Defending Computer Networks
Lecture 5: Intro to Networks

Stuart Staniford

Adjunct Professor of Computer Science

Logistics

- Problems registering in class still?
- T.A. Office Hours Friday 2pm-3pm (Gates 413)
- Supplementary lecture Thursday 6pm

Lost Readings

- Cowan et al *StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks*
- Shacham et al *On the Effectiveness of Address-Space Randomization*
- Hovav Shacham *The Geometry of Innocent Flesh on the Bone*

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

SALTED HASH- TOP SECURITY NEWS

By Steve Ragan | Follow

NEWS

Researcher discloses zero-day vulnerability in FireEye

NTS

On Sunday, Kristian Erik Hermansen disclosed a zero-day vulnerability in FireEye's core product, which if exploited, results in unauthorized file disclosure. As proof, he also posted a brief example of how to trigger the vulnerability and a copy of the `/etc/passwd` file. What's more, he claims to have three other vulnerabilities, and says they're for sale.

Shortly after this story went live, Hermansen responded to our email requesting additional information. He said that while working with another researcher (Ron Perris), the two discovered thirty vulnerabilities in FireEye's product, including multiple remote root issues.

"I tried for 18 months to work with FireEye through responsible channels and they balked every time. These issues need to be released because the platforms are wrought with vulnerabilities and the community needs to know, especially since these are Gov-approved Safe Harbor devices with glaring remote root vulnerabilities," Hermansen told Salted Hash via email.

"No one should be trusting these devices on their network if FireEye can't be bothered to fix the problems. As a security company, their standards should be higher."

https://fireeyeapp/script/
NEI_ModuleDispatch.php?
module=NEI_AdvancedConfig&function=HapiGet
FileContents&name=../../../../../../../../../../../etc/
passwd&extension=&category=operating
%20system
%20logs&mode=download&time=...&mytoken=...

root:aaaaa:16209:0:99999:7:::
bin:*:15628:0:99999:7:::
daemon:*:15628:0:99999:7:::
adm:*:15628:0:99999:7:::
lp:*:15628:0:99999:7:::
sync:*:15628:0:99999:7:::
shutdown:*:15628:0:99999:7:::

Researcher to FireEye: If you're not paying, I'm not talking

When asked, Hermansen was unable to confirm FireEye's statement that they've reached out to him, but he wasn't without thoughts regarding contact:

"What frustrates me is they are all ears now, when they ignored the issues for a long time," he said, adding that he will let the company sit for a bit while they try to fix what they know.

"When they implement a bug bounty or security rewards process I will reply to them. Until then, they get cold silence as reciprocity. They have been giving me lip service about implementing such a program for more than a year. Let them announce it publicly and then I will talk to them again. I'm sure there are lots of other bugs in their products that are not yet disclosed."

Again, FireEye hammered home their desire for responsible disclosure, which might lead some to think that Hermansen didn't make an honest attempt. Only, the fact is, he did try to disclose the vulnerabilities, the process failed due to financial reasons.

blackmail

n. the crime of threatening to reveal embarrassing, disgraceful or damaging facts (or rumors) about a person to the public, family, spouse or associates unless paid off to not carry out the threat. It is one form of extortion (which may include other threats such as physical harm or damage to property). (See: **extortion**)

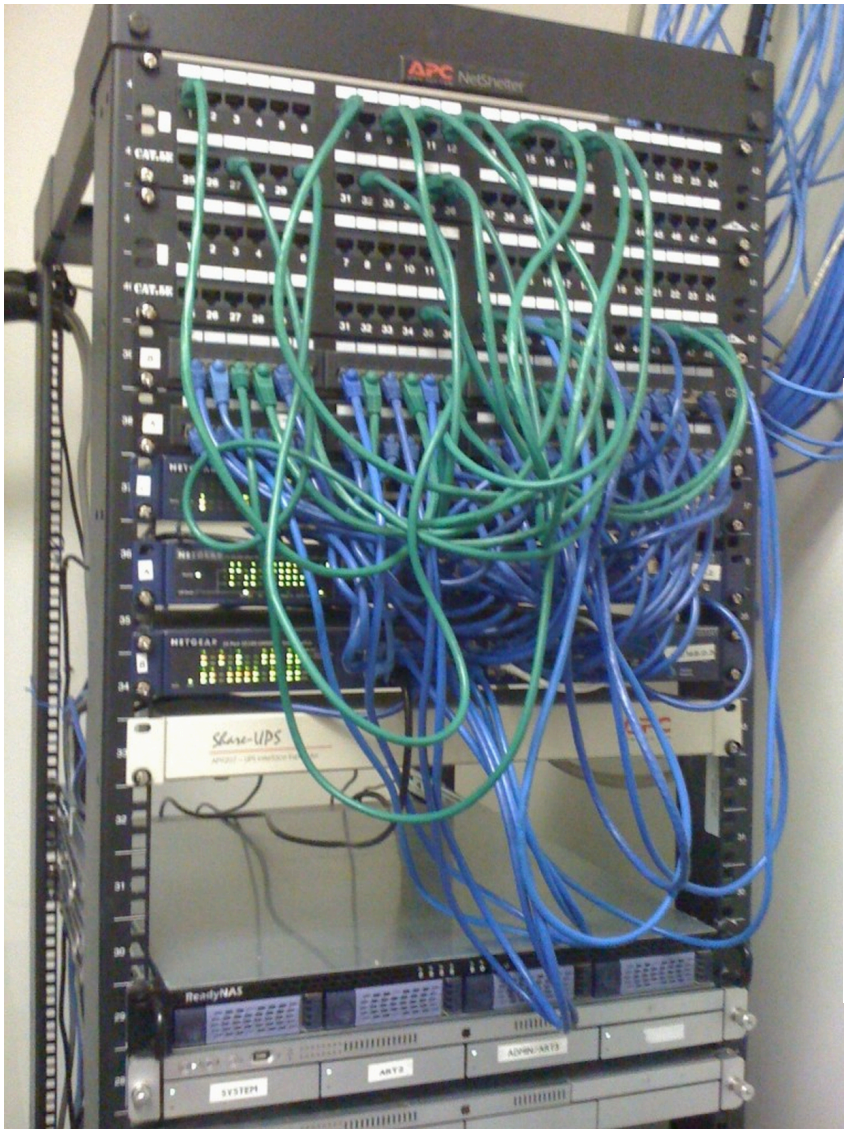
Goals for Today

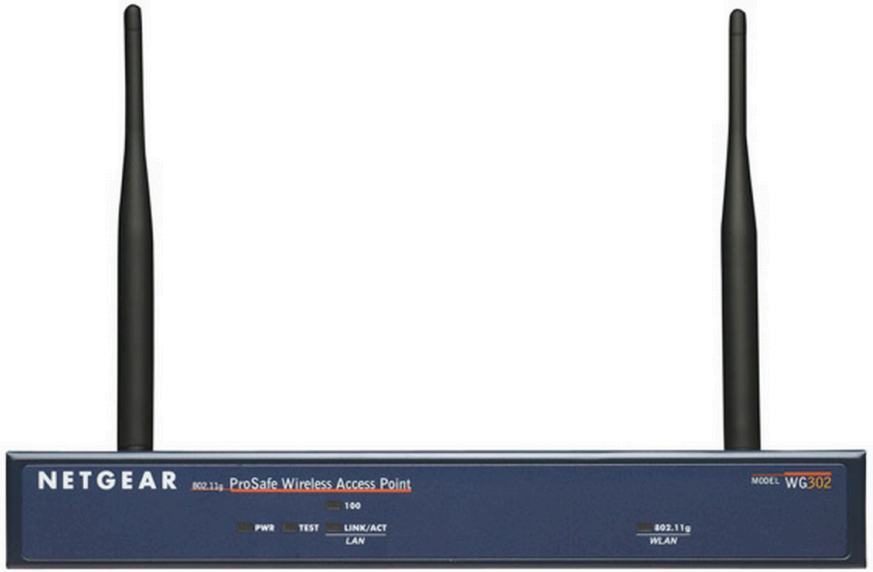
- Ethernet
- Start TCP/IP
- Relationship between them (ARP)

Ethernet Basics

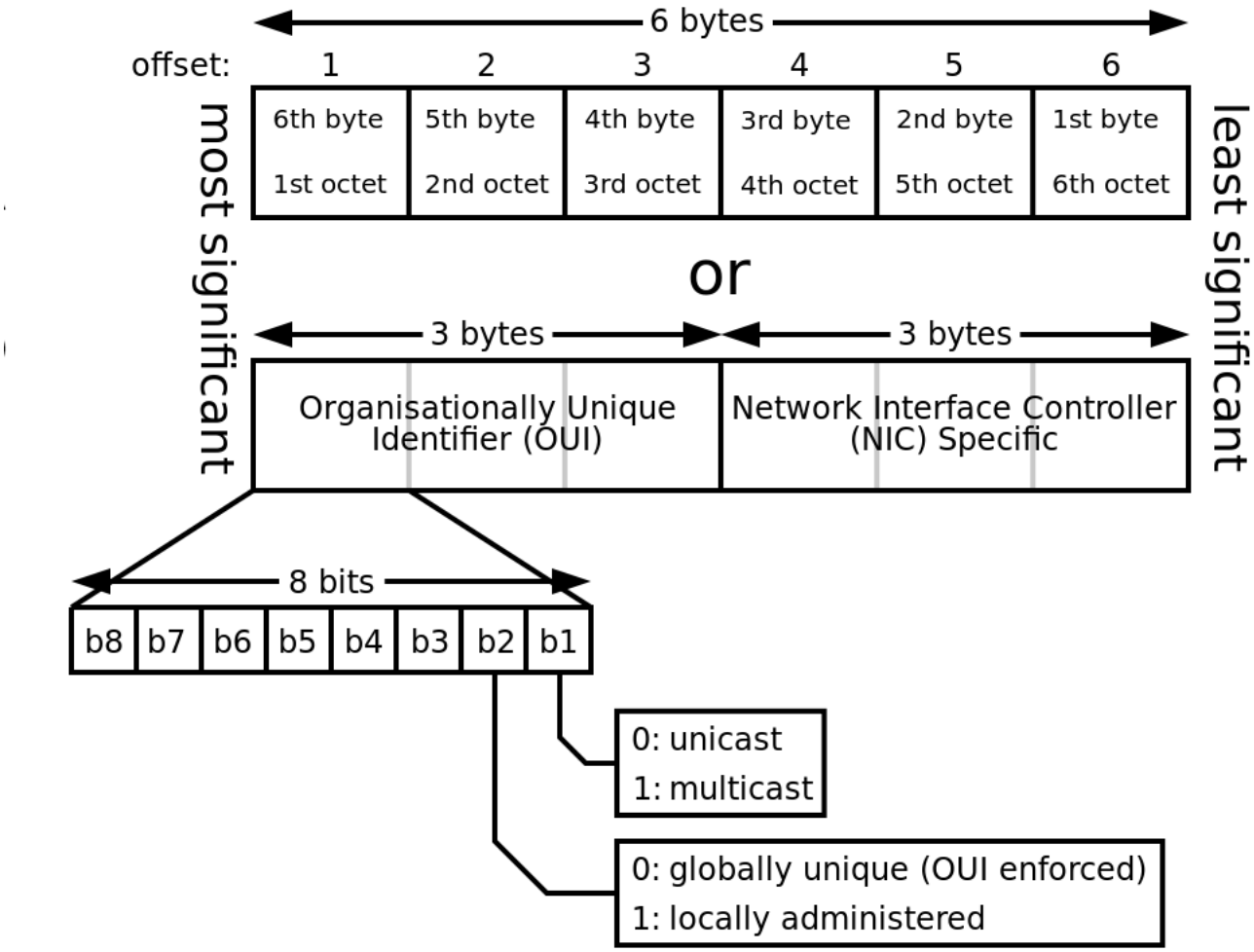
- Ethernet is a physical layer protocol/technology
  - One of many competing physical layers
  - Most popular, but others still important
    - Eg for long-haul cables
- For delivering packets of data
  - Called “frames” in ethernet lingo
  - From one machine to another
- Originally a LAN technology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

Ethernet Now





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) →								

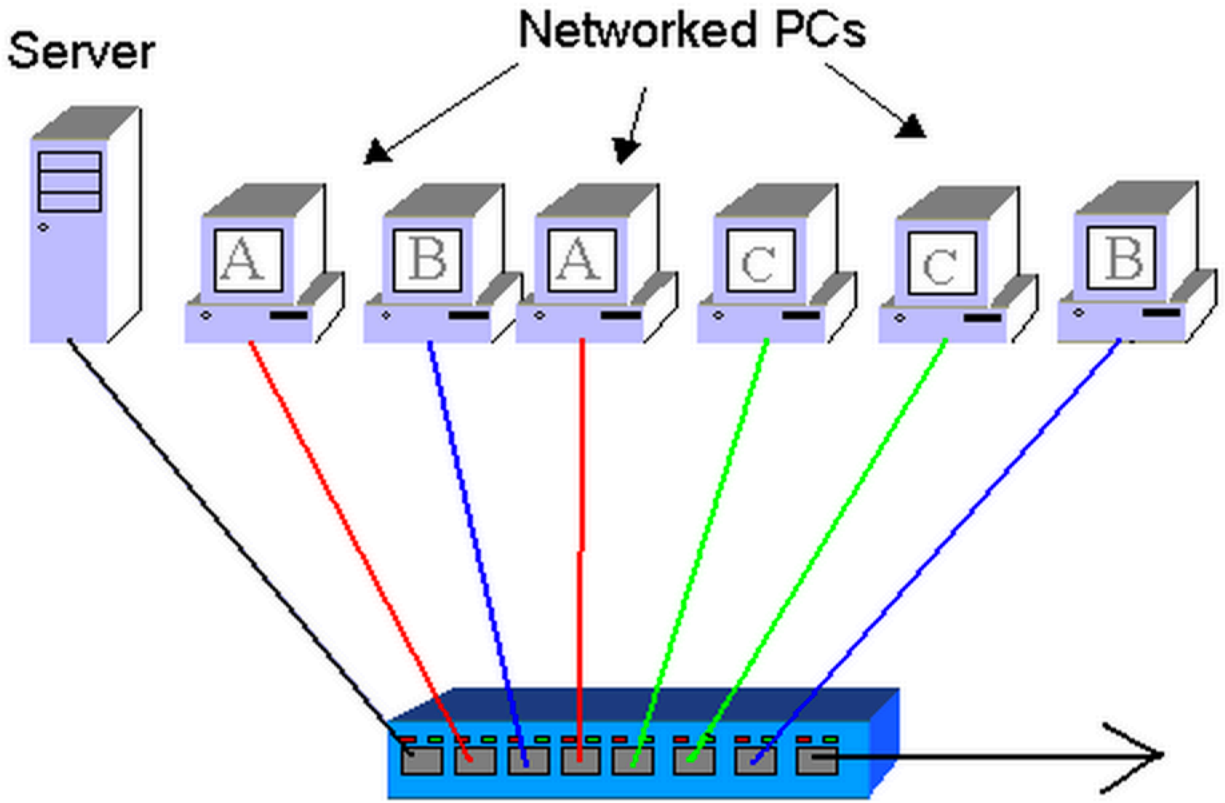
1500 is typical MTU for ethernet

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

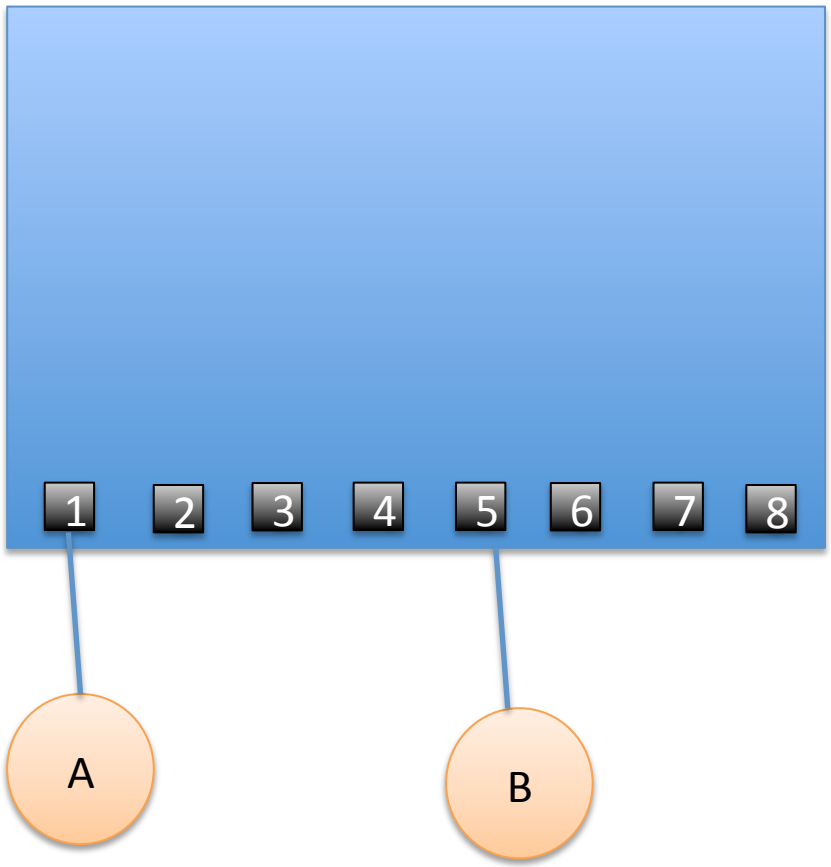
http://www.cavebear.com/archive/cavebear/Ethernet/type.html

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

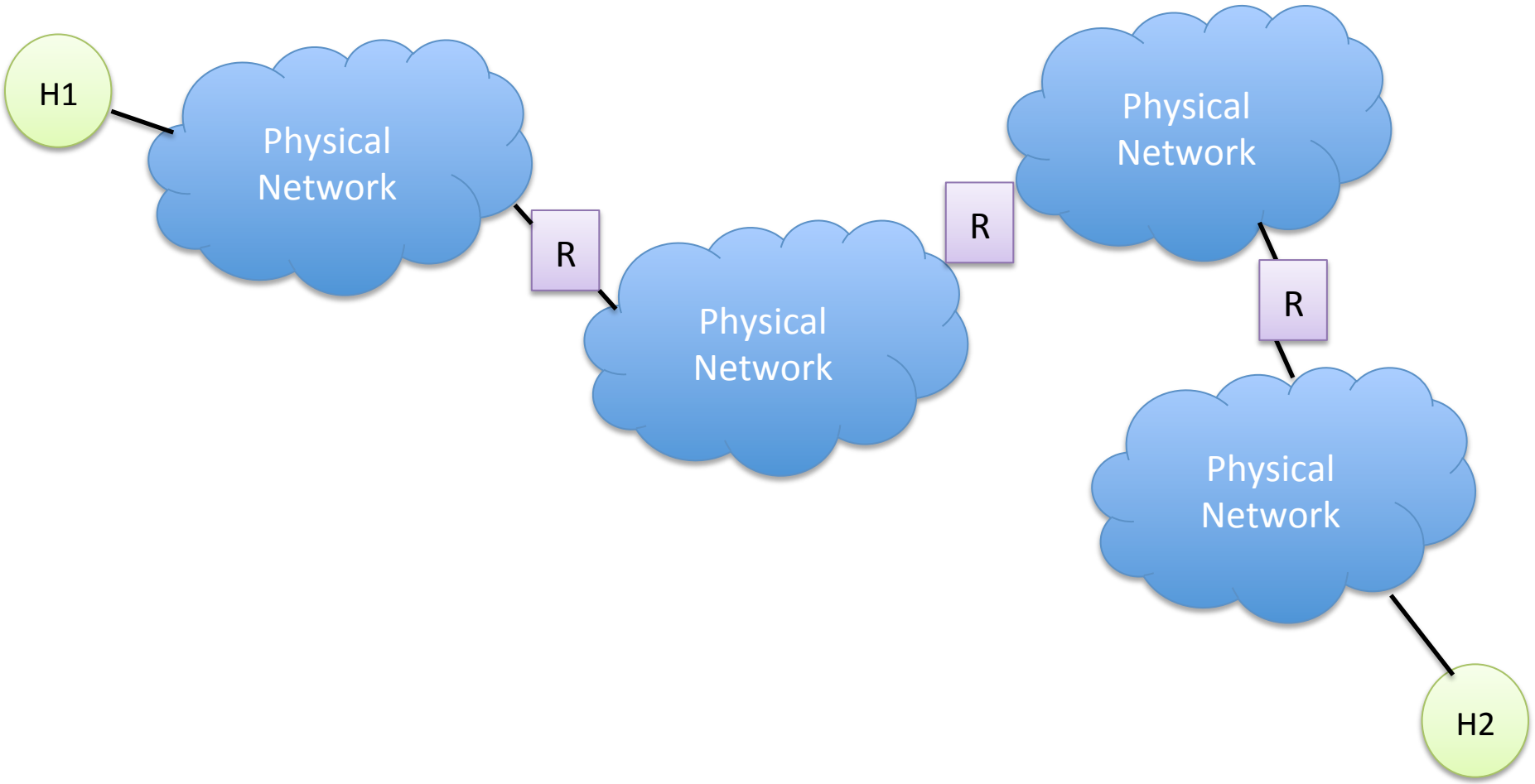
CAM Table Overflow

- 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

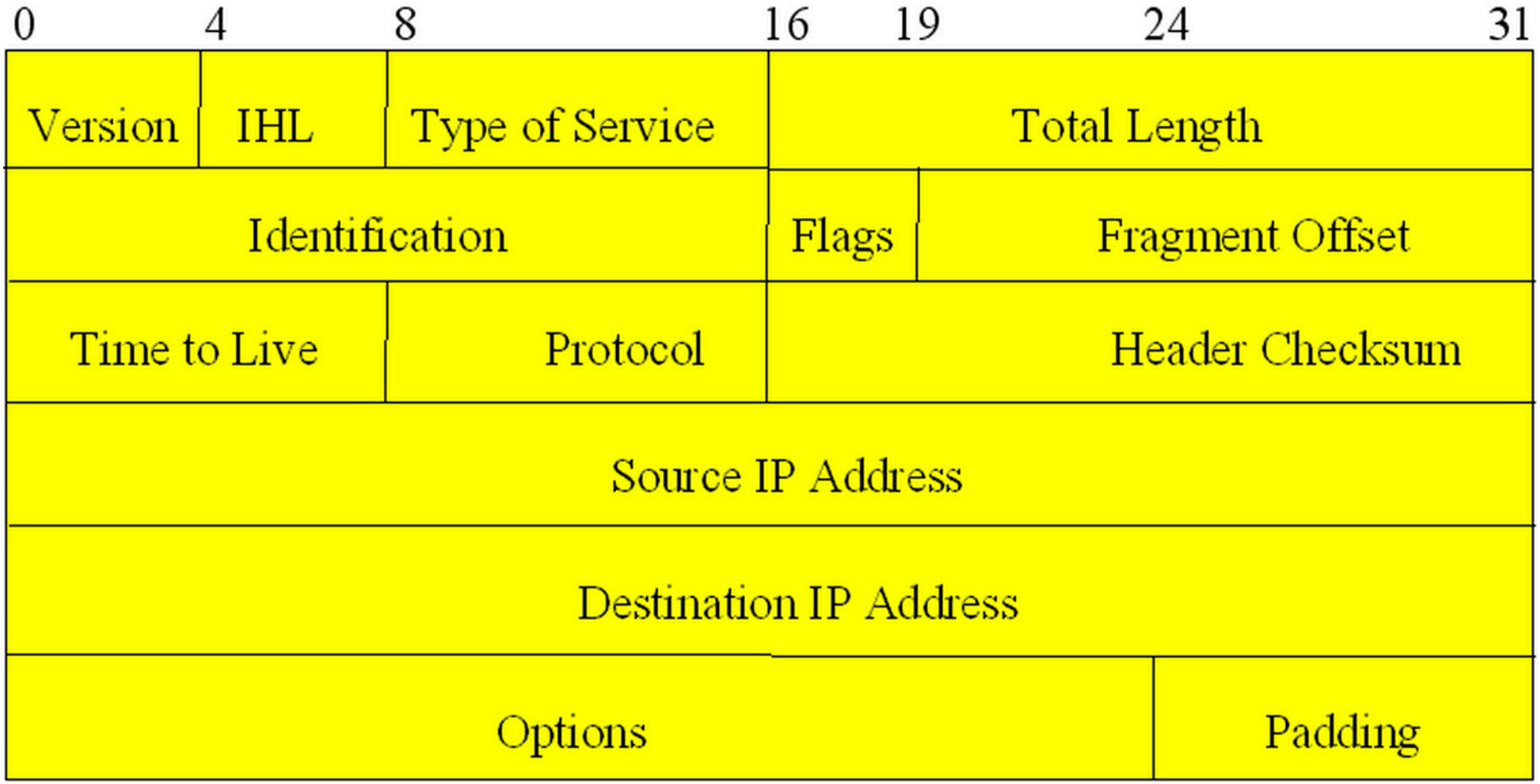
Core IP Concept



IP Address (v4)

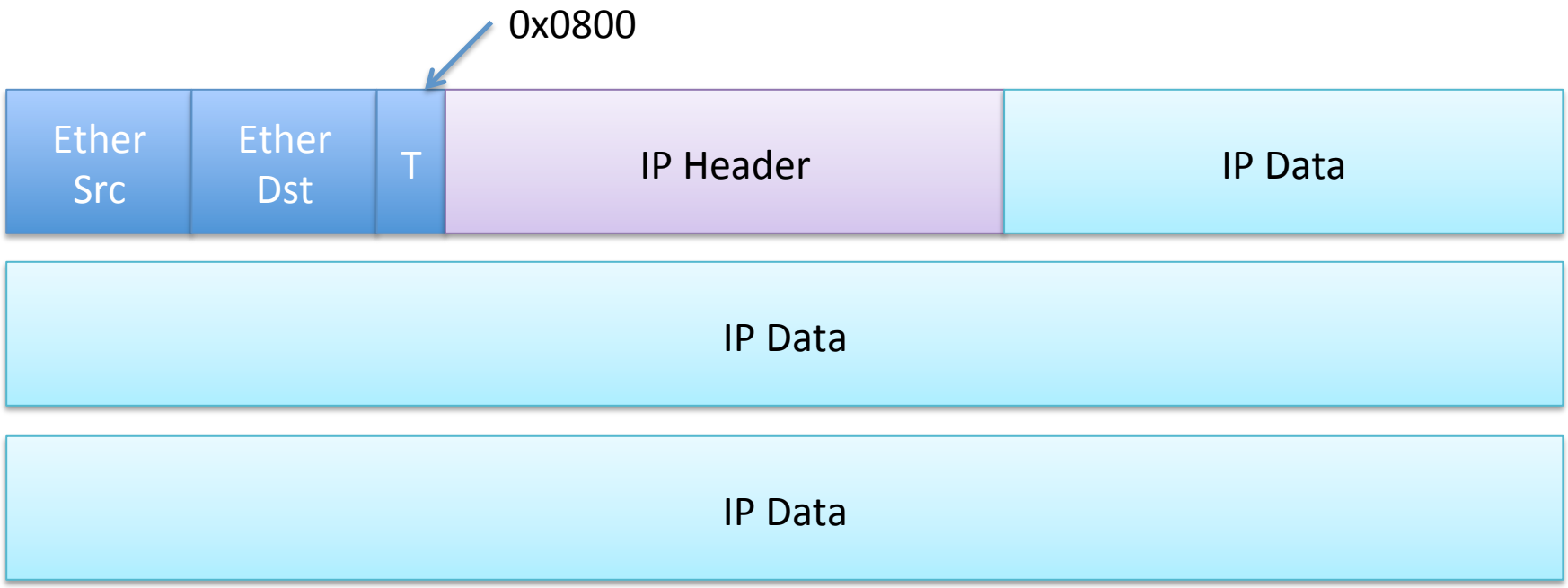
- Four bytes
- Written 192.168.254.6
  - "dotted decimal"
- Ifconfig –a
- Originally a global static identifier
  - Encoded location on Internet
  - Has become much more complex
- Example in wireshark

IP Header

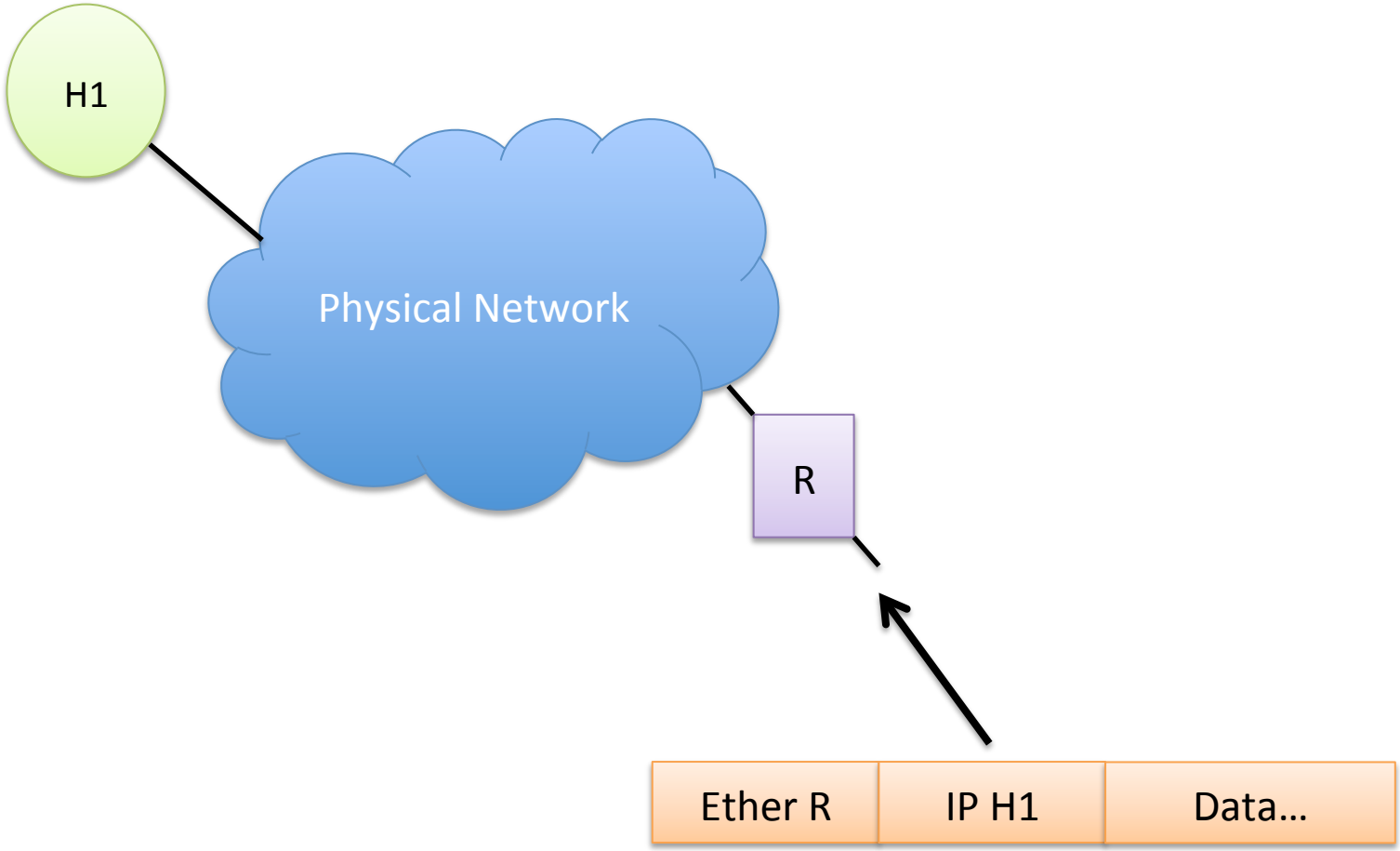


http://cs.uccs.edu/~cs522/msgformat/format.htm

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

ARP Spoofing

- Everyone that sees an arp broadcast request
  - Will associate the sender MAC/IP in their table
  - Good for low maintenance handling of change
  - Bad for security
- As a dark-arts practitioner
  - I can broadcast a request,
    - pretending to be someone else
  - Everyone will then think I'm them
  - Now I get all their traffic and can do evil

Recall

Bartemius Crouch Jr impersonating Alastor Moody

Defenses Against ARP Spoofing

- Static ARP entries
  - Works but inconvenient – doesn't scale
- Force ARP to conform to DHCP
  - Cisco Dynamic ARP Inspection (DAI)
  - Doesn't help with static IPs
    - Have to be individually configured
- Monitoring tools
  - Arpwatch (http://ee.lbl.gov/)
  - Alerts when ip addresses shift to a new ether address

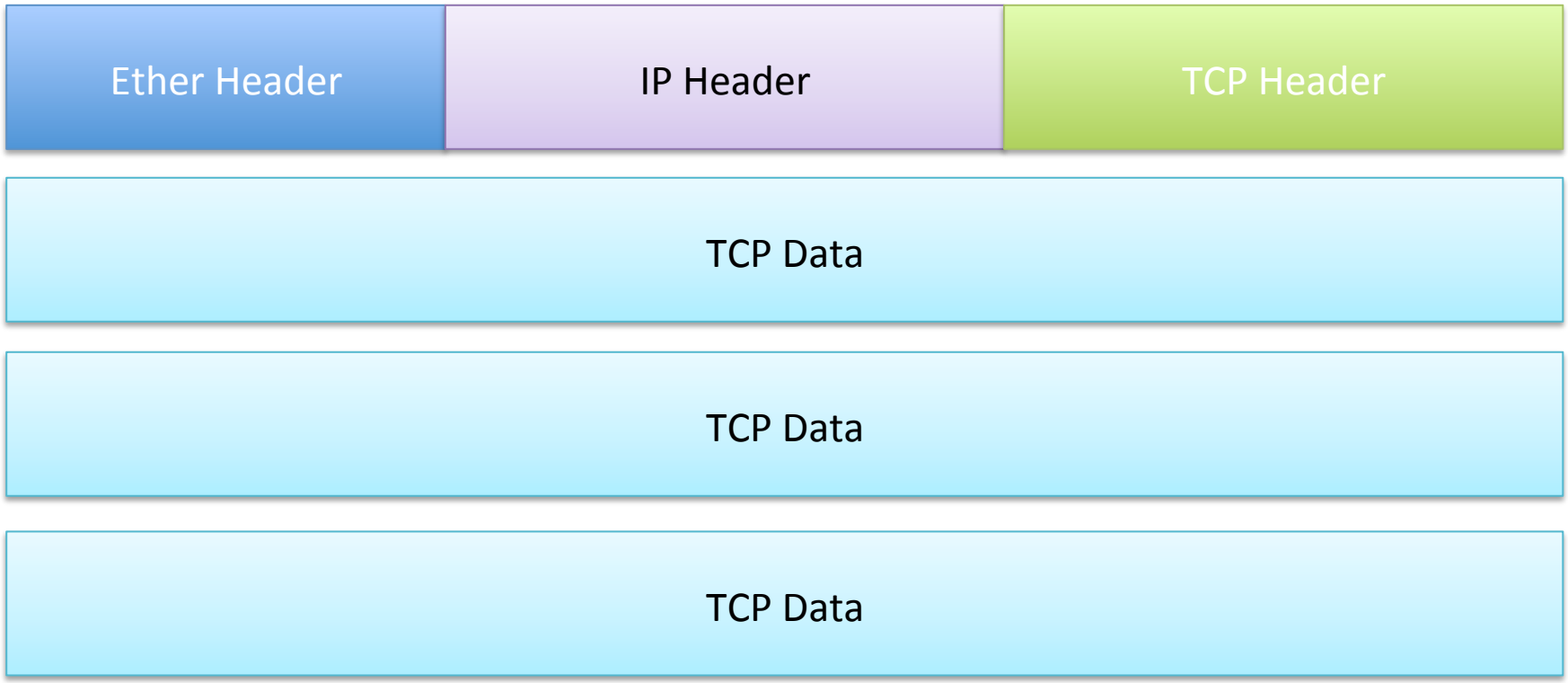
Intro to TCP

- Transmission Control Protocol
- RFC 793 (1981)
- Provides for delivery of stream of data
  - Reliably
  - In order
  - Bi-directionally
  - Between client and server *applications*
    - Not just hosts like IP

Protocol Relationship

- TCP is known as a transport layer protocol
- Goes over the network layer protocol (IP)
  - To provide additional services (reliability, etc)
- Which goes over physical layer (ethernet)
- TCP *segments* are nested inside ip packets
- Nested inside ethernet frames

Ethernet/IP/TCP Nesting



TCP Header Format