Defending Computer Networks
Lecture 6: TCP and Scanning

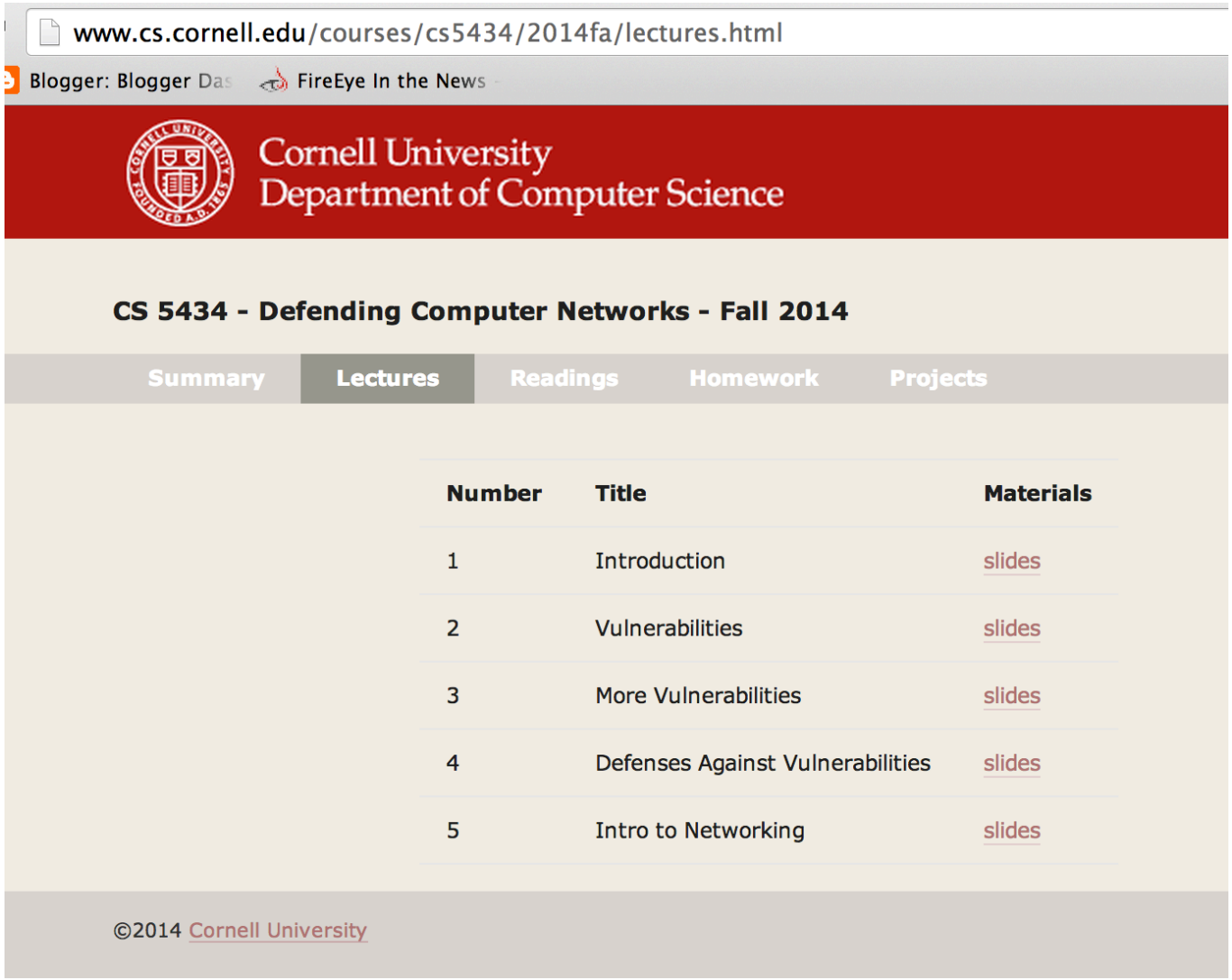
Stuart Staniford

Adjunct Professor of Computer Science

Logistics

- HW1 due tomorrow
- First quiz will be Tuesday September 23rd.
  - Half hour quiz at start of class.
  - Covering everything in class through Thurs Sep 18th and all readings assigned by then.
  - Shorter lecture will continue after quiz to end of normal timeslot.

Revision Materials



Additional Reading

- Fyodor. *The Art of Port Scanning*. http://nmap.org/p51-11.html.
  - You can skim the code section if time pressed.
- Note again you are being pointed at intro papers that are dated.
  - Have to start somewhere.
  - Practical network attack/defense is not a timeless body of knowledge.
  - Constantly evolving arms race between attackers and defenders coming up with new techniques.

Latest News

USIS to lose federal contracts after cyberattack compromises security of 25,000 government workers

By The Associated Press September 9, 2014 - 08:07 pm

WASHINGTON (AP) - A congressional spokeswoman says the federal Office of Personnel Management plans to terminate its massive contracts with USIS, the major security clearance contractor that was targeted last month by a cyberattack. The computer network intrusion compromised the personal files of as many as 25,000 government workers.

More on this story

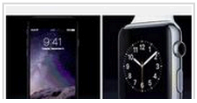
- Security breach hits 25,000 federal workers

Marnee Banks, spokeswoman for Sen. Jon Tester of Montana, says OPM officials notified Tester's office Tuesday that the agency had decided to sever its relationship with USIS by the end of September. An official announcement is expected Wednesday.

The Virginia-based contractor handles almost half of the security clearances for more than 5 million government workers and also provides support for numerous agencies.

Hot on WJLA.com

Today's most talked about stories



Apple unveils new iPh larger iPhone 6 Plus a smartwatch

http://www.wjla.com/articles/2014/09/usis-to-lose-government-work-after-cyberattack-compromises-security-of-25-000-government-workers-106.html

More News

Digital jihad: ISIS, Al Qaeda seek a cyber caliphate to launch attacks on US

By **Jamie Dettmer** · Published September 11, 2014 · FoxNews.com 210 463 112

Jihadists in the Middle East are ramping up efforts to mount a massive cyber attack on the U.S., with leaders from both Islamic State and Al Qaeda - including a hacker who once broke into former British Prime Minister Tony Blair's Gmail account - recruiting web savvy radicals, FoxNews.com has learned.

Islamic militants brag online that it is only a matter of time before they manage to pull off a highly disruptive attack on America's infrastructure or financial system. In addition, Islamic State, the terror group that claims to have established a caliphate across Syria and Iraq, boast openly of plans to establish a "cyber caliphate," protected by jihadist developed encryption software from behind which they hope to mount catastrophic hacking and virus attacks on America and the West.

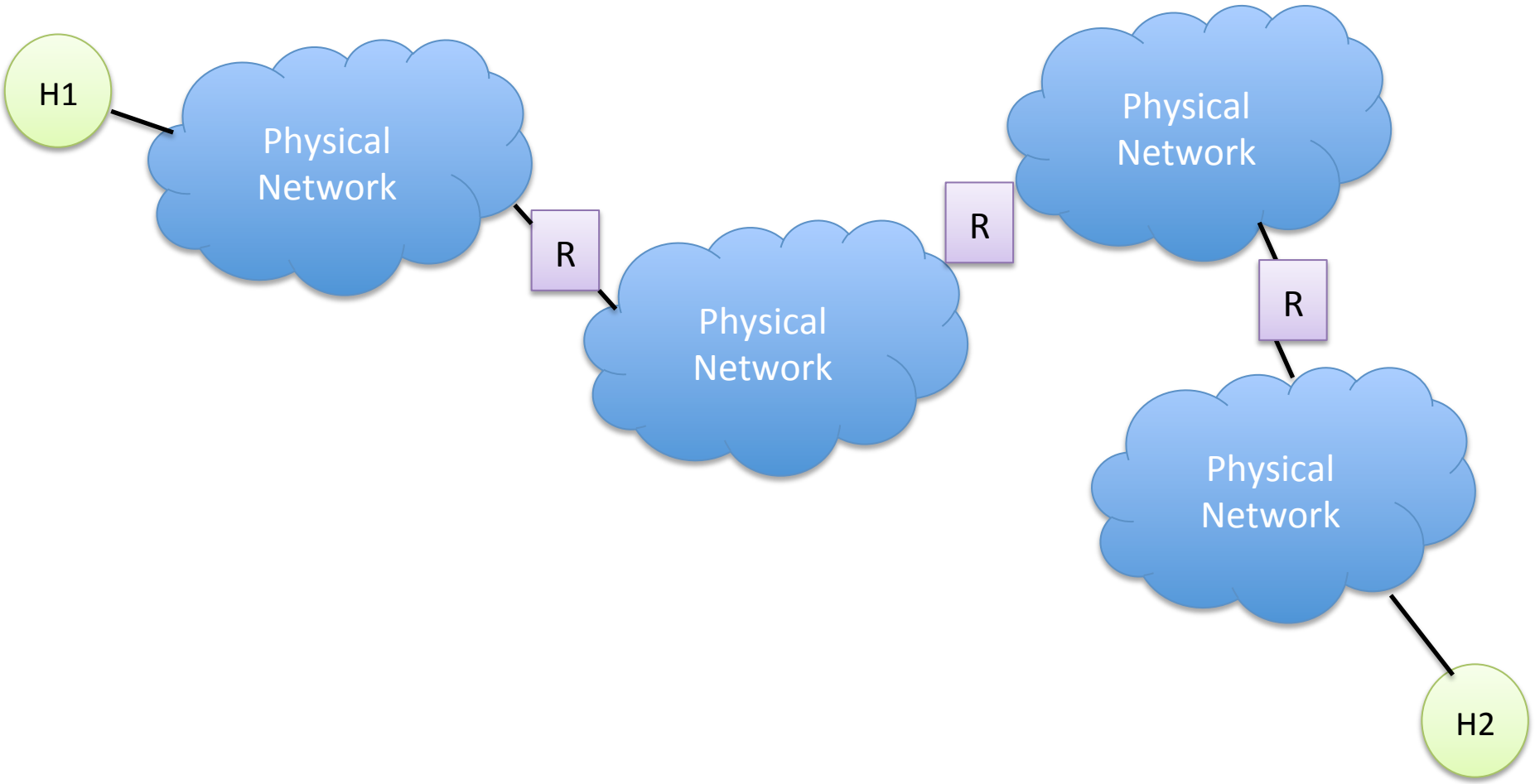
World Video

http://www.foxnews.com/world/2014/09/11/digital-jihad-isis-al-qaeda-seek-cyber-caliphate-to-launch-attacks-on-us/

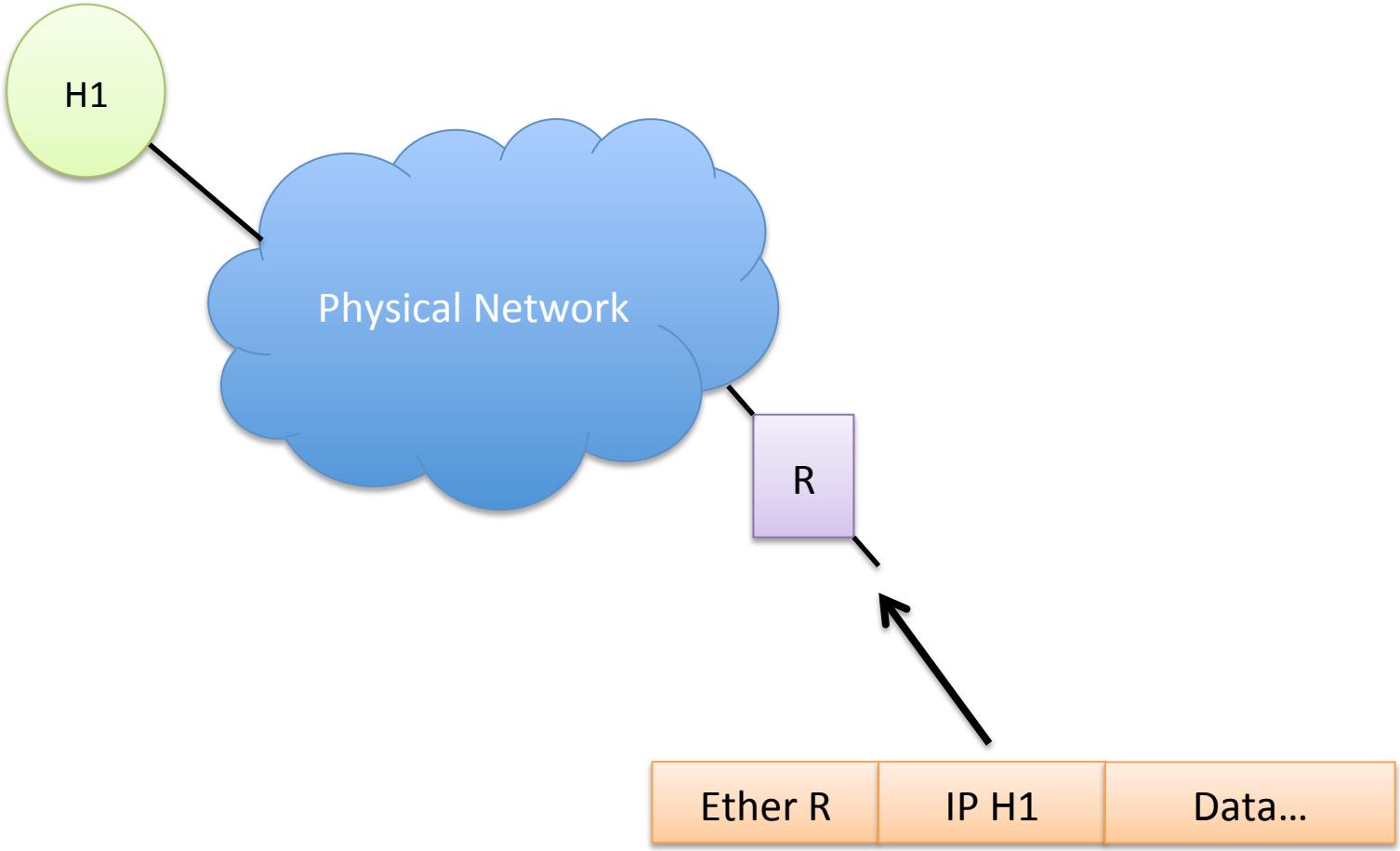
Main Goals for Today

- Finish up Arp Spoofing from Last Time
- Basics of TCP Protocol
- IP Address Space
- Leading to port scanning
  - Maybe start today
  - HW2 will be building a simple portscanner

Refresh on Ether/IP



Address Resolution: The Problem



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

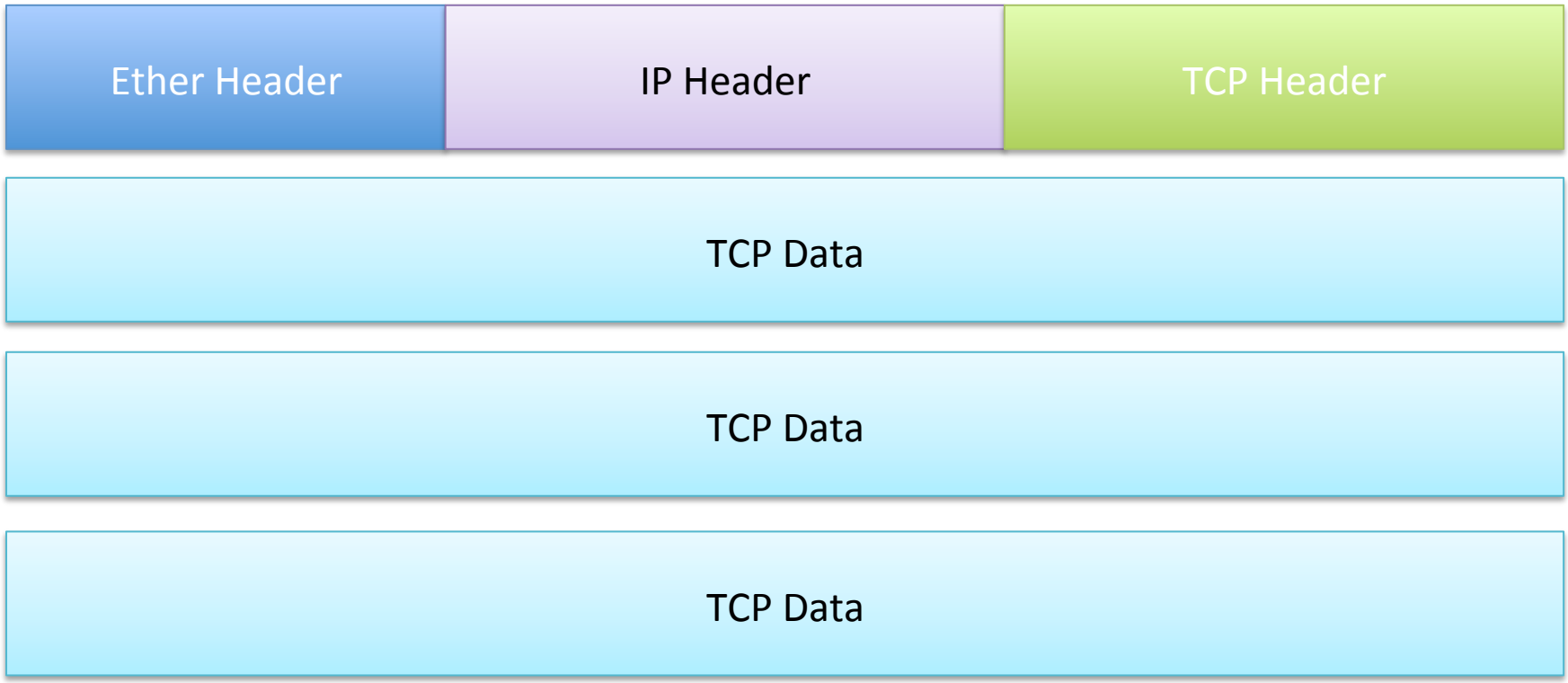
Intro to TCP

- 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

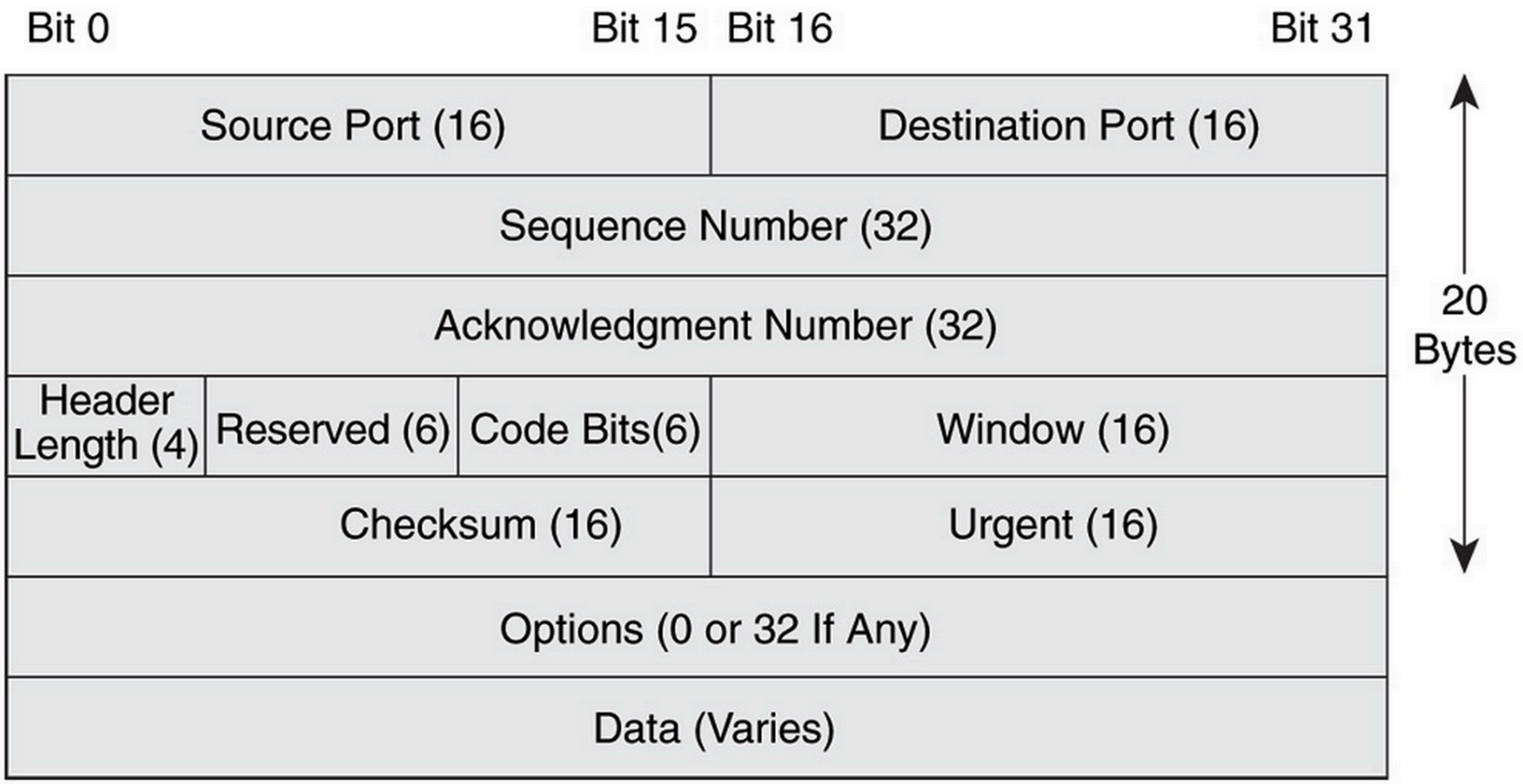
Protocol Relationship

- 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



TCP Port Number

- 2 byte quantity (so 65536 possible port #s)
- Server binds to a fixed port
  - Typically "well known" (below 1024):
    - HTTP: 80
    - HTTPS: 443
    - SMTP: 25
    - SSH: 22
- Client typically is assigned a port by OS
  - High numbered
- In some high volume situations port numbers wrap after a while

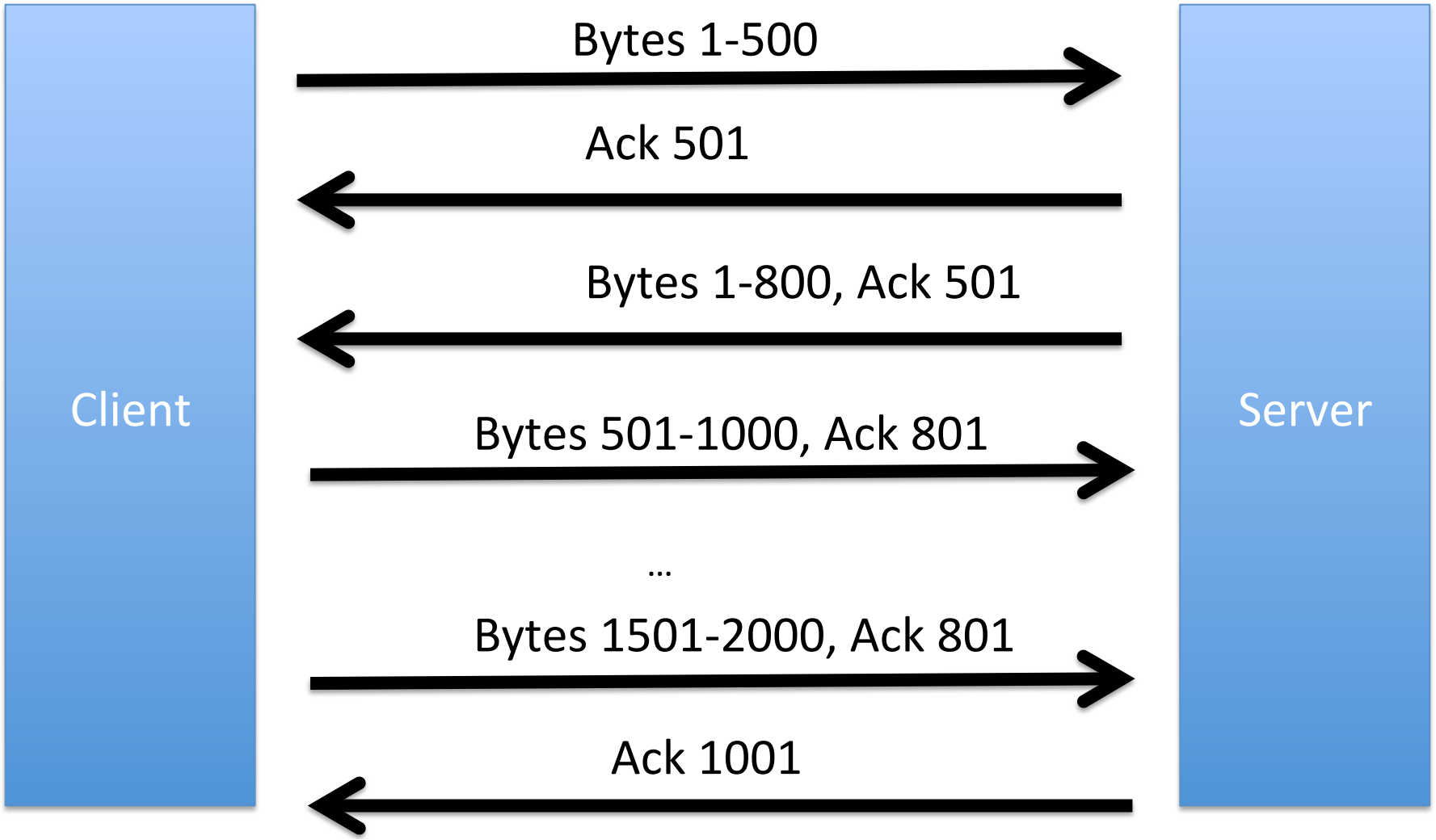
TCP Connections

- Name for the bidirectional stream
  - Between client application and server application
- Defined by the fivetuple
  - Source IP
  - Source port
  - Dest IP
  - Dest port
  - Time

How Reliability/In-Order is done

- Checksums to detect outright transmission error
  - Retransmit if bad
- 32 bit sequence numbers for each byte
  - To detect missing data
  - Retransmit if doesn't show up after a while
- Each segment can
  - Carry some data (indicated by seq number)
  - Acknowledge some data in other direction
    - Ack sequence number

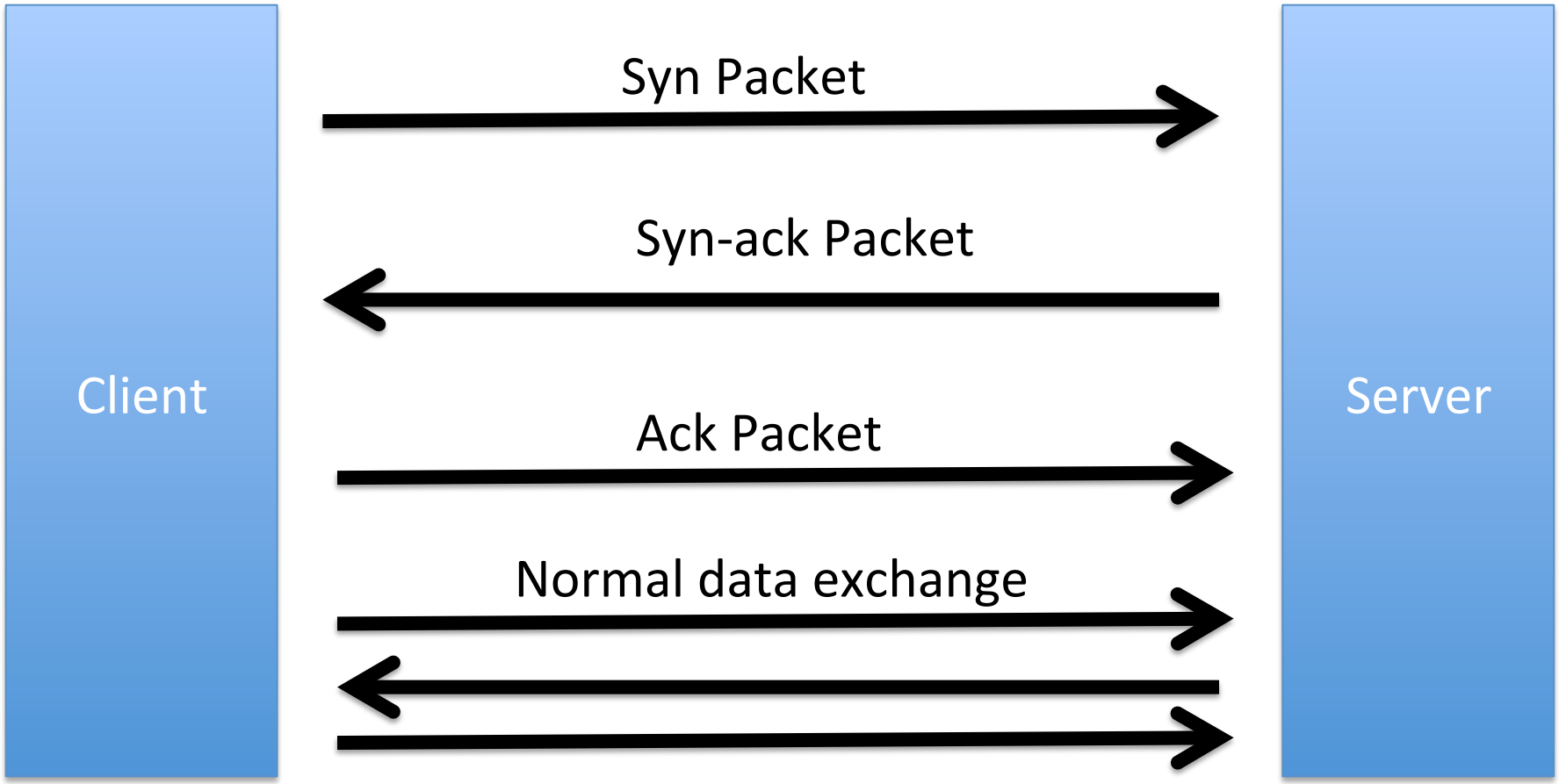
Let's work through an example



TCP 3-way handshake

- Serves to have client and server agree they are talking
- Also establishes initial sequence numbers
  - In both directions
  - Can't have fixed start (eg zero)
  - Too easy for bad guys if predictable
    - A man in the middle can interfere

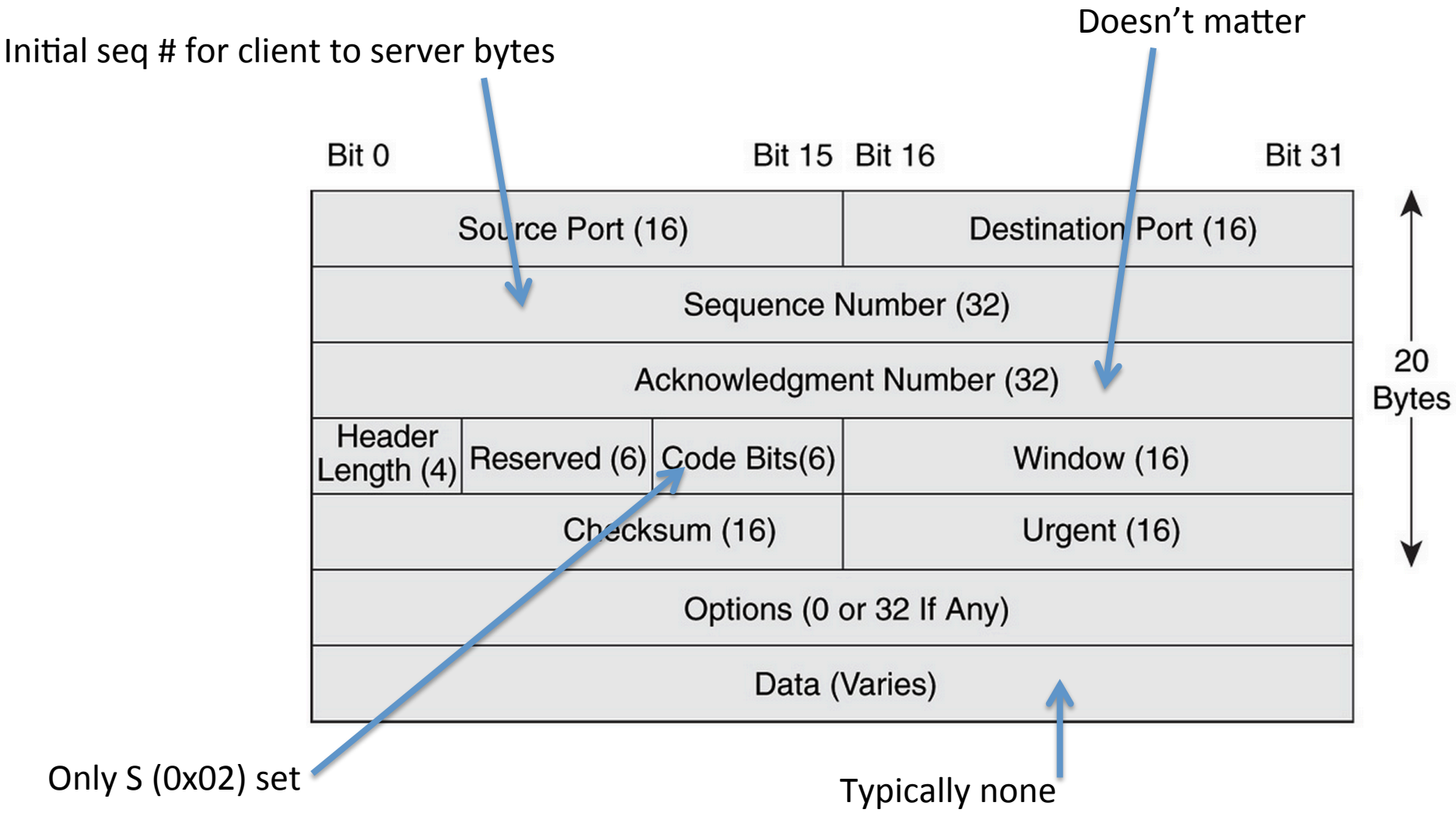
Handshake packets



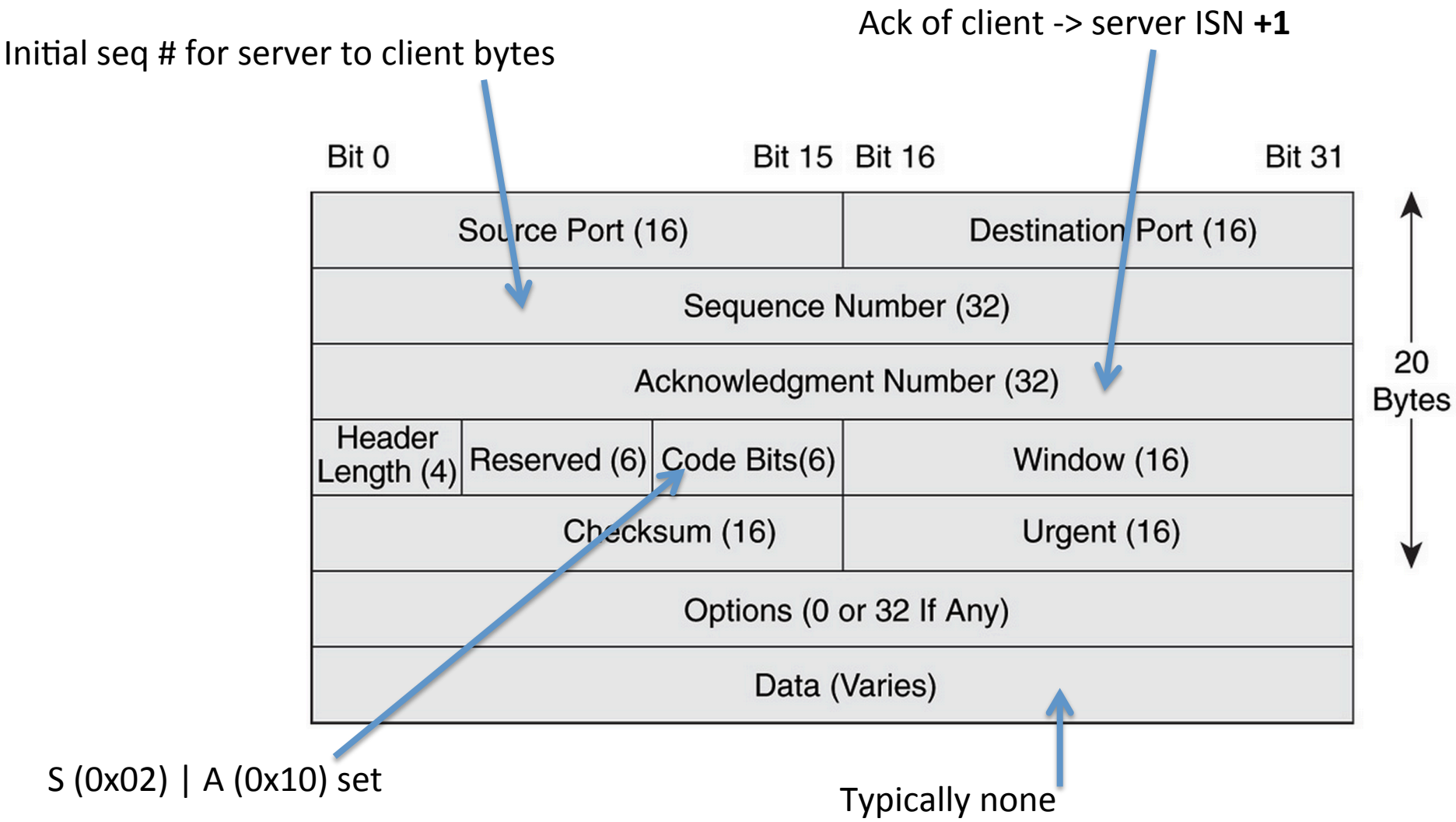
“Syn Packet”

- First packet in handshake
- Makes use of TCP flags byte field in header
  - 0x01 FIN (F)
  - 0x02 SYN (S)
  - 0x04 RST (R)
  - 0x08 PSH (P)
  - 0x10 ACK (A)
  - 0x20 URG (U)
  - 0x40 ECE
  - 0x80 CWR

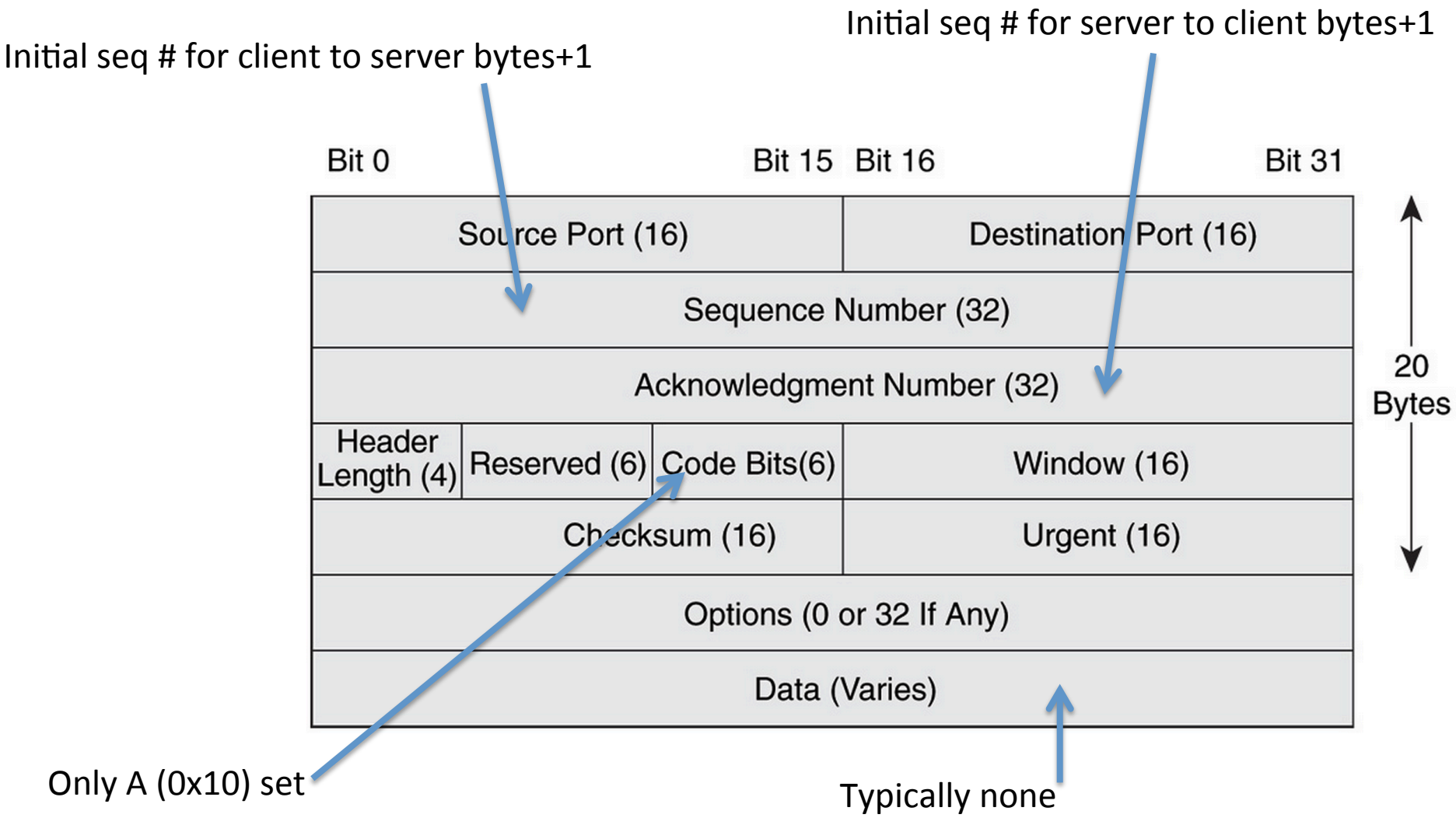
Syn Packet Layout



Syn-ack packet



Final Handshake Ack



IP Address Space

- Different organizations get different amounts
  - Class A: x.0.0.0/8 (2^{24} = 16,777,216)
    - x.1.1.1 is in, as is x.254.254.254)
    - Huge org eg (DOD is 11.0.0.0/8 IBM is 9.0.0.0/8)
  - Class B: x.y.0.0/16 (2^{16} = 65536)
    - Mid-sized organization
      - eg Cornell has 128.253.0.0/16, 128.84.0.0/16, 132.236.0.0/16 and 140.251.0.0/16
  - Class C: x.y.z.0/24 (2^{8} = 256)
    - Small organizations.
  - Can also have intermediate bitmasks.
    - eg /22

Internal Address Spaces

- RFC 1918
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- These addresses are not “routable”
- They will not be delivered across the Internet
  - Not allowed on there, technically.
- Need a special translator device at boundary
  - “NAT box” = Network Address Translation
  - Converts them to internet routable addresses

Port Scan Scenarios

- Bad guy wants to map an address space
  - Old style: across the internet
    - Still happens for internet facing servers
    - But rarely can map entire networks any more
  - Newer style: has a compromised machine on an internal network
  - Wants to know “what servers are here?”
  - Specifically, which machines have open ports?

Class B Portscan Example

- 2^16 addresses
- Say bad guy just scans on port 80
  - Eg say he knows an IIS or Apache exploit.
  - Send out 2^{16} syn packets to port 80
    - x.y.0.0, x.y.0.1, x.y.0.2,… x.y.255.254
  - "Horizontal scan on port 80"
  - See who sends back a syn-ack.
    - Means they have a process answering on port 80.
  - Find all the web servers this way.
  - Attack em!
    - Start with sending an ack pkt to establish conn.
    - Or not – if we don't send the 3rd handshake, system typically won't log.
      - Half-open connection

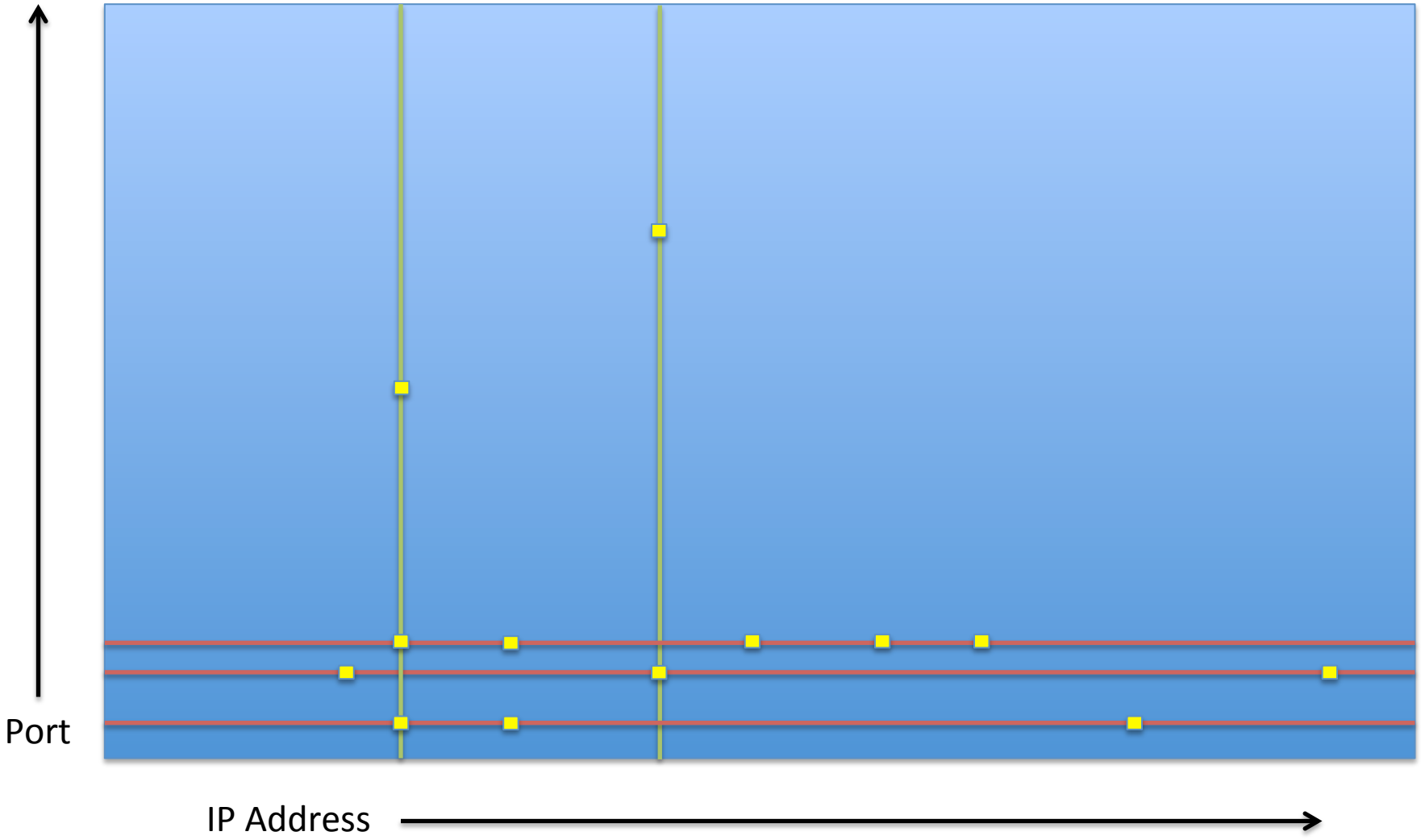
Vertical Port Scan of 1 IP

- Targetting a single IP address.
- Scan all 2^{16} ports.
- Find all ports answering

What Happens if Port Not Open

- No machine at all.
  - Typically get an ICMP response from a router
    - Special protocol for Internet error message packets
    - Saying no host at this address
- Machine but with closed port
  - Typically get a reset packet
  - Like a syn-ack, but with R set instead of S and A
  - Semantics – "stop this immediately"
- Security system (firewall)
  - Silence (depending on configuration)

Visualizing Scans



Small Piece of a Large Random Scan