

# Defending Computer Networks

## *Lecture 5: Intro to Networks*

Stuart Staniford

Adjunct Professor of Computer Science

# Logistics

- We have a T.A.!
  - Zhiyuan Teo [zt27@cornell.edu](mailto:zt27@cornell.edu)
  - “Everyone calls me ‘zee’”
  - Will be doing hw/quiz grading
  - (607) 279-8025
  - Office: Upson 4107a
  - Office hours: ???
- 5 Minute Break Experiment

# Additional Reading

- Jeff King *ARP Poisoning Attack and Mitigation Techniques*
  - [http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white\\_paper\\_c11\\_603839.html](http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11_603839.html)

# Latest News (eweek.com)

## Microsoft Takes Aim at Critical Outlook Vulnerability

By Sean Michael Kerner | Posted 2013-09-10 [Email](#) [Print](#)

[f Share](#) 2 [t Tweet](#) 8 [g+ Google +](#) 1 [in Share](#) 1 [f Like](#) 6 [f Recommend](#) 6



**Microsoft fixes 47 different security issues in its September Patch Tuesday update affecting multiple products, including Outlook, SharePoint and Internet Explorer.**

Microsoft is out with its monthly Patch Tuesday update, this time issuing 13 security bulletins, four of which are rated critical. Overall, the update patches 47 different vulnerabilities across the 13 advisories, spanning multiple Microsoft products, including Windows, Office, SharePoint and Internet Explorer.

Among the critical advisories this month is [MS13-068](#), which details a vulnerability in Microsoft Outlook that could allow for remote code execution.

"A remote code execution vulnerability exists in the way that Microsoft Outlook parses specially crafted S/MIME email messages," Microsoft's bulletin states. "An attacker who successfully exploited this vulnerability could take complete control of an affected system."

# More News (zdnet.com)

## Update Flash, Shockwave ASAP! Adobe also patches Acrobat and Reader

**Summary:** (Correction:.) Surprise updates to Adobe Flash Player and Shockwave Player address critical vulnerabilities at high risk of exploit. Less urgent, but still serious updates for Adobe Acrobat and Reader are also available.



By [Larry Seltzer](#) for [Zero Day](#) | September 10, 2013 -- 15:32 GMT (08:32 PDT)

Follow @lseltzer

Comments

11

★ Votes

0

Like

146

Tweet

71

Share

more +

Adobe today released security updates for [Flash Player](#), [AIR](#), [Shockwave Player](#), [Acrobat and Reader](#). The updates for Flash Player and Shockwave Player on Windows and Mac address a vulnerability which Adobe classifies as Priority 1, which indicates that it is being exploited in the wild at a high risk of exploit.

The updated versions of Flash Player on Windows and Mac are 11.8.800.168 and 11.7.700.242. Earlier 11.7 and 11.8 versions are vulnerable. Updates are also available for Flash Player on Linux and Android, as well as Adobe AIR and the Adobe AIR SDK. These are not as severe and updating is not as high a priority.

# Where We Are in Syllabus

## Rough Lecture Syllabus:

- ✓ 1. The technical nature of software vulnerabilities and techniques used for exploiting them.
- ✓ 2. The pressures of commercial software development, and why firms very rarely produce secure software, even though they should.
- ☞ 3. Basics of monitoring a network, intro/refresher on TCP/IP. Switches, wireless access devices, routers.
  4. Network reconnaissance techniques – ping sweeps, port scans, etc.
  5. Algorithms for detecting port scans on the network.
  6. Firewalls and network segmentation as a defense against inbound attacks.
  7. Detecting exploits with string matching approaches (Snort and similar).
  8. Network layer approaches to evading detection.
  9. Large scale attacks – worms and distributed denial of service.
  10. HTTP attacks as a way around the firewall. Drive-by downloads and social engineering.
  11. Defending against HTTP attacks. Web-proxies, in-browser defenses, anti-virus systems.
  12. SMTP attacks – spear-phishing, and defenses against it.
  13. HTTPS: Encryption and virtual private networks as a means to maintain confidentiality.
  14. The modern enterprise network: what a large-scale network looks like, and emerging trends affecting it (BYOD, cloud).
  15. Legal and ethical issues in defending networks.

# Main Goals for Today

- Basics of Ethernet networks
- Basics of IP packets
- Arp translation and arp spoofing

# Ethernet Basics

- Ethernet is a physical layer protocol/technology
  - One of many competing physical layers
  - Most popular, but others still important
    - Eg for long-haul cables
- For delivering packets of data
  - Called “frames” in ethernet lingo
  - From one machine to another
- Originally a LAN technology
  - Now sometimes used for sizeable networks

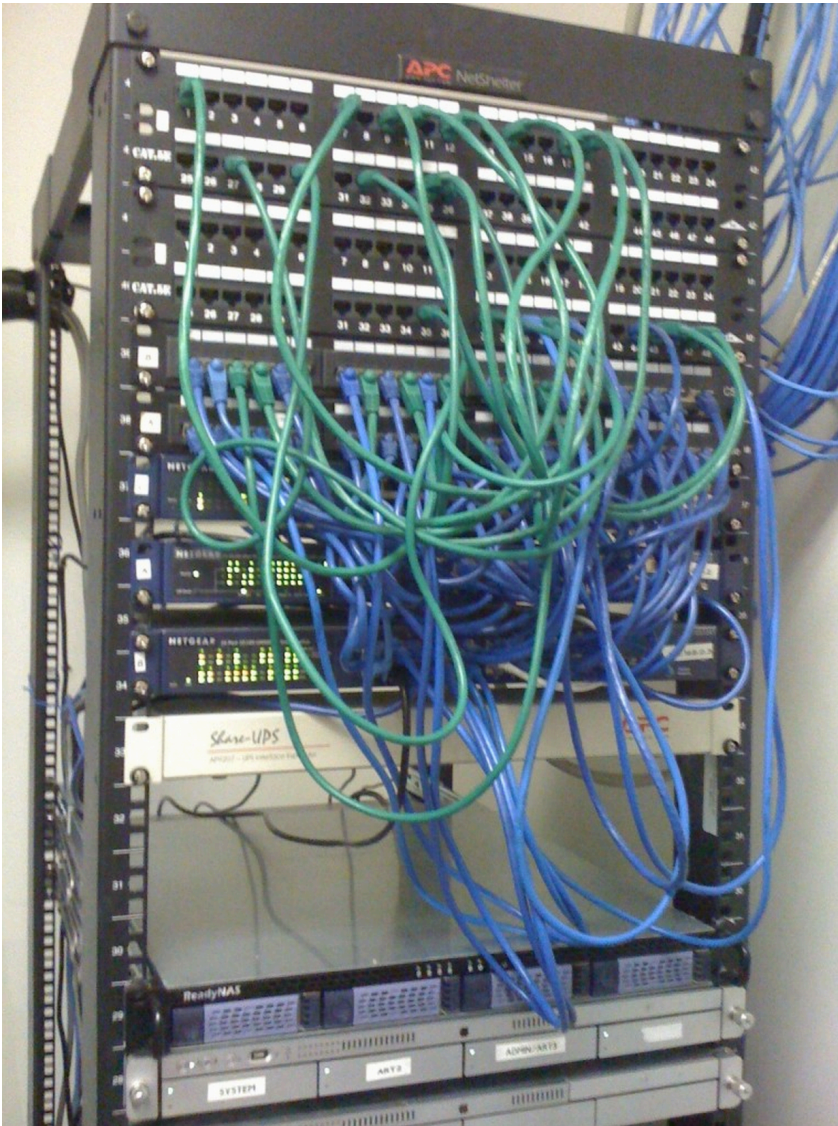


# Ethernet Then



10Base5

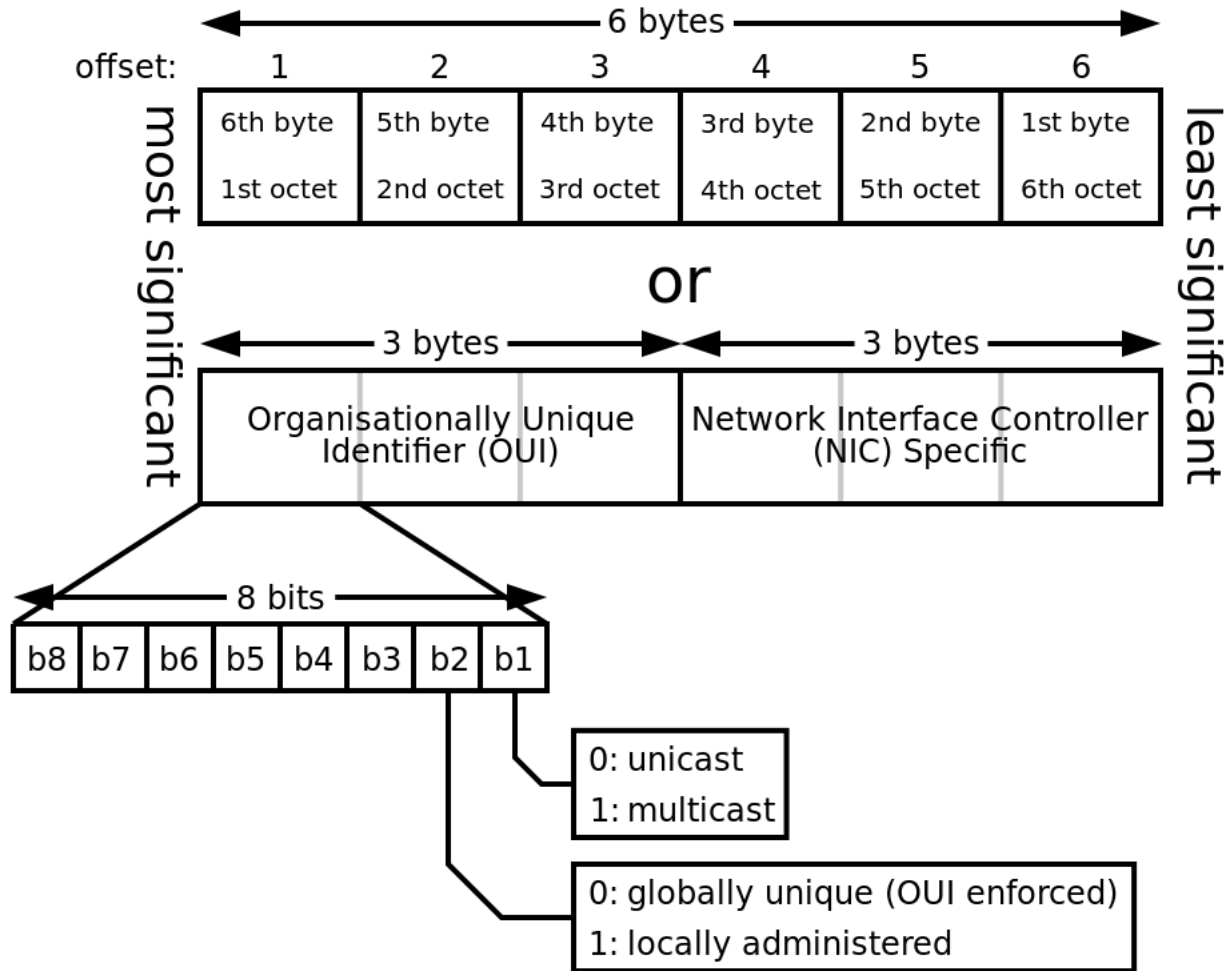
# Ethernet Now



# Ethernet Addresses

- 6 byte address
- `ifconfig -a` (alt: `tcpdump -D`)
- Every network interface has a hard-coded address
  - (But it's possible to forge in software...)
- Globally unique
  - Achieved by assigning vendor preambles

# Ethernet address



# Broadcast

- Originally broadcast – all computers hooked to the same wire
- Each interface listens to all traffic
  - Only pays attentions to packets with its address
  - Except for...

# Promiscuous Mode

- Possible to put interface/OS into special mode
- Where it looks at every packet, whether or not it's addressed.
- This is the basis of network monitoring.
- Let's do it:
  - `sudo tcpdump -i en0 -c 5 -e`
  - `sudo tcpdump -i en0 -c 5 -e not ether host 14:10:9f:e3:7d:a3`

# Ethernet Frame

802.3 Ethernet frame structure									
Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interframe gap	
7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46-1500 octets	4 octets	12 octets	
		← 64–1518 octets (68-1522 octets for 802.1Q tagged frames) →							
		← 84–1538 octets (88-1542 octets for 802.1Q tagged frames) →							

1500 is typical MTU for ethernet

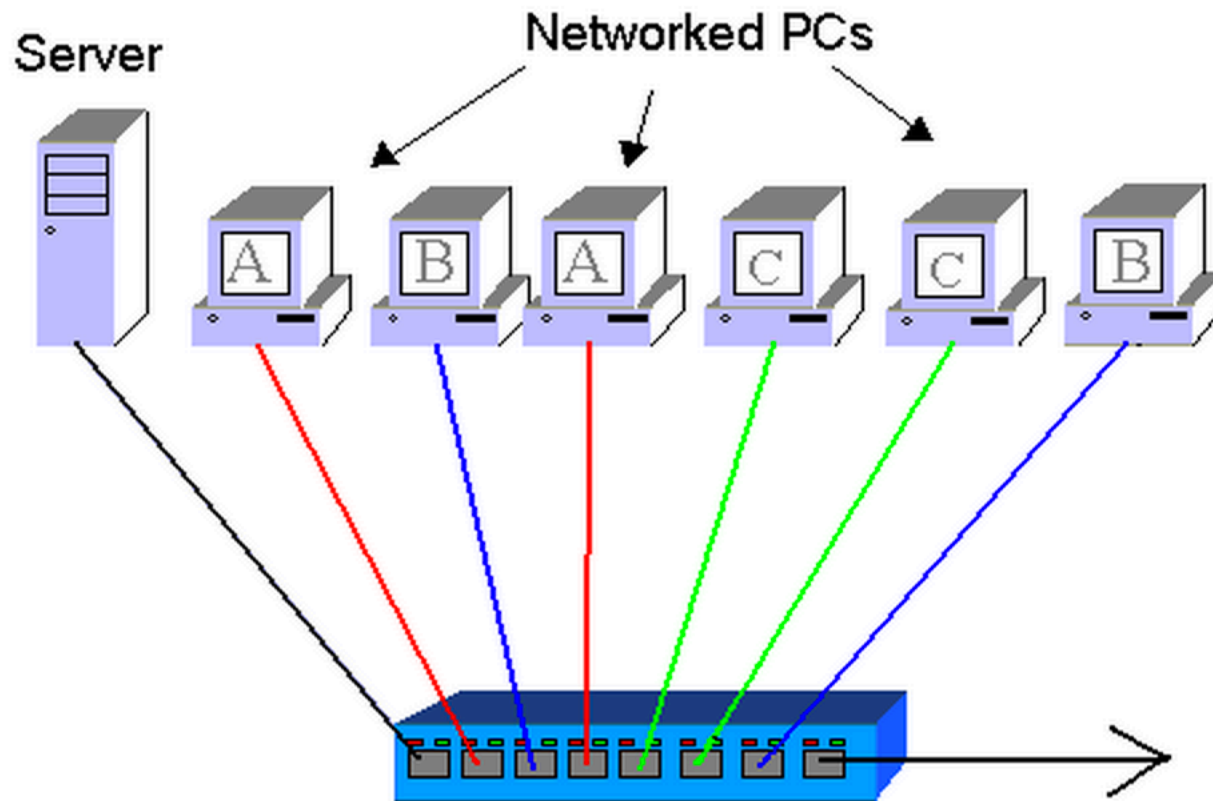
# Ethernet Type Codes

Note	Hex	
@	0000-05DC	IEEE802.3 Length Field (0.:1500.)
+	0101-01FF	Experimental
	0200	Xerox PUP (conflicts with 802.3 Length Field range) (see 0A00)
	0201	Xerox PUP Address Translation (conflicts ...) (see 0A01)
	0400	Nixdorf (conflicts with 802.3 Length Field)
+*	0600	Xerox NS IDP
	0601	XNS Address Translation (3Mb only)
+*	0800	DOD Internet Protocol (IP)
+	0801	X.75 Internet
+	0802	NBS Internet
+	0803	ECMA Internet
+	0804	CHAOSnet
+	0805	X.25 Level 3
+*	0806	Address Resolution Protocol (ARP) (for IP and for CHAOS)
	0807	XNS Compatibility
	081C	Symbolics Private
+	0888-088A	Xyplex
	0900	Ungermann-Bass network debugger
	0A00	Xerox IEEE802.3 PUP
	0A01	Xerox IEEE802.3 PUP Address Translation
	0BAD	Banyan Systems
	0BAF	Banyon VINES Echo
	1000	Berkeley Trailer negotiation
	1001-100F	Berkeley Trailer encapsulation for IP
	1234	DCA - Multicast
*	1600	VALID system protocol
	1601	VALID system protocol

<http://www.cavebear.com/archive/cavebear/Ethernet/type.html>

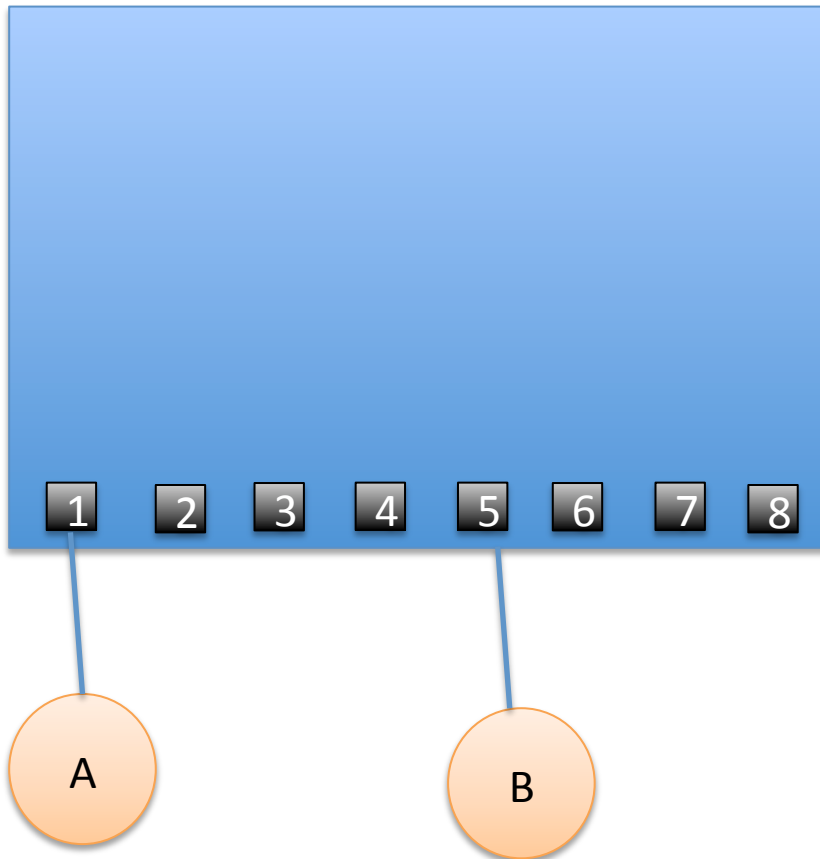


# Switched Ethernet



Source: [http://engweb.info/courses/various/gnotes/ethernet\\_overview.html](http://engweb.info/courses/various/gnotes/ethernet_overview.html)

# CAM Table



A: A->B

S: Ah, A is on 1

S: Broadcast A->B pkt

B: B->A

S: Ah, B is on 5

Switch has no more need  
to broadcast about A or B

# CAM Table Overflow

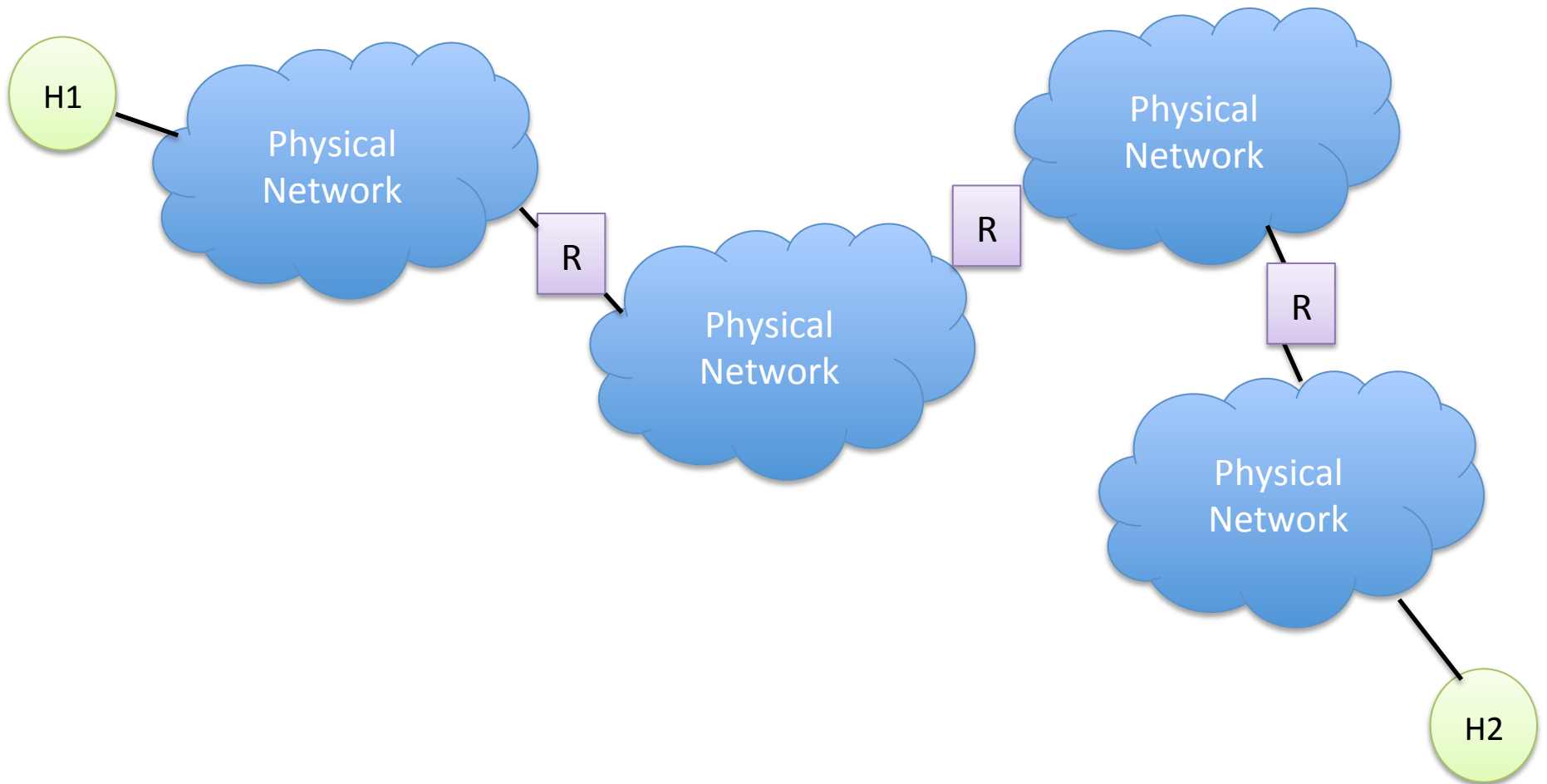
- If the switch sees too many MAC addresses
  - CAM table fills up
  - Then just broadcasts everything
  - Makes it easier to sniff everyone's traffic
- Can be mitigated with port security
  - Switch rules about what Macs on what port
  - Or how many Macs per port

5 Minute Break

# IP: Internet Protocol

- Core part of TCP/IP suite of protocols
- Defined by IETF (Internet Engineering Task Force)
- Protocol for global exchange of packets
- Across many physical networks

# Core IP Concept



# IP Address (v4)

- Four bytes
- Written 192.168.254.6
  - “dotted decimal”
- Ifconfig -a
- Originally a global static identifier
  - Encoded location on Internet
  - Has become much more complex
- `sudo tcpdump -i en0 -c 5`

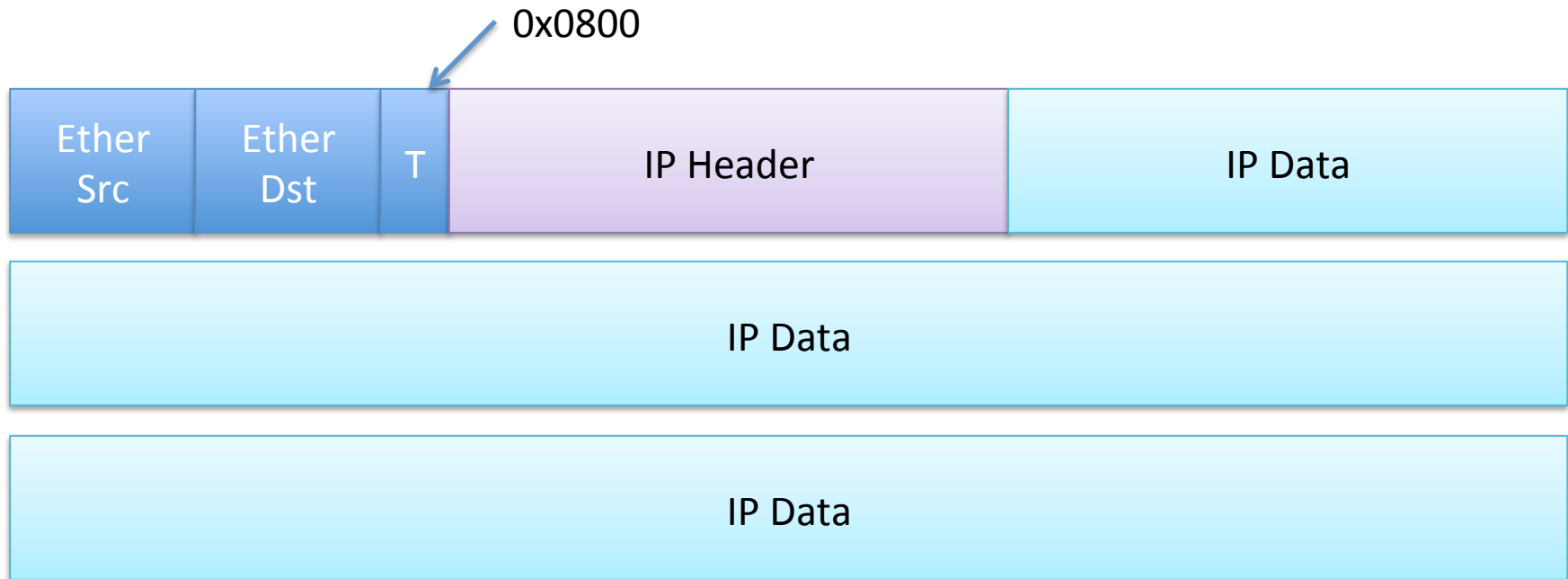
# IP Header

0	4	8	16	19	24	31
Version	IHL	Type of Service	Total Length			
Identification			Flags	Fragment Offset		
Time to Live	Protocol		Header Checksum			
Source IP Address						
Destination IP Address						
Options					Padding	

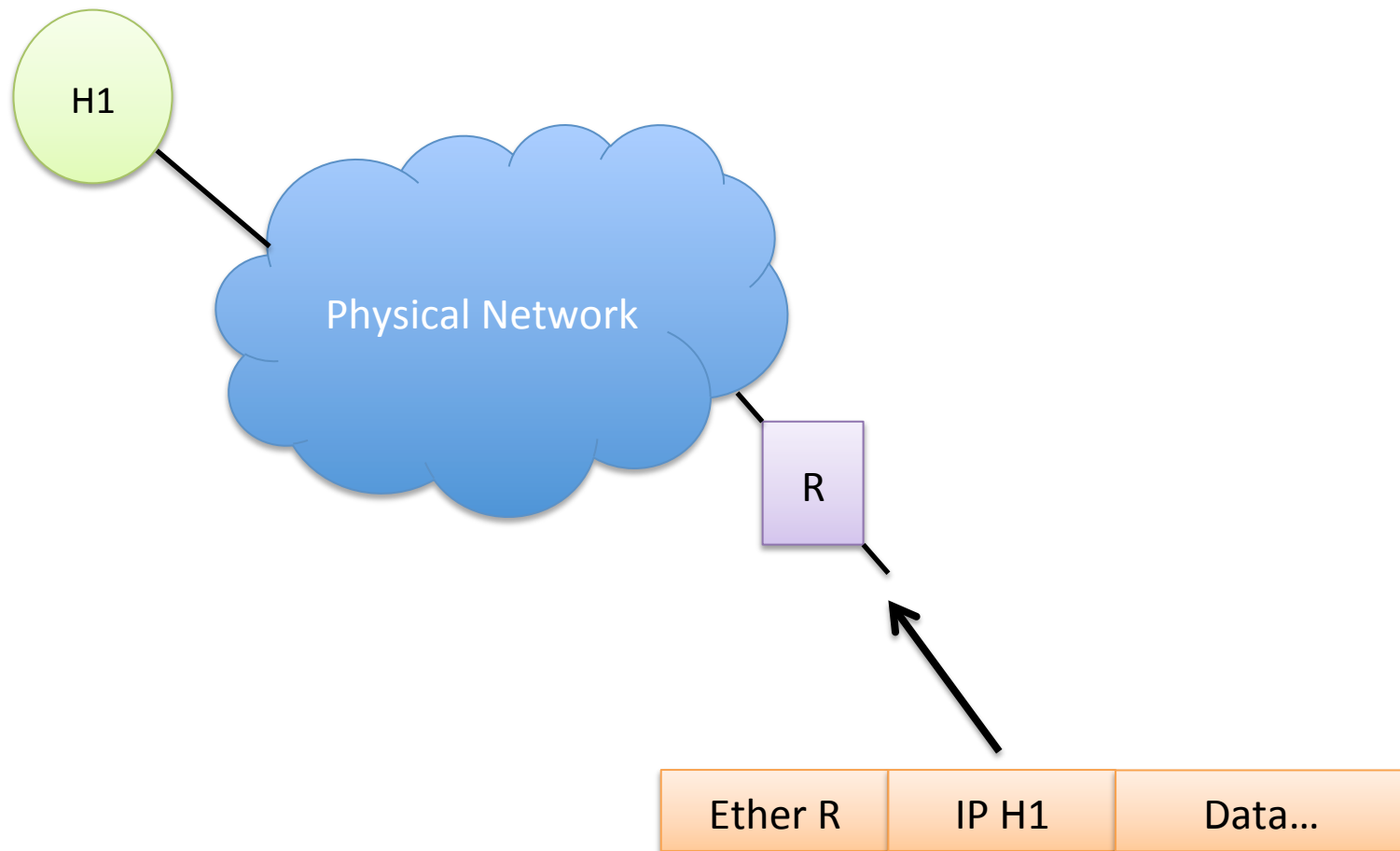
<http://cs.uccs.edu/~cs522/msgformat/format.htm>



# Ethernet IP Nesting




# Address Resolution: The Problem




# Address Resolution Protocol

- Part of Internet protocol suite
  - RFC 826 (1982).
- Wrapped inside an ethernet packet
  - or other hardware layer
  - Ethertype 0x0806
- Basically asks where a given IP packet should go
  - As a physical layer (eg ethernet) address
- Runs on a single physical network
  - Never transmitted across routers

# ARP Packet Format

Ethernet = 0x0001 

IP = 0x0800 

1 = request, 2 = reply 

Internet Protocol (IPv4) over Ethernet ARP packet		
bit offset	0 – 7	8 – 15
0	Hardware type (HTYPE)	
16	Protocol type (PTYPE)	
32	Hardware address length (HLEN)	Protocol address length (PLEN)
48	Operation (OPER)	
64	Sender hardware address (SHA) (first 16 bits)	
80	(next 16 bits)	
96	(last 16 bits)	
112	Sender protocol address (SPA) (first 16 bits)	
128	(last 16 bits)	
144	Target hardware address (THA) (first 16 bits)	
160	(next 16 bits)	
176	(last 16 bits)	
192	Target protocol address (TPA) (first 16 bits)	
208	(last 16 bits)	

# Operation of ARP request

- Given an IP,
  - Look up in local arp table
  - “arp -a -n |less” to see table
- If not in table, send a broadcast
  - to ethernet ff:ff:ff:ff:ff:ff
  - Asking for that destination IP address
- Also includes our ethernet and ip address

# ARP response

- Recipient
  - Reverses src/dest fields
  - Fills out its correct MAC address
  - Changes opcode to 2
  - Sends out in an ethernet packet directly to requester (not broadcast)
- Now communication can be established from requester to responder