Defending Computer Networks
Lecture 5: Intro to Networks

Stuart Staniford

Adjunct Professor of Computer Science

Logistics

- Problems registering in class still?
- Reminder HW1 due Friday midnight

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

Latest News

SECURITY

Home Depot Data Breach Could Be the Largest Yet

By NICOLE PERLROTH SEPTEMBER 8, 2014 6:58 PM 84 Comments

Home Depot confirmed on Monday that hackers had broken into its in-store payments systems, in what could be the largest known breach of a retail company's computer network.

The retailer said the exact number of customers affected was still not clear. But a person briefed on the investigation said the total number of credit card numbers stolen at Home Depot could top 60 million. By comparison, the breach last year at Target, the largest known attack to date, affected 40 million cardholders.

The breach may have affected any customer at Home Depot stores in the United States and Canada from April to early last week, said Paula Drake, a company spokeswoman. Customers at Home Depot's Mexico stores were not affected, nor were online shoppers at HomeDepot.com. Personal identification numbers for debit cards were not taken, she said.

http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked

Latest News

This Week in Tech: Lawmakers take on cybersecurity

19 16 9 COMMENTS 1

By Julian Hattem - 09/08/14 08:03 AM EDT

It's going to be a busy week for cybersecurity, after a digital intrusion at HealthCare.gov raised new alarms on Capitol Hill.

The Senate Homeland Security and Governmental Affairs Committee has scheduled a hearing to explore cybersecurity and terrorism for Wednesday morning. Intelligence and digital security officials from the Department of Homeland Security (DHS), the National Counterterrorism Center and the FBI will testify.

Committee Chairman Tom Carper (D-Del.) last week called the intrusion into HealthCare.gov "deeply troubling." The hack did not result in any user's information being stolen and occurred on a test server but appeared to be launched from a foreign country.

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.

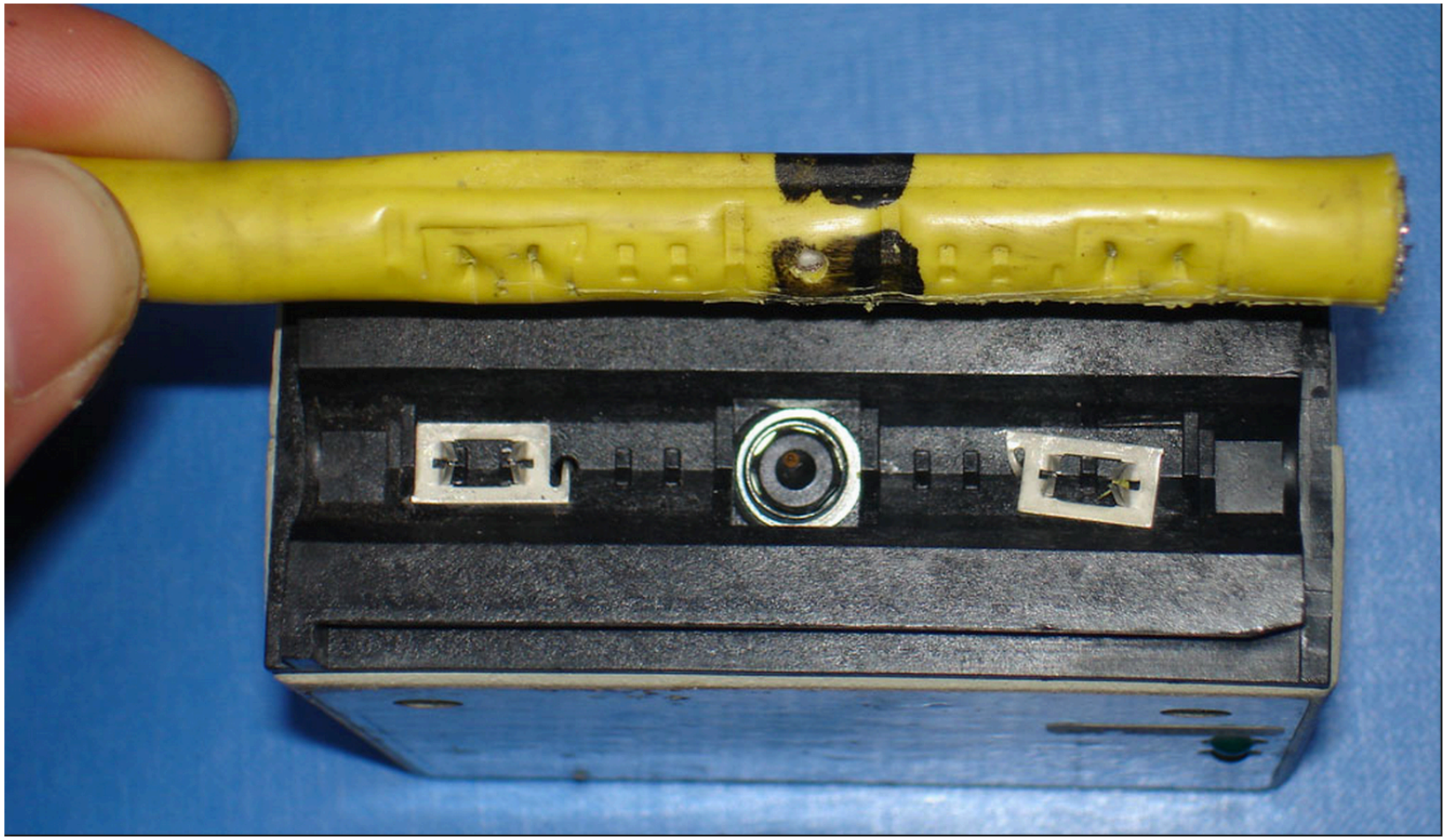
Main Goals for Today

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

Ethernet Basics

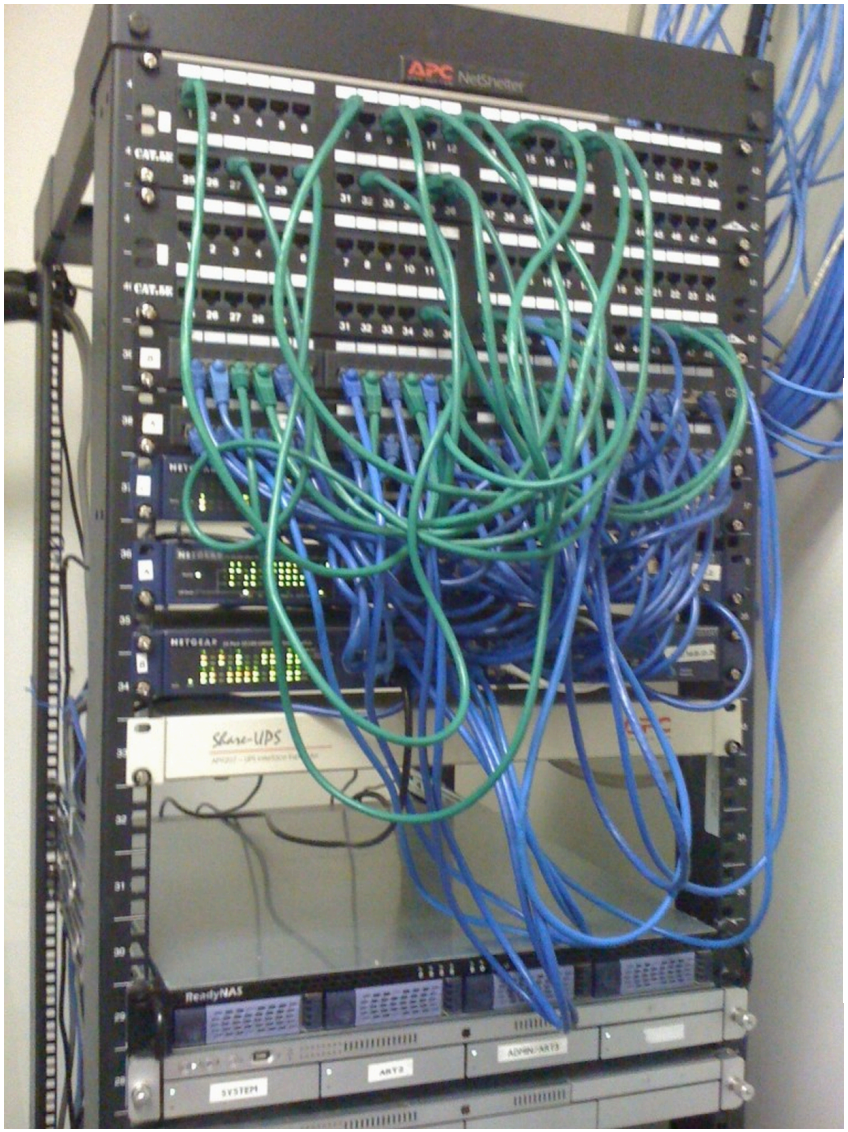
- Ethernet is a physical layer protocol/technology
  - One of many competing physical layers
  - Most popular, but others still important
    - Eg for long-haul cables
- For delivering packets of data
  - Called “frames” in ethernet lingo
  - From one machine to another
- Originally a LAN technology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

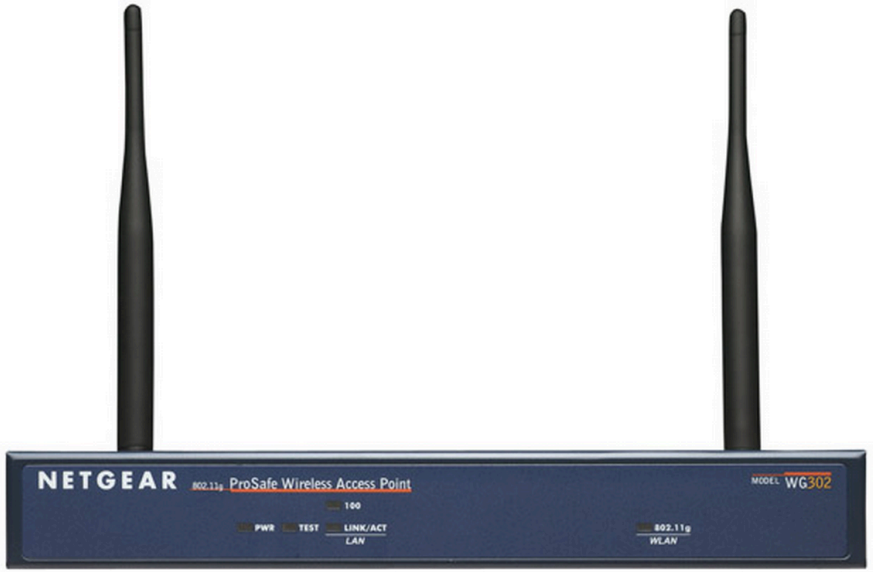
Ethernet Then



10Base5

Ethernet Now

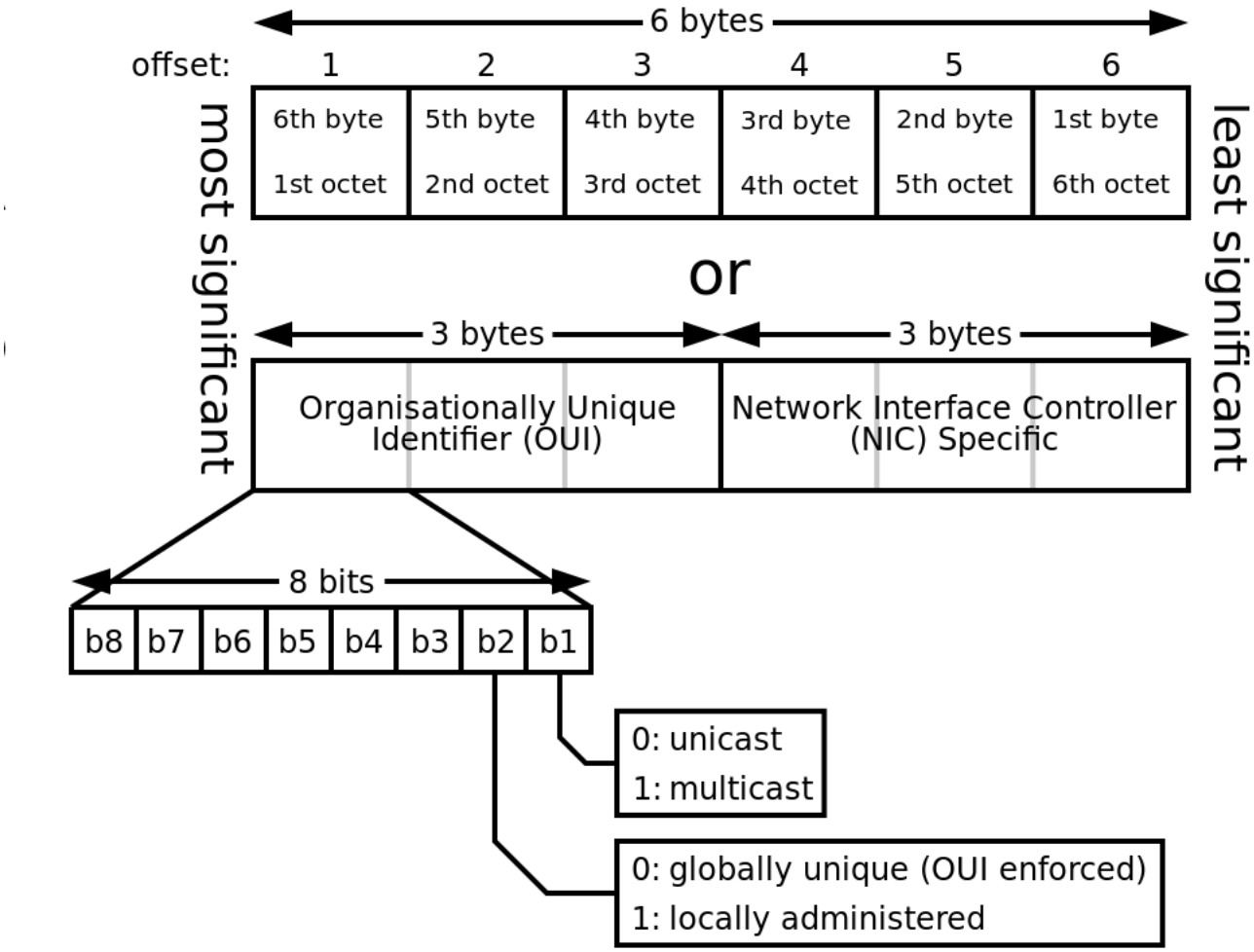




Ethernet Addresses

- 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) →								

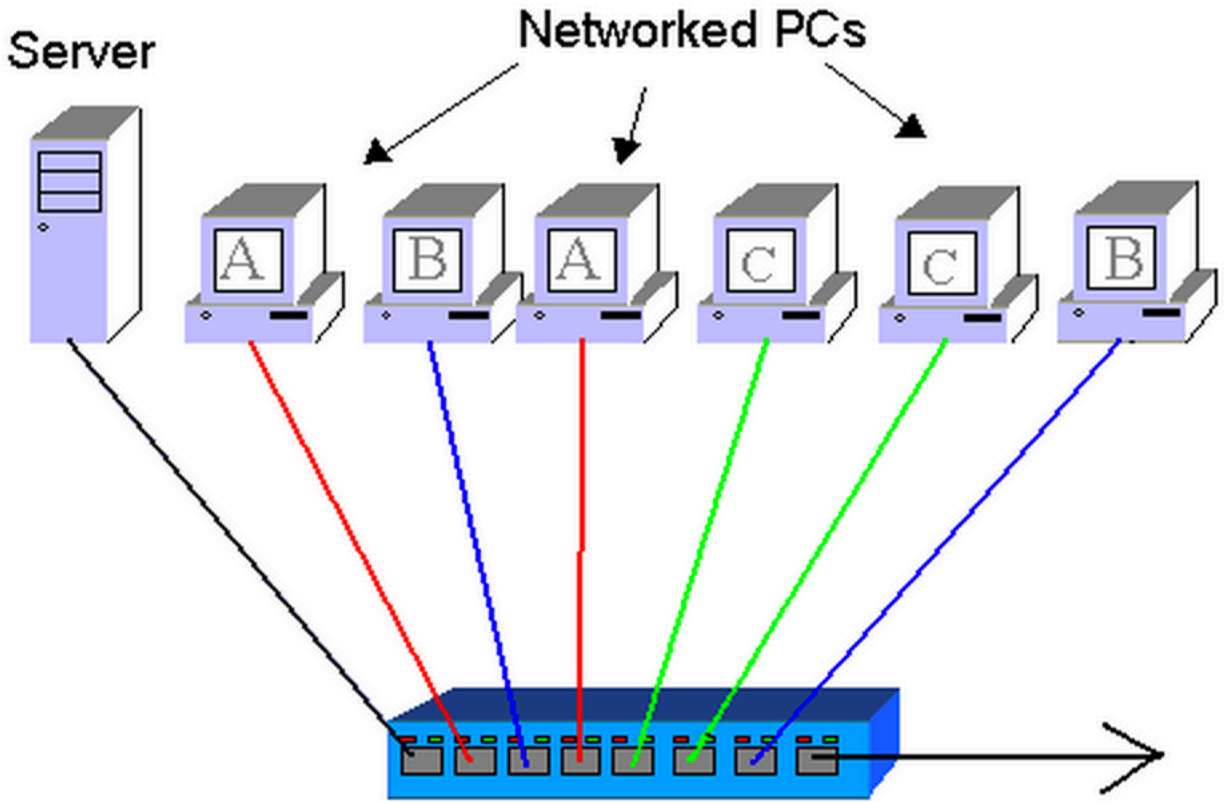
1500 is typical MTU for ethernet

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

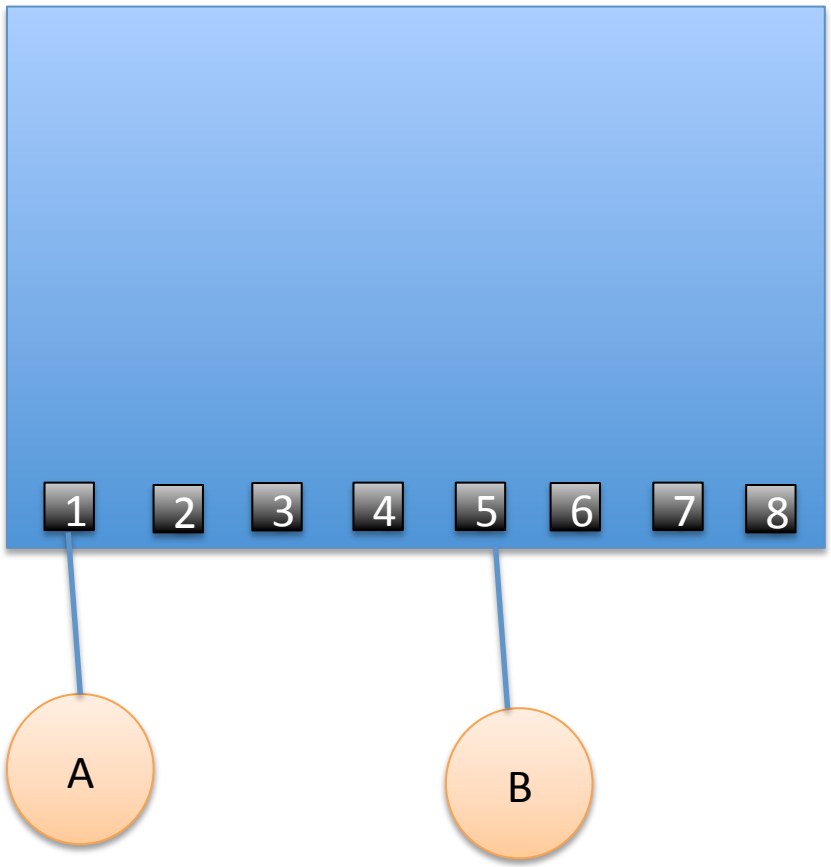
http://www.cavebear.com/archive/cavebear/Ethernet/type.html

Switched Ethernet



Source: 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

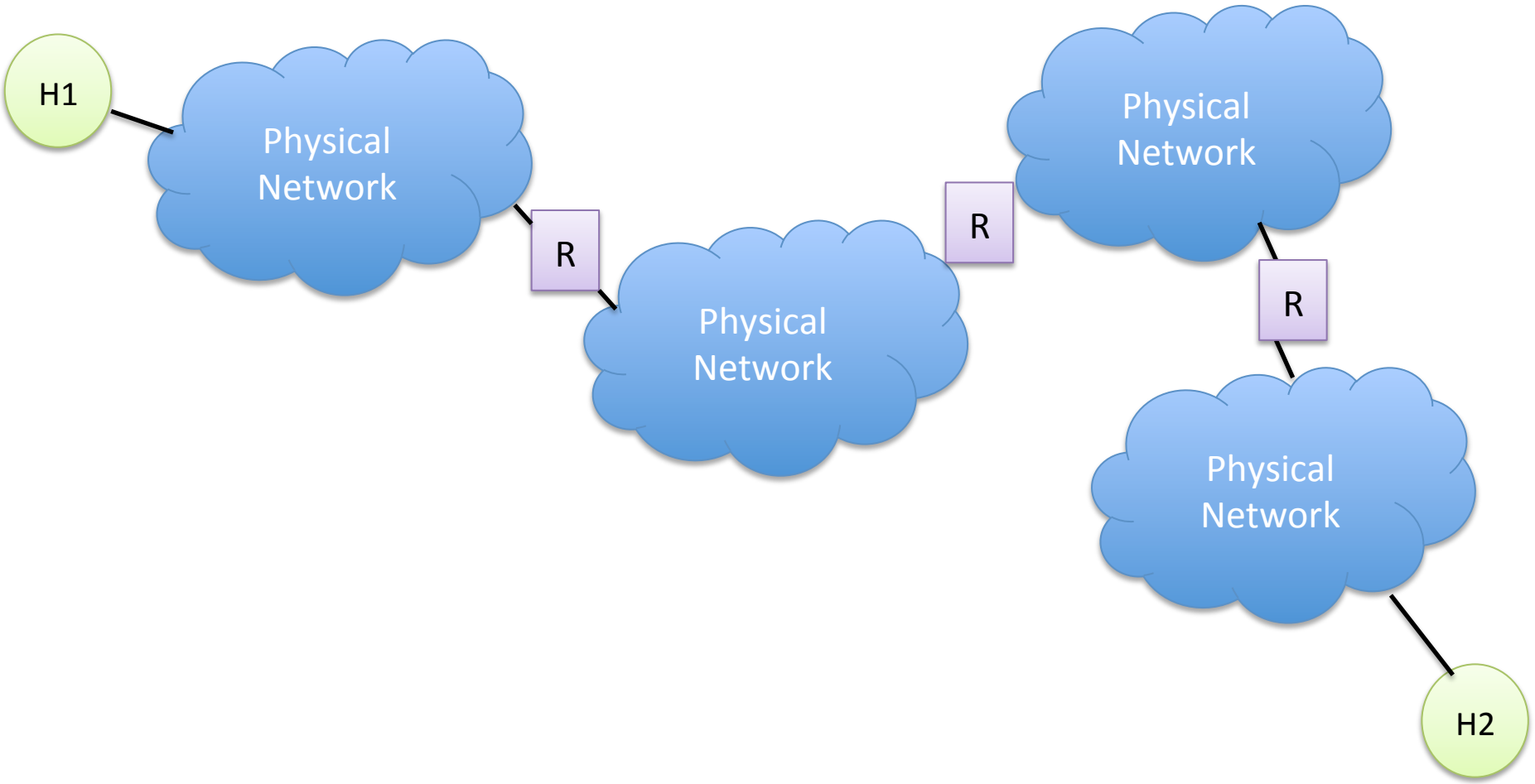
CAM Table Overflow

- 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

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

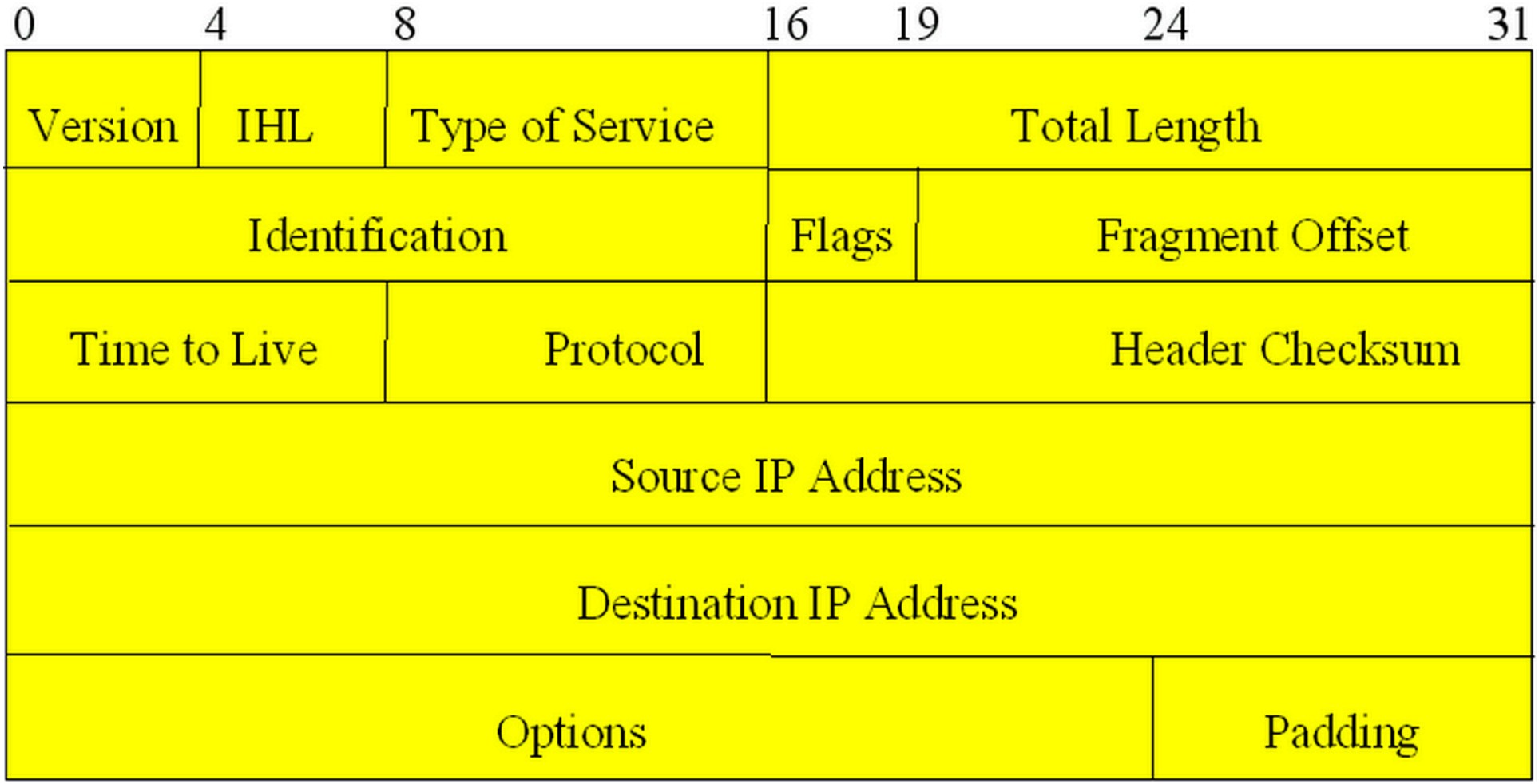
Core IP Concept



IP Address (v4)

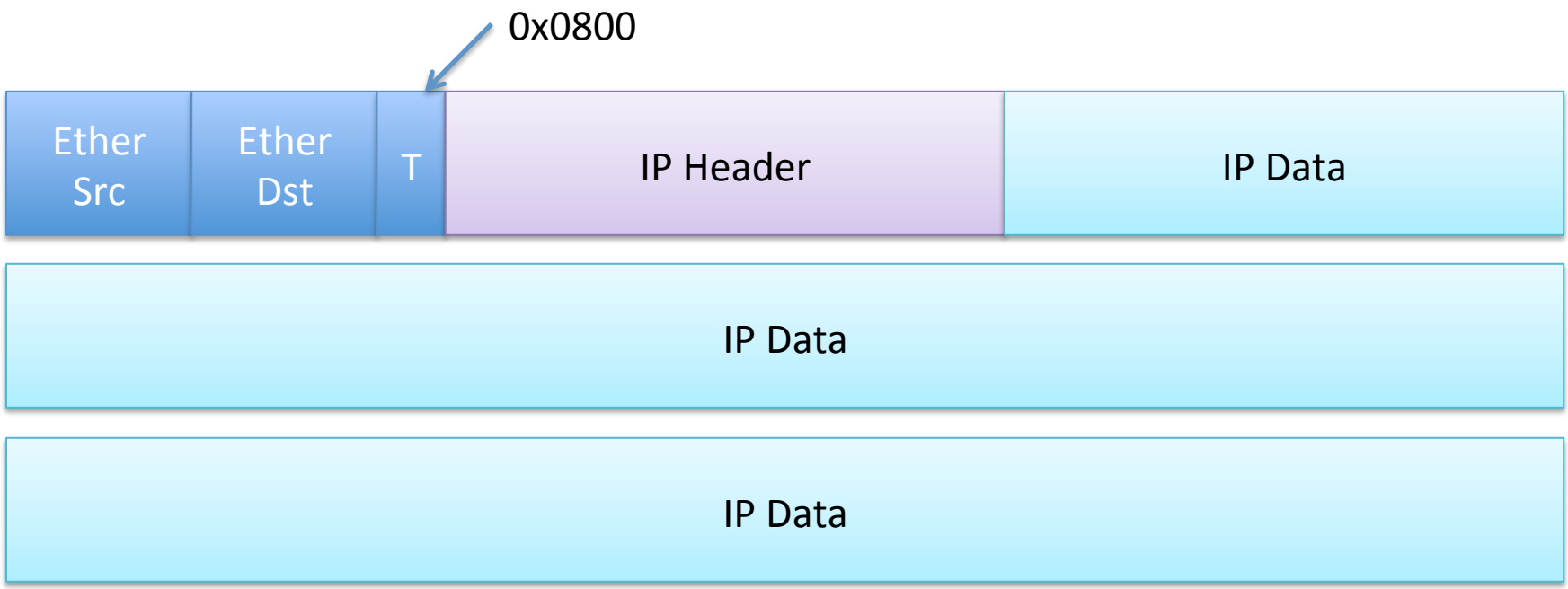
- Four bytes
- Written 192.168.254.6
  - "dotted decimal"
- Ifconfig –a
- Originally a global static identifier
  - Encoded location on Internet
  - Has become much more complex
- Example in wireshark

IP Header

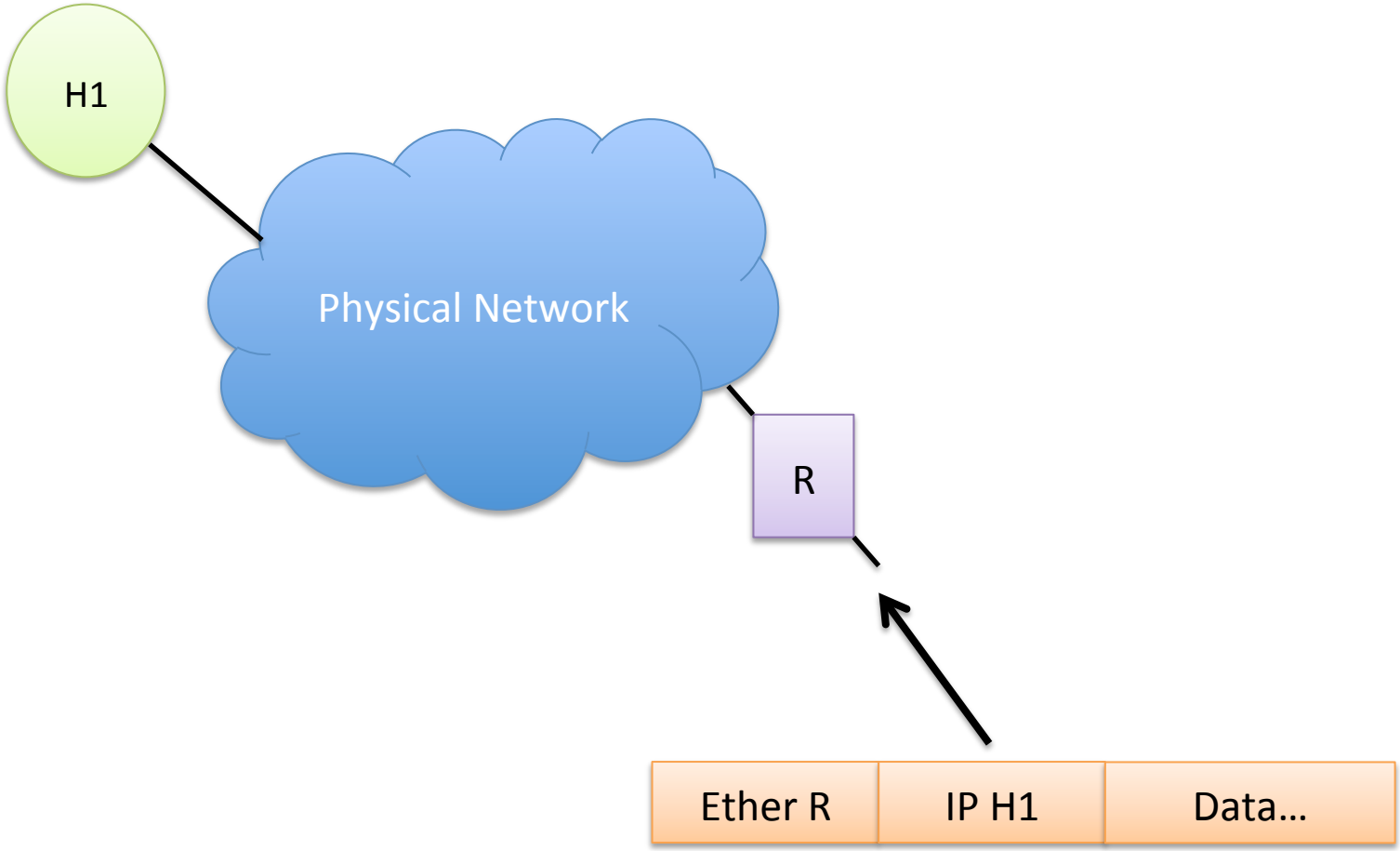


http://cs.uccs.edu/~cs522/msgformat/format.htm

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