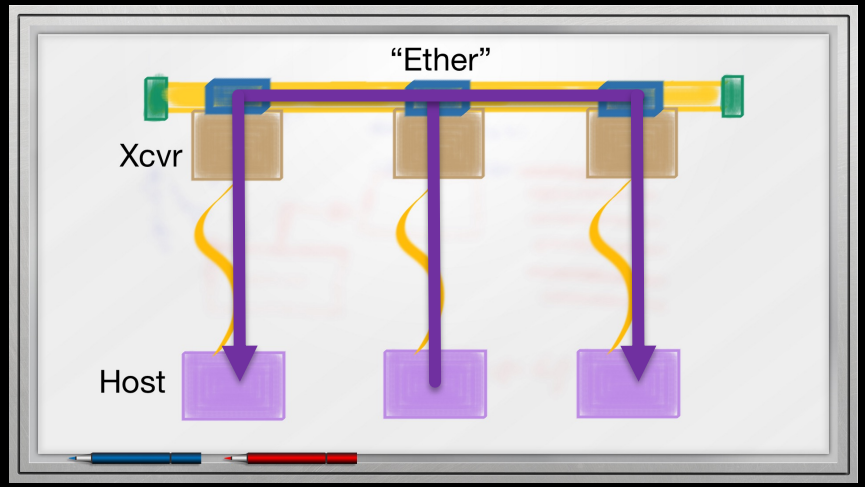
Ethernet

- Ubiquitous and popular LAN technology
- Invented at Xerox Palo Alto Research Center (PARC) in the 1970s. Operated at 3 Mbps
- Standardized in 1978 by Digital Equipment Corp., Intel and Xerox (*DIX*) and speed bumped to 10 Mbps
- Institute of Electrical and Electronics Engineers (IEEE) released a compatible version of the standard known as *802.3*

A Bit of History… 10Base5

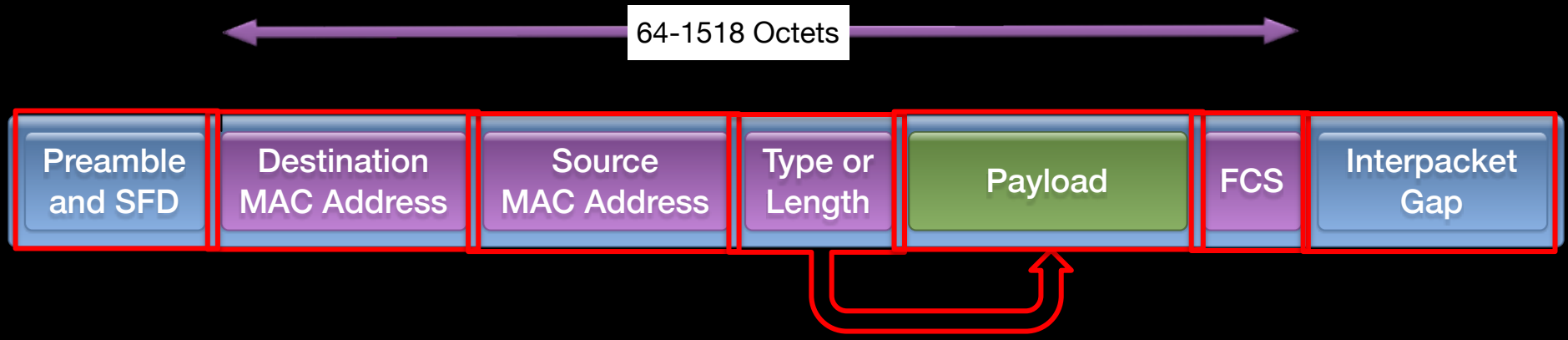


10Base5 LAN



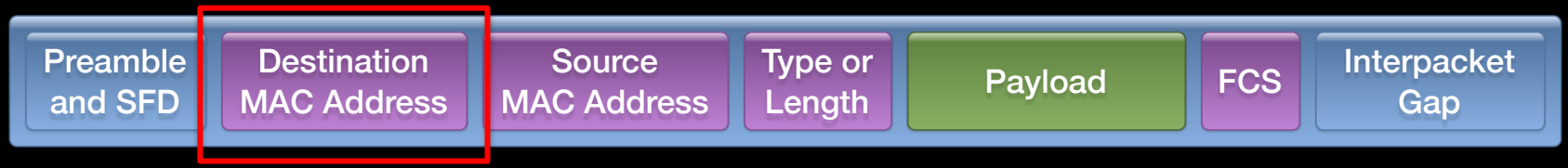
- **CSMA/CD**
- **Broadcast Multiple Access**
- **Half-duplex** (send or receive)
- Forms a **Collision Domain**
- Limited geographic distance and host count

Ethernet Frame



- **Octets** are units of 8-bits where **byte** may be ambiguous. We will use octets and bytes interchangeably in this course, although octet is less ambiguous/more correct
- Payload is limited to 1500 octets (MTU)

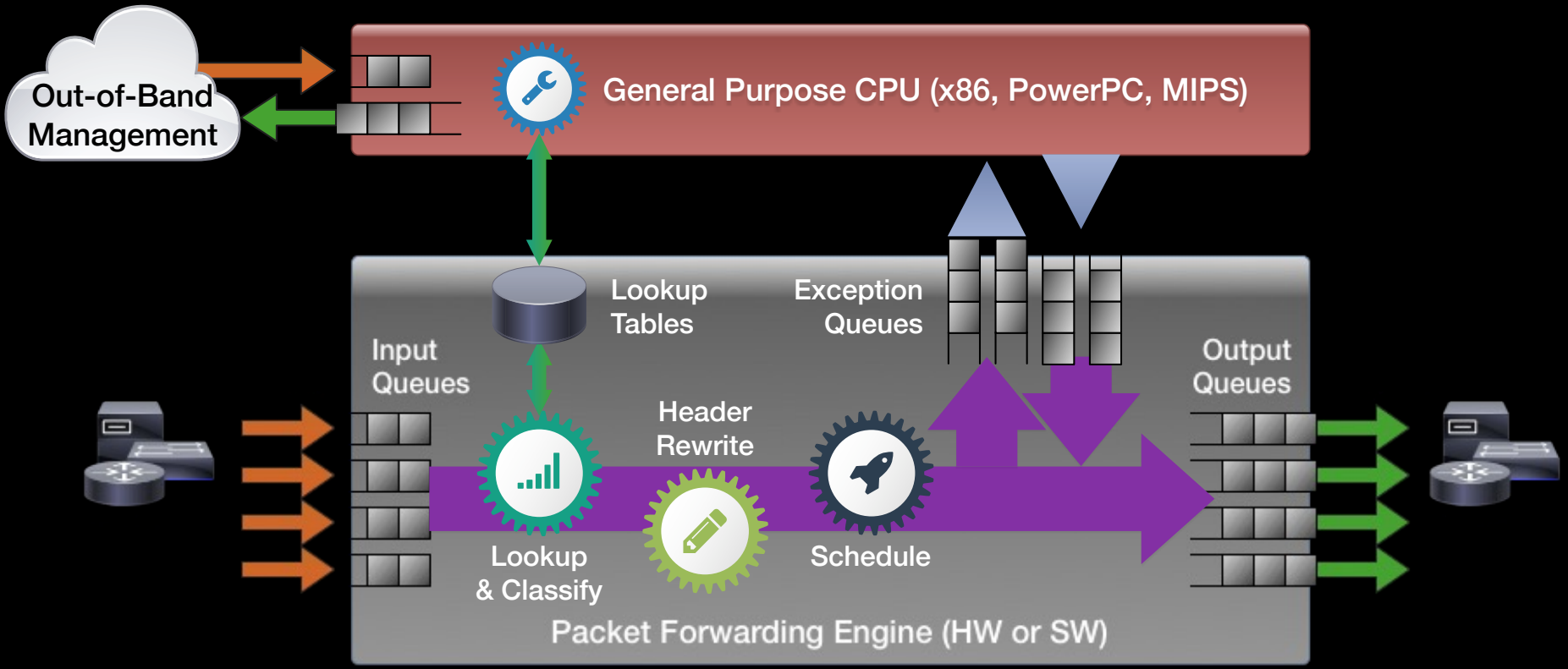
L2 Addressing and Promiscuous Mode



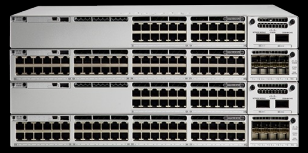

```
2. root@cmm-kali2: ~ (ssh)
root@cmm-kali2:~# ip link show eth2
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_f
ast state UP mode DEFAULT group default qlen 1000
    link/ether 52:54:00:ec:a1:54 brd ff:ff:ff:ff:ff:ff
root@cmm-kali2:~#
root@cmm-kali2:~# ip link set eth2 promisc on
root@cmm-kali2:~# ip link show eth2
4: eth2: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc
 pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether 52:54:00:ec:a1:54 brd ff:ff:ff:ff:ff:ff
root@cmm-kali2:~#
```

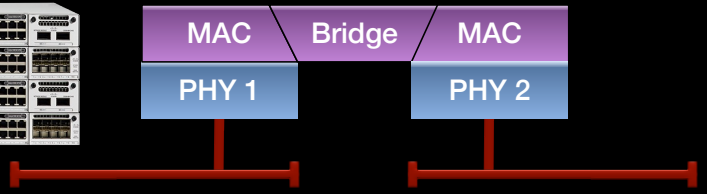
- Interfaces are are configured with a burned-in MAC address
- NICs will not interrupt the host for destination MAC addresses that do not match its interface
  - **Exceptions**: Broadcast (`ff-ff-ff-ff-ff-ff`) and Multicast
- You can change this behavior with promiscuous mode, meaning the NIC interrupts the CPU for every packet
- Packet capture software like Wireshark does this by default

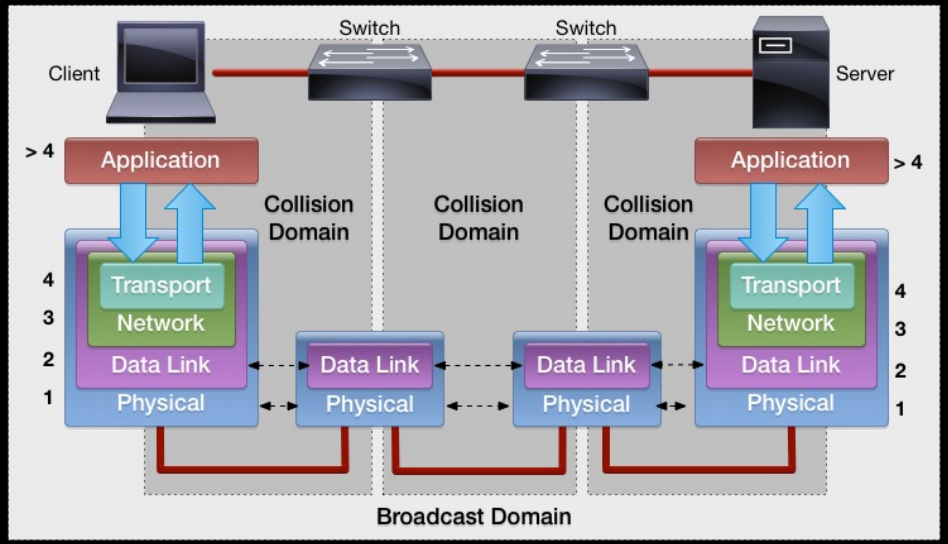
Basic Forwarding Device Architecture



Bridges and Switches

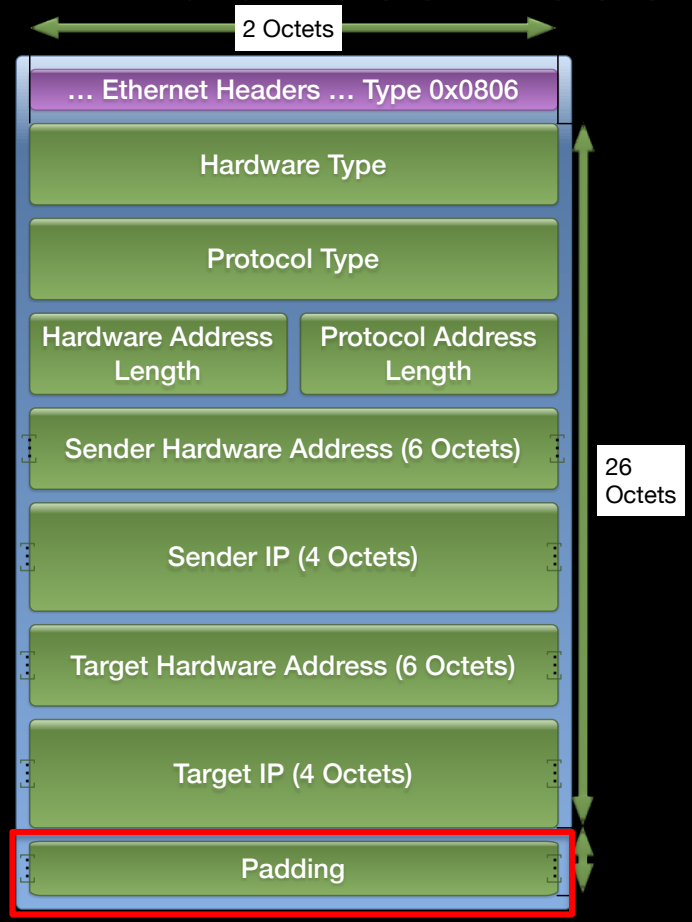






- Switches create a broadcast domain from a collection of individual LAN segments
- Switches learn, filter, and forward frames based on source and destination MAC addresses
- Switches can be internally partitioned using Virtual LANs (VLANs), which can be carried externally using 802.1Q tagged frames. Cisco calls these “Trunks”

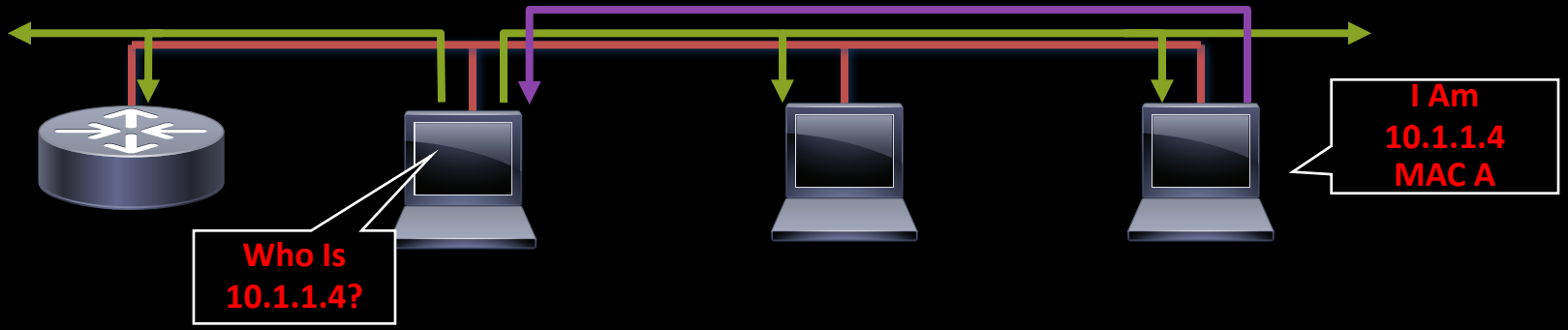
Address Resolution Protocol (ARP)



- Machines on a link have to translate from a target IP address to a MAC address to send a frame
- Each host and router has an ARP cache, which you'll see can be manipulated
- ARP has a large padding field to meet the 64 byte size requirement of Ethernet

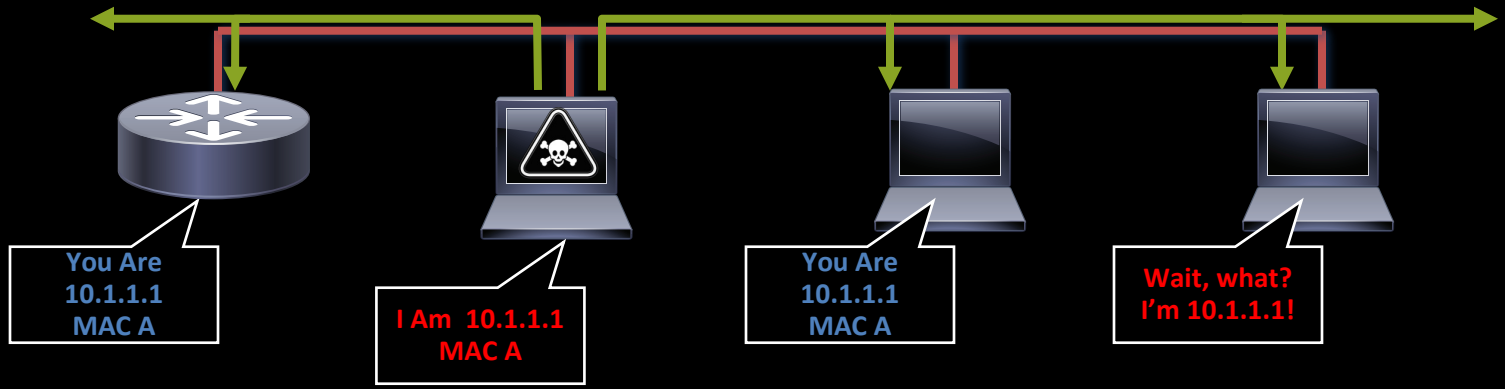
ARP Functionality

- Before a station can talk to another station it must do an ARP request to map the IP address to the MAC address
  - ARP request is broadcast using EtherType 0x0806
- 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



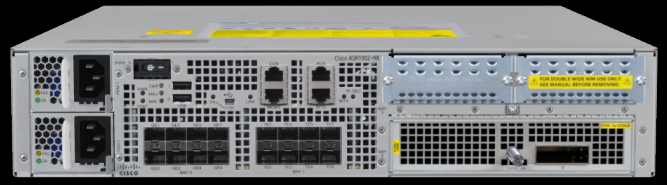
Gratuitous ARP

- According to the ARP RFC (826), a client is allowed to send an unsolicited ARP reply; this is called a gratuitous ARP; other hosts on the same subnet can store this information in their ARP tables
- Anyone can claim to be the owner of any IP/MAC address they like
- ARP attacks use this to redirect traffic



ARP Spoofing Tools

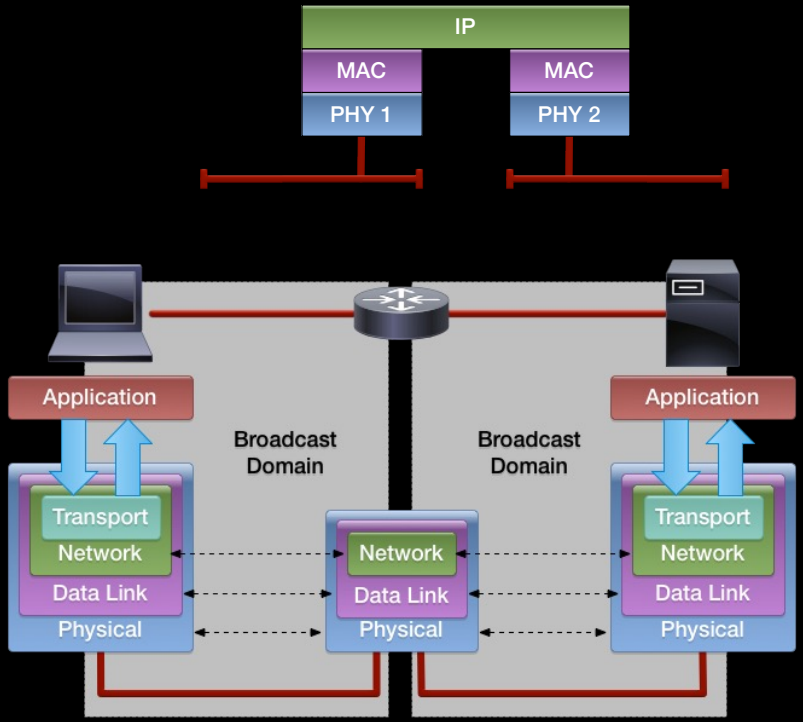
- Dsniff
  - One of the original tools
- Scapy
  - arpcachepoison()
- Ettercap
  - Curses and GUI for easy MITM
  - Captures passwords: FTP, Telnet, SMTP, HTTP, POP, NNTP, IMAP, SNMP, LDAP, RIP, OSPF, PPTP, MS-CHAP, SOCKS, X11, IRC, ICQ, AIM, SMB, Microsoft SQL, etc.
- Cain & Abel
  - Windows-based MITM tool and cracker
- Metasploit Framework
  - Includes some tools for packet generation
- Roll your own
  - Scapy
  - libnet
  - etc



What Routers Really Do

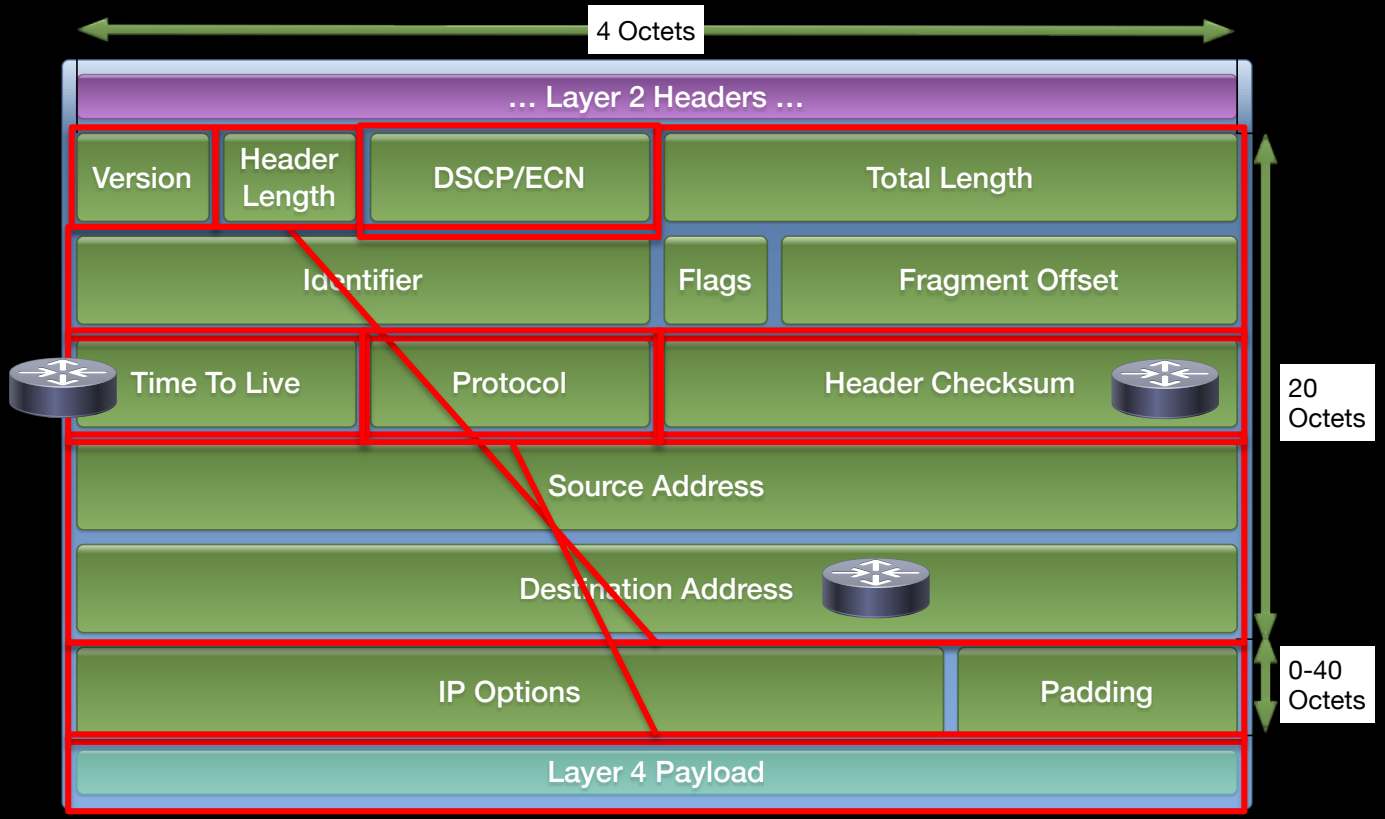
- Maintain and manipulate routing information (Routing Information Base [RIB])
  - Listen for updates and send updates to neighbors
- Construct the forwarding table – called the Forwarding Information Base (FIB) from information in the RIB
- Classify and Forward packets at Layer 3
  - Update TTL/hop limit, recalculate header checksum, rewrite the Layer 2 header information
- Filter packets using Access Control Lists based on Layer 3 and optionally, upper layer information such as TCP ports
- Management tasks – SNMP, NETCONF, SSH, Traceroute, etc.

Routers



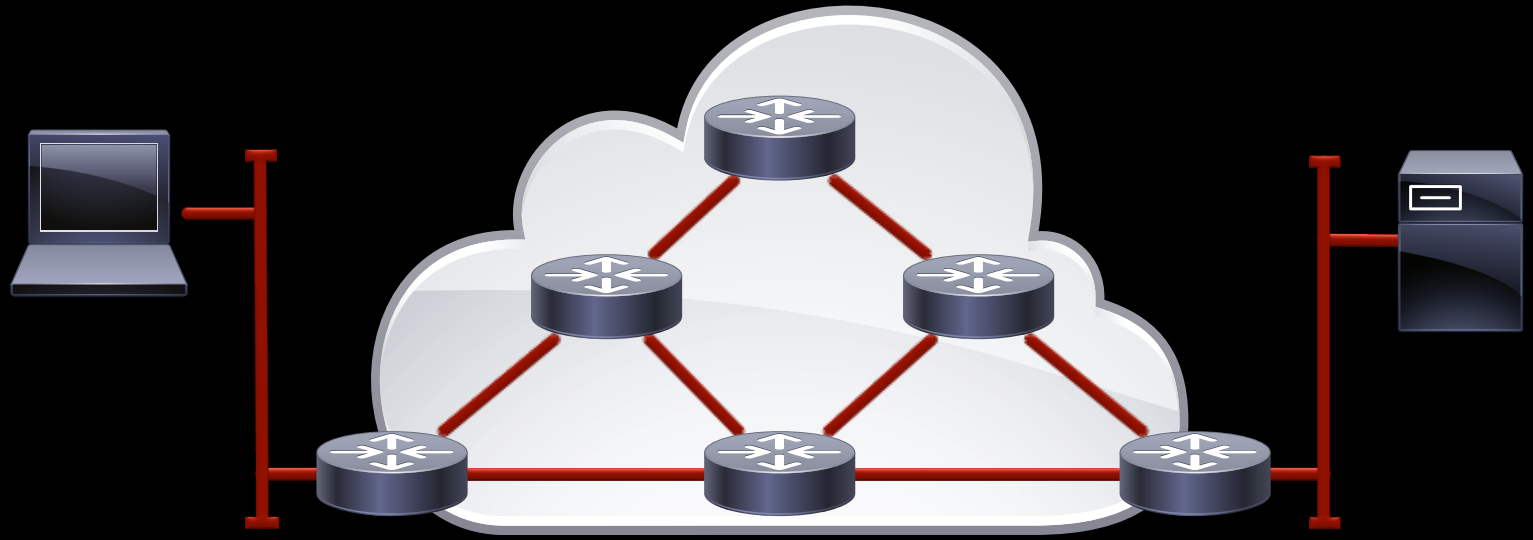
- Routers create internetworks from groups of Broadcast Domains
  - These can be Links or VLANs
- Routers do not forward broadcast packets
- Hosts must be informed of the router's IP address on the link (Default Gateway) to forward packets

Internet Protocol (IPv4) Packet



- It's not as complicated as it might look
- Let's break things up into groups for more insight into how things work

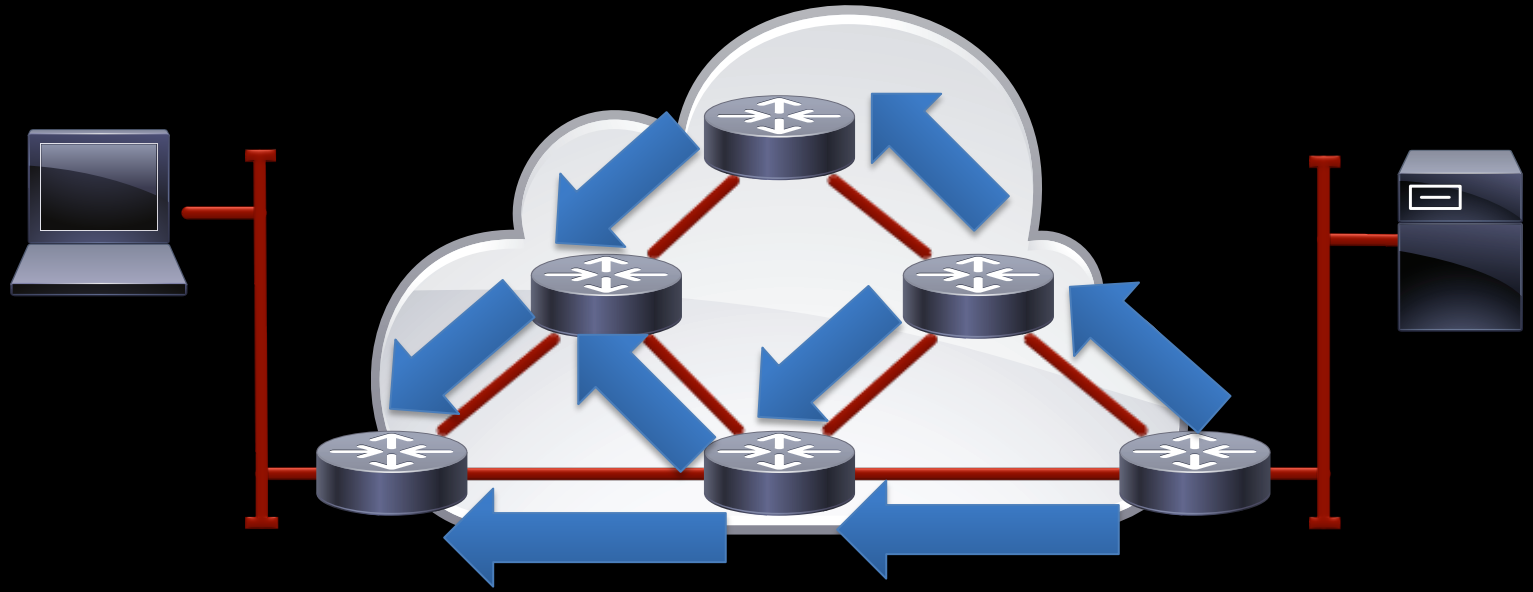
How Do We Get There from Here?



- Our path choice is based on the location of the destination
- Location is represented by the prefix of the address
- The most specific and most attractive (lowest metric) path wins

How Do We Get There from Here?

Routers discover prefixes using Interior Gateway Protocols (IGP).

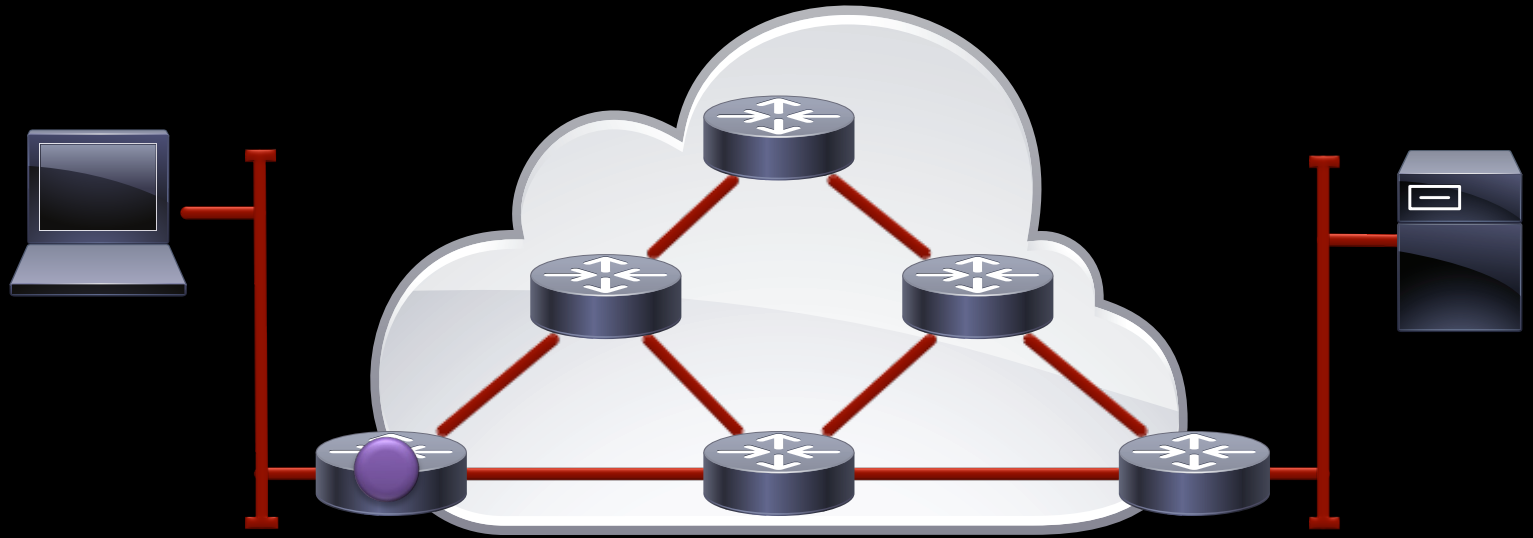


How Do We Get There from Here?

Client wants to talk to 172.30.14.10. Sees destination isn't on the local link.
Discovers the MAC address of the default gateway using ARP broadcast.
Sends th

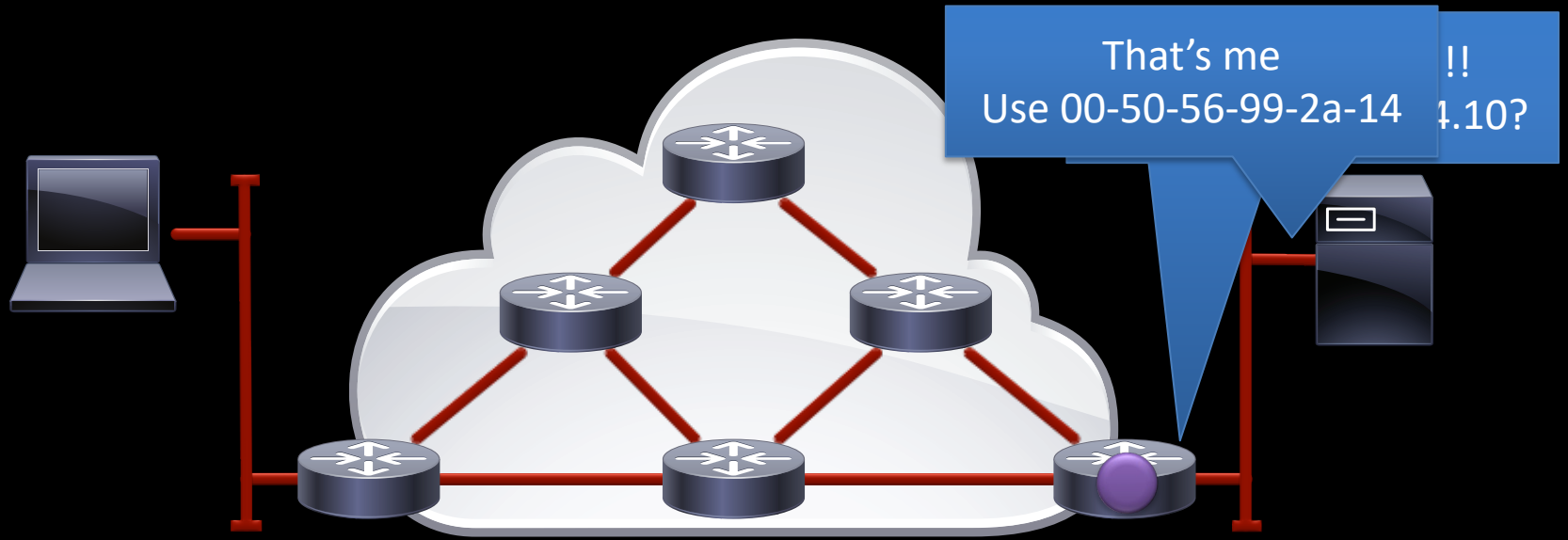
How Do We Get There from Here?

Routers forward the packet towards the destination hop-by-hop, rewriting Layer 2 information until the last hop router is reached

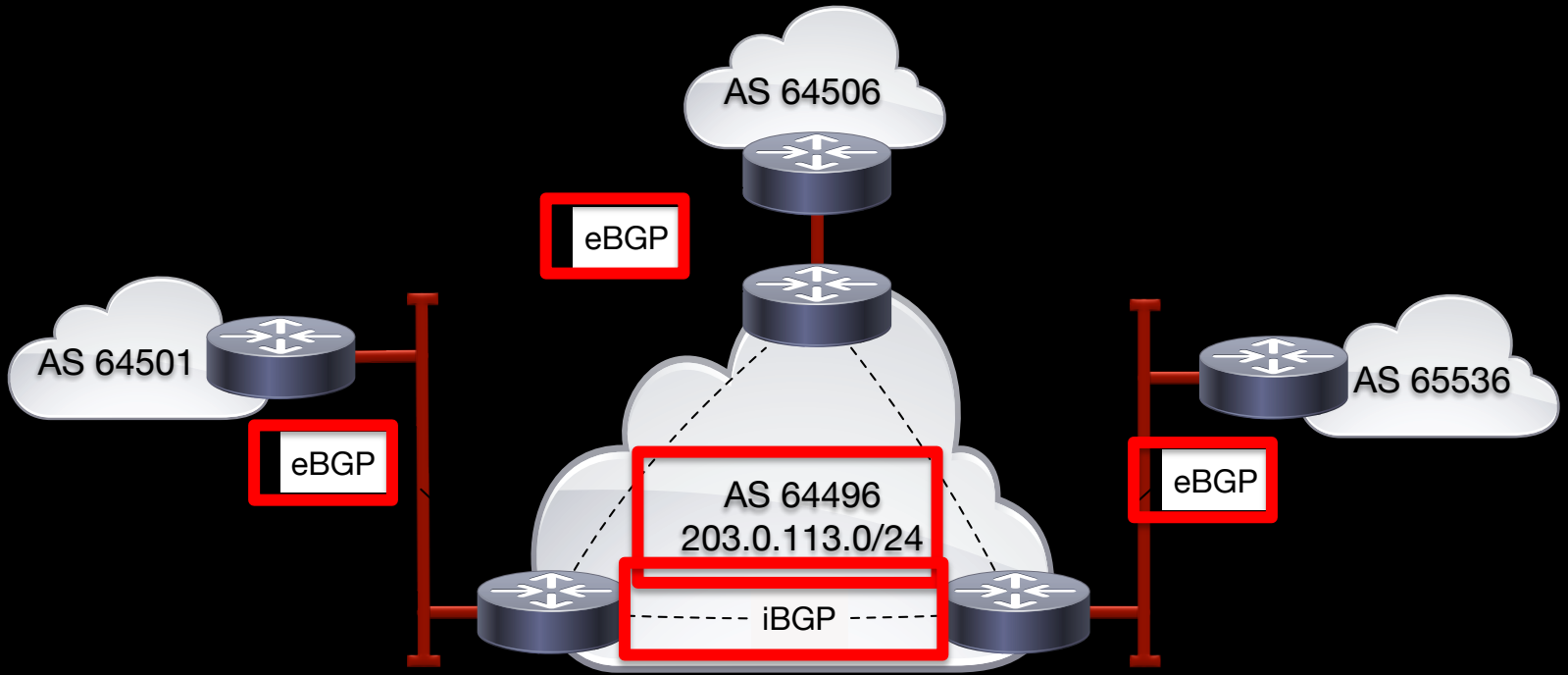


How Do We Get There from Here?

Last hop router sees it's attached to the destination in the packet.
Discovers the MAC address of the destination host using ARP;
Forwards the packet using the discovered MAC address.

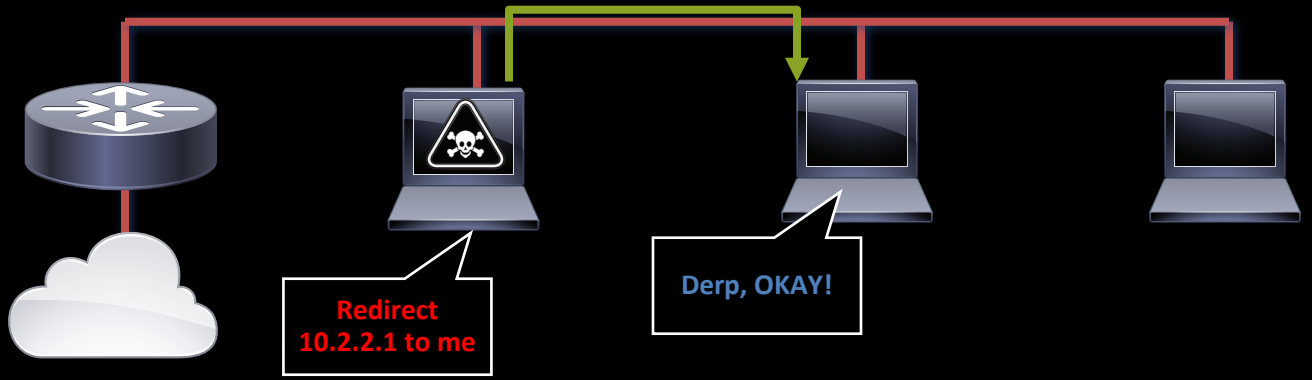


Autonomous Systems & BGP



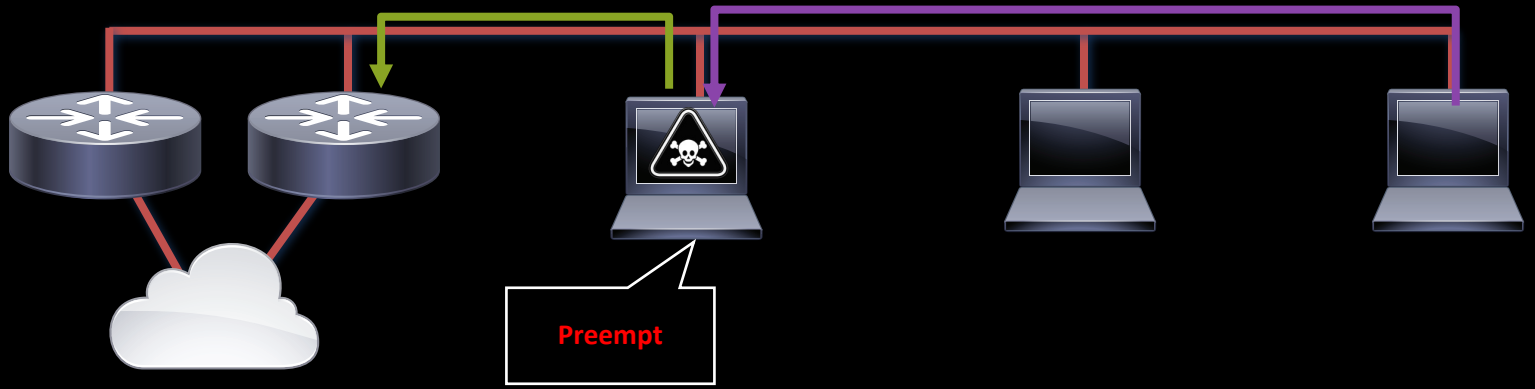
ICMP Redirects

- ICMP redirects instruct a host to send packets for a particular destination off-link to a different first-hop “router”
- Attacker with knowledge of packet headers for a particular flow can send an ICMP redirect and intercept
- More stealthy & selective, but only one way and more difficult to pull off



First Hop Redundancy Protocols

- Protocols like HSRP are used to provide first-hop default-gateway redundancy
- If using HSRP without MD5 authentication, an attacker can preempt the active router, steal the virtual IP and MAC address and intercept all packets from host ➔ router

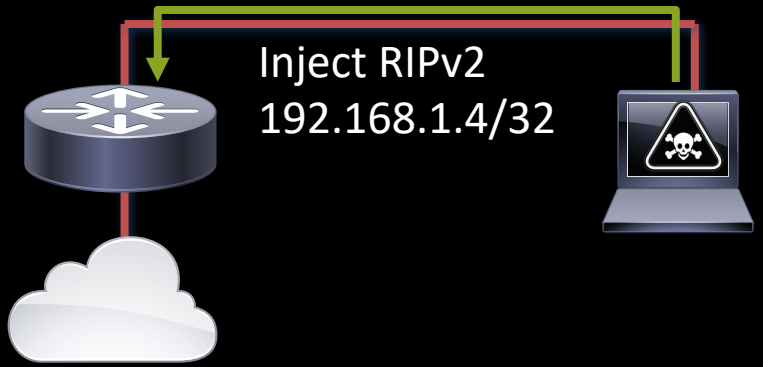


Attacking Routing Protocols

- These are very powerful attacks--can neutralize ACLs and intercept packets to critical infrastructure such as RADIUS or TACACS+ servers
- IGPs (RIP, OSPF, IS-IS, EIGRP) are easiest to attack, especially when no authentication is in use. Attacking IGPs can sometimes open up BGP!
- Use “more specific” (longer prefixes) or “more attractive” (lower metric) routes to modify the RIB

Attacking Routing Protocols

- So you've modified the router RIB and diverted a route to your machine…now what?
- Assume that IP! Add a secondary IP address on your host and set up a static route using an explicit source:




```
# ip address add 192.168.1.4/32 dev eth2
# ip route add 192.168.3.1/32 via
  192.168.2.1 src 192.168.1.4
```

Attacking Management Protocols…in particular…

SNMP!

Security Not My Problem

- At least in SNMPv1/v2c, the idea of security is ludicrous:
  1. UDP based protocol
  2. Protected only via a cleartext passwords
  3. ACLs are no help (see #1)
- SNMPv3 is much better. If you must use SNMP, use v3

Decrypting Router Passwords

- Cisco type 7 uses a well-known Vigenère cipher
  - Lots of on-line resources to decrypt
  - ciscodecrypt on your training VM

```
username admin password 7 0955411C54174711004D
```

- Cisco type 5 MD5
  - Salted MD5, use John The Ripper or oclHashCat for GPUs

```
enable secret 5 $1$5zt.$msdztajdDdbYMmu.MlmKx1
```

- Juniper Type 9
  - Another Vigenère cipher, a few on-line decryptors
  - Perl module: http://search.cpan.org/dist/Crypt-Juniper/lib/Crypt/Juniper.pm
- Huawei/HP/H3C cipher
  - Single DES with static key, converted to ASCII using a radix
  - Python script: https://github.com/grutz/h3c-pt-tools

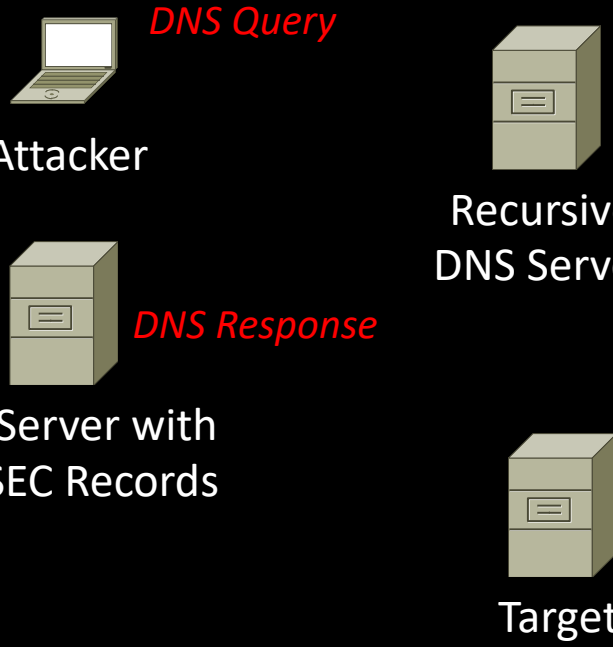
DENIAL OF SERVICE

Distributed Denial of Service

- Anyone can become the target or the attacker
- Brian Krebs removed from Akamai, 665Gb/s
  http://www.zdnet.com/article/krebs-on-security-booted-off-akamai-network-after-ddos-attack-proves-pricey/
- Anonymous' Low Orbit Ion Cannon (LOIC) agent is pretty simple to detect and defend against:
  https://tools.cisco.com/security/center/viewAlert.x?alertId=22056
- Other attacks can be mitigated using similar techniques

DNS Amplification Attack Basics

- Recursive DNS servers are used to disguise the source and complicate mitigation
- Attacker controls the “amplification record” which determines response size
- Responses are much larger than queries
- UDP can be spoofed, sending DNS responses to any target!
- Botnets/Zombies can be used to amplify the effect!



DNS Amplification Attack: Query vs. Response

- Running the following command generates a small query (78 bytes)

```
squatch@mybox#  dig ANY dnssec-deployment.org @149.20.64.21 +edns=0
```

- But it generates a large response (2548 bytes, or 32x amplification)

```
dnssec-deployment.org.  3445    IN      DNSKEY  257 3 5 AwEAAcK5cfm1WwR5F1d2xlVHnX2tJ1hKJeCVFZ1e5cxneVQRdhrjgAOo W1nsO1x
btD8kvQ/1MZc0xypKcGUBLb1pQfLmH05e1J4IIPuSi2OEvE0I 5ApOt5wccjIIRbyaCQd6wlqo6nOishB71GyQeii++HvMOdvJVIsmQDzq zz9F0guA2YymB
aaQuuT/1DyCrmFJ6jnNc8Fa6sZnGsw+JOaryFwNVhpM CbvEITm8PVhrUQDaNDz7+a85XVpgdYx2QTyWCIzViFJHKD+ybwLKmrXh wppr+kLSRBqymI8A6io
9X0KkYvSsbtcUQdblVw0N2TvwPvLfSdb2Sp+k QLKDF8Cyg8M=
dnssec-deployment.org.  3445    IN      DNSKEY  256 3 5 AwEAAbHt78xg07JcR4iK97hJaIoPoyKpn2KwGq1+m/YUYnKT+xeHXhUM A1TxN8L
ecbASrjmY4iL4vibd4Xes4h4kzHVAmypkptKsE4cb1NSQTyqj g8U/SfhDZttwsuGsb4S/USPKktqaB7VEUoLHzwqwTRb5d7YrGzhNCRTJ ll+amyj9
dnssec-deployment.org.  3445    IN      RRSIG   DNSKEY 5 2 3600 20130427191211 20130328181211 47809 dnssec-deployment.or
g. ajkEzM8VdRX2yF41DxasDKxH/eS+34XD4goD+s35ufNIAHULwigAosWo 2KgempfcPy2M4WBLYSMDlJBAgO9Za8W7oddusZnP9A2LoI1MgOEtwf0d dgw
CHZ8+oVhZnrq0H1OC26WtUrC0zLaBU/07z4Zb5oWt0jEMhiWZgBnh 9LrUq70KRdDlwlqUQmwjTlJyZ7p9/8IBrtR1NEcwgREqEncgh238W5BW eGAdoEUUT
w9yArshYa3Kj7UALgz5HmtQgM6Nqv2svaPQJNtoyB+6NBUG KEQvXYbDsmirjhe7GwxpOb09wI4oP1zZTD9qEHDf9TNNwQGqsSIGjn2s 9n6roQ==
dnssec-deployment.org.  3445    IN      RRSIG   DNSKEY 5 2 3600 20130427191211 20130328181211 65517 dnssec-deployment.or
g. Uk3S2MWTaW4vLQ471e8ex6O2mZMOWCw9OL5TjKcIj6t3x3u6antr5hQZ FBul4e2jWoheY3b3rdJ5ktESEH3aEFjVc0fGa95SNWZHNeLPKH7uxQKa Pw7
pfjINvNmCg3RNnmcHKrxNPWufHNuX6lnXSiyho4NmDRl5xy/0Dafu l4c=

;; ADDITIONAL SECTION:
ns1.dnssec-deployment.org. 3445 IN      A       168.150.236.43
ns1.dnssec-deployment.org. 3445 IN      AAAA    2001:470:1f00:187::1

;; Query time: 787 msec
;; SERVER: 149.20.64.21#53(149.20.64.21)
;; WHEN: Tue Apr  9 10:46:26 2013
;; MSG SIZE  rcvd: 2548
```

DNS Amplification Attacks

1. Attacker sends DDoS command to botnet
2. Botnet sends requests for amplification record through open resolver, spoofed from Target
3. The reply is forwarded to Target through recursive DNS server, saturating link.

DNS Server with DNSSEC records

Attacker

Botnet Hosts

Recursive DNS Server

Target

NTP MONLIST Attack Basics

- MONLIST command, described in CVE-2013-5211, provides a list of the last servers that queried an NTP server
- Attacker controls the number of servers querying the NTP server, up to a maximum of 600
- Responses can be 206x larger than queries
- UDP can be spoofed, sending NTP responses to any target!
- Again, Botnets/Zombies can be used to amplify the effect!

Attacker

Spoofed MONLIST command with sources of the target

NTP Server

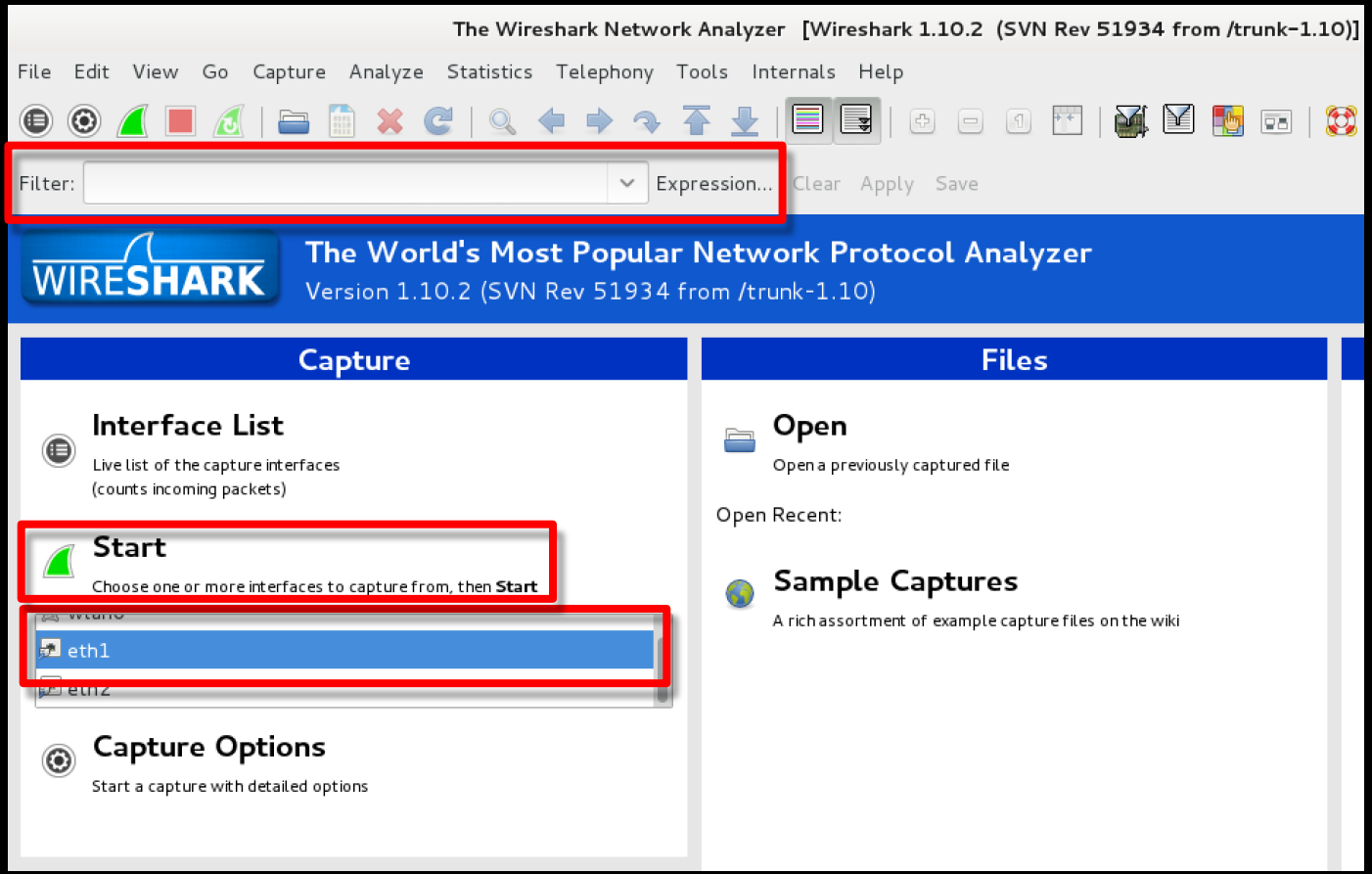
Target

DNS/NTP Amplification Attacks: Lessons Learned

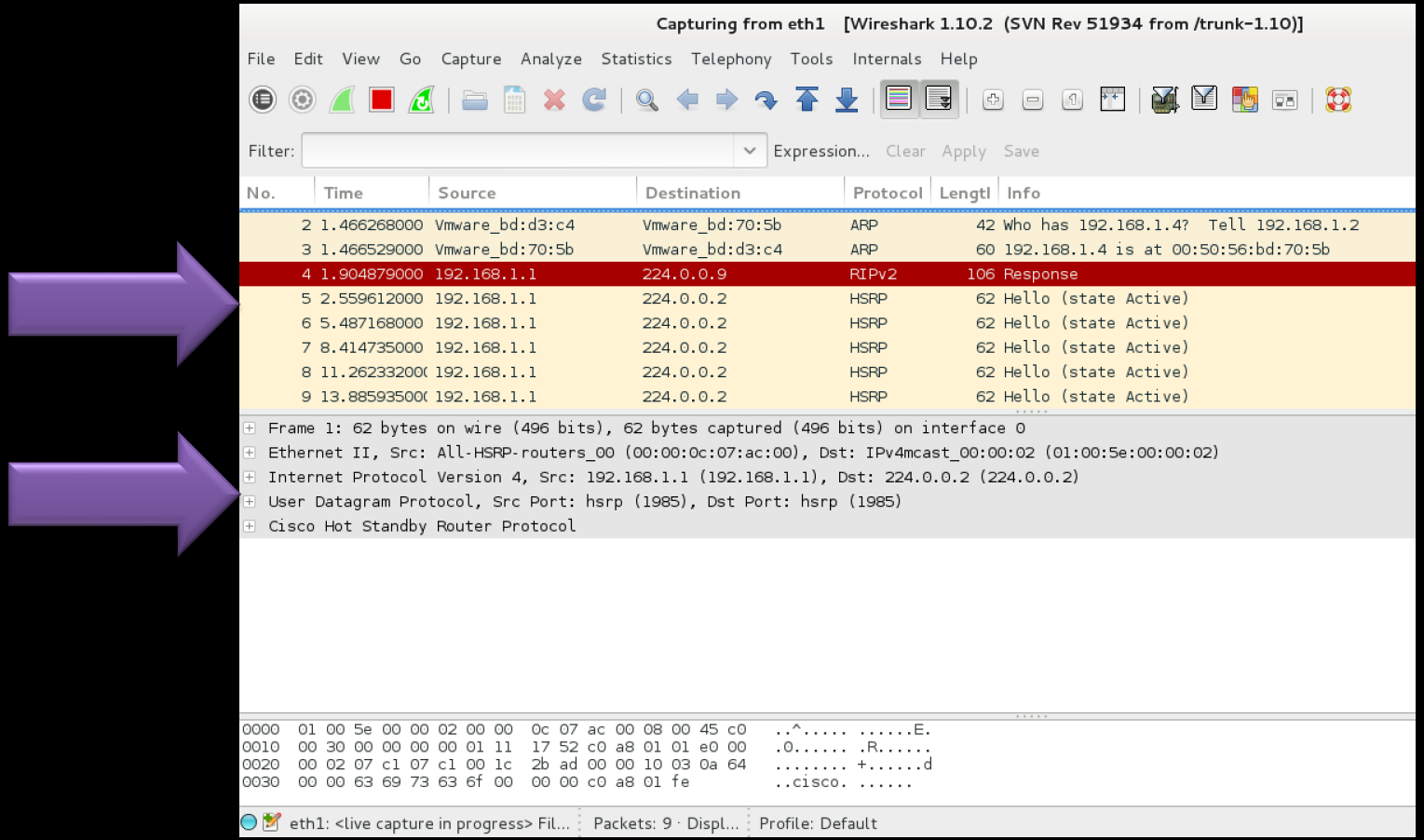
- BCP-38 -- Learn it, live it, love it
- Recursive DNS servers are bad to have available to anyone on the Internet, and their use and misconfiguration often goes unnoticed
- Fixing your own DNS infrastructure will prevent you from participating in DDoS, but will not protect you from attack.
- Internet border routers or firewalls may block or rate limit the traffic, but if the upstream link is saturated, the DDoS still succeeds.
- Clean bandwidth solutions from ISPs appear to help.

Sometimes It’s Not From the Network…

Wireshark


The Wireshark Network Analyzer [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.10.2 (SVN Rev 51934 from /trunk-1.10)
Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
eth1
Capture Options
Start a capture with detailed options
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki

Wireshark


Capturing from eth1 [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Lengtl Info
2 1.466268000 Vmware_bd:d3:c4 Vmware_bd:70:5b ARP 42 Who has 192.168.1.4? Tell 192.168.1.2
3 1.466529000 Vmware_bd:70:5b Vmware_bd:d3:c4 ARP 60 192.168.1.4 is at 00:50:56:bd:70:5b
4 1.904879000 192.168.1.1 224.0.0.9 RIPv2 106 Response
5 2.559612000 192.168.1.1 224.0.0.2 HSRP 62 Hello (state Active)
6 5.487168000 192.168.1.1 224.0.0.2 HSRP 62 Hello (state Active)
7 8.414735000 192.168.1.1 224.0.0.2 HSRP 62 Hello (state Active)
8 11.26233200(192.168.1.1 224.0.0.2 HSRP 62 Hello (state Active)
9 13.88593500(192.168.1.1 224.0.0.2 HSRP 62 Hello (state Active)
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: All-HSRP-routers_00 (00:00:0c:07:ac:00), Dst: IPv4mcast_00:00:02 (01:00:5e:00:00:02)
Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 224.0.0.2 (224.0.0.2)
User Datagram Protocol, Src Port: hsrp (1985), Dst Port: hsrp (1985)
Cisco Hot Standby Router Protocol
0000 01 00 5e 00 00 02 00 00 0c 07 ac 00 08 00 45 c0 ..^..... ......E.
0010 00 30 00 00 00 00 01 11 17 52 c0 a8 01 01 e0 00 .0..... .R......
0020 00 02 07 c1 07 c1 00 1c 2b ad 00 00 10 03 0a 64 .... +......d
0030 00 00 63 69 73 63 6f 00 00 00 c0 a8 01 fe ..cisco. ......
eth1: <live capture in progress> Fil... Packets: 9 · Displ... Profile: Default

Scapy 101

- Scapy is a python-based TCP/IP packet generator tool/library

```
>> ip = IP(dst=’10.10.10.1’)
>> ip
<IP  dst=10.10.1.1 |>
>> icmp=ip/ICMP()
>> ls(icmp)
…some stuff happens here…
>> sr1(icmp)
…some stuff happens here…
```

Scapy Commands

`>> ls()` List layers available

`>> lsc()` List commands available

`>> conf` View current configuration

`>> arpcachepoison()` Poison the ARP cache of a target

`>> send()` Send at layer 3

`>> sendp()` Send at layer 2

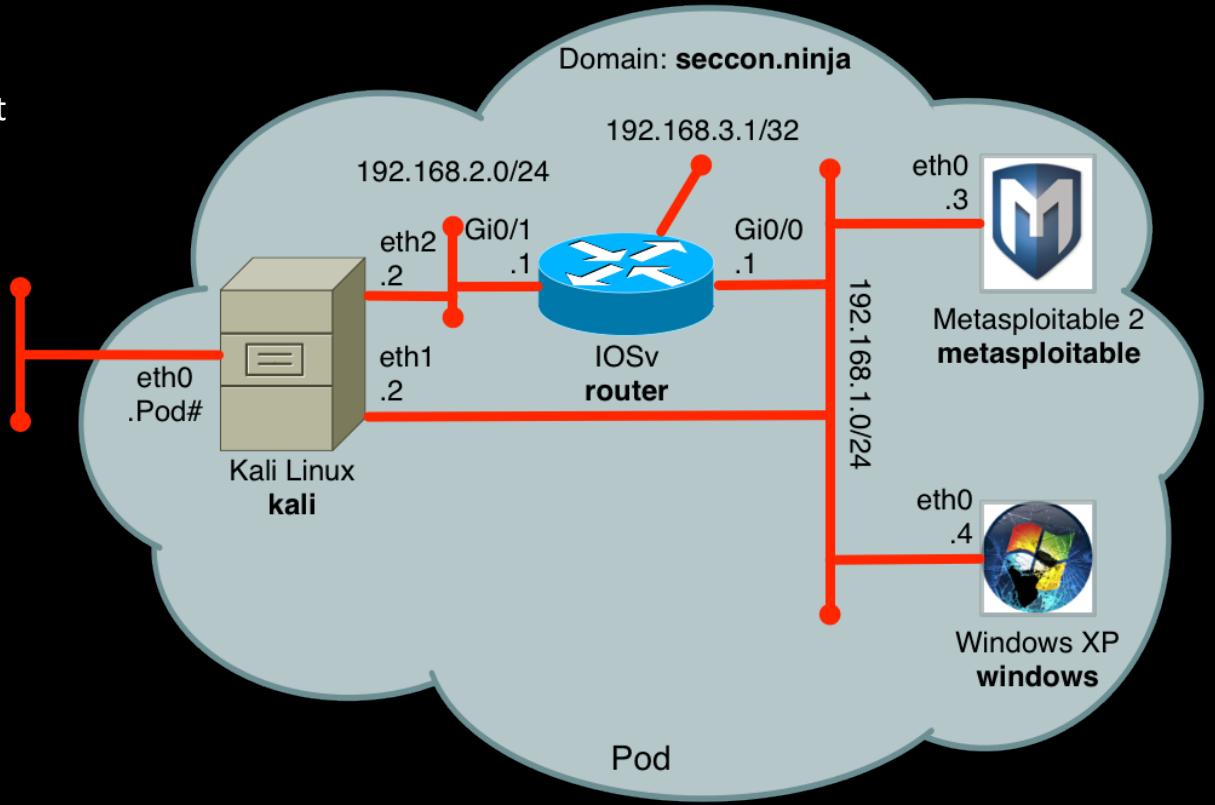
`>> rdpcap()` Load PCAP file (not PCAP-NG)

`>> help(command)` Get help on any command

NETWORKING LAB

Topology & Exercises

- **Goal**: Break into the IOS router at the center of the network using TELNET and a locally configured username and password
- Poison the ARP cache of the IOSv router to send packets to kali
- Grab the Complete Router Configuration using SNMP and Decrypt Passwords using ciscodecrypt
- Break into the IOS router at the center of the network using TELNET and the administrator username and password



Q&A

Thank You!