Defending Computer Networks
Lecture 6: TCP and Scanning

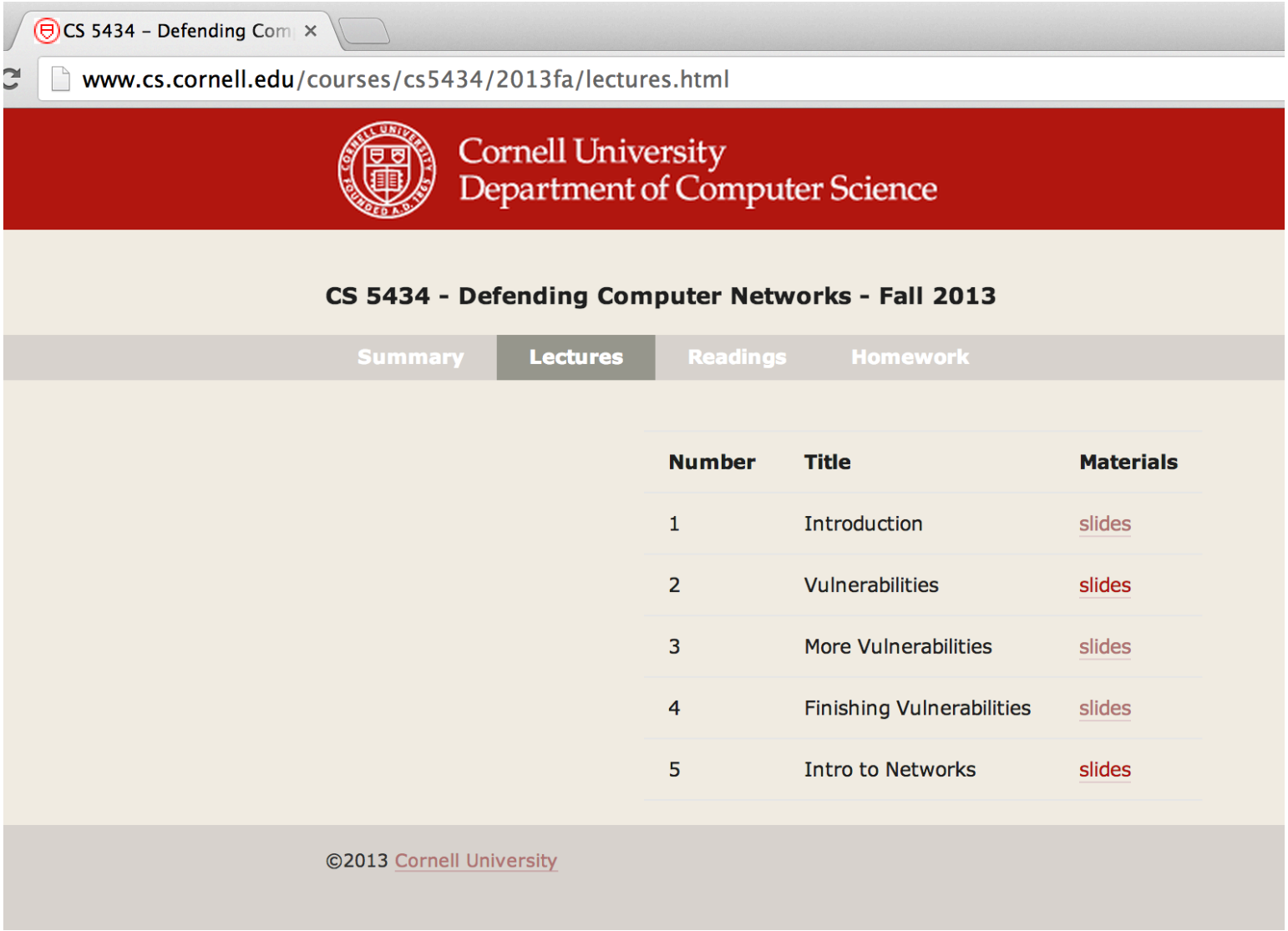
Stuart Staniford

Adjunct Professor of Computer Science

Logistics

- 5 Minute Break Experiment
  - Worth it?
- First quiz will be Tuesday September 24th.
  - Half hour quiz at start of class.
  - Covering everything in class through Thurs Sep 19th 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

Argentina, Brazil agree on cyber-defense alliance against US espionage

Published time: September 15, 2013 03:30
Edited time: September 16, 2013 08:00

Handout picture released by the Argentine Defence Ministry showing Brazil's Defence Minister Celso Amorim (L) listens to his Argentine counterpart Agustin Rossi speaking after signing a bilateral agreement on cooperation in cyber defence, during a meeting in Buenos Aires on September 13, 2013 (AFP Photo)

Defense ministers of Brazil and Argentina have pledged to cooperate closely to improve cyber defense capabilities following revelations of the scale of US spying on Latin American countries.

"We need to reflect on how we cooperate to face these new forms of attack," Brazil's defense minister, Celso Amorim, said at a conference in Buenos Aires.

Trends
NSA leaks

Tags
Hacking, Intelligence, Internet, Scandal, WikiLeaks

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.

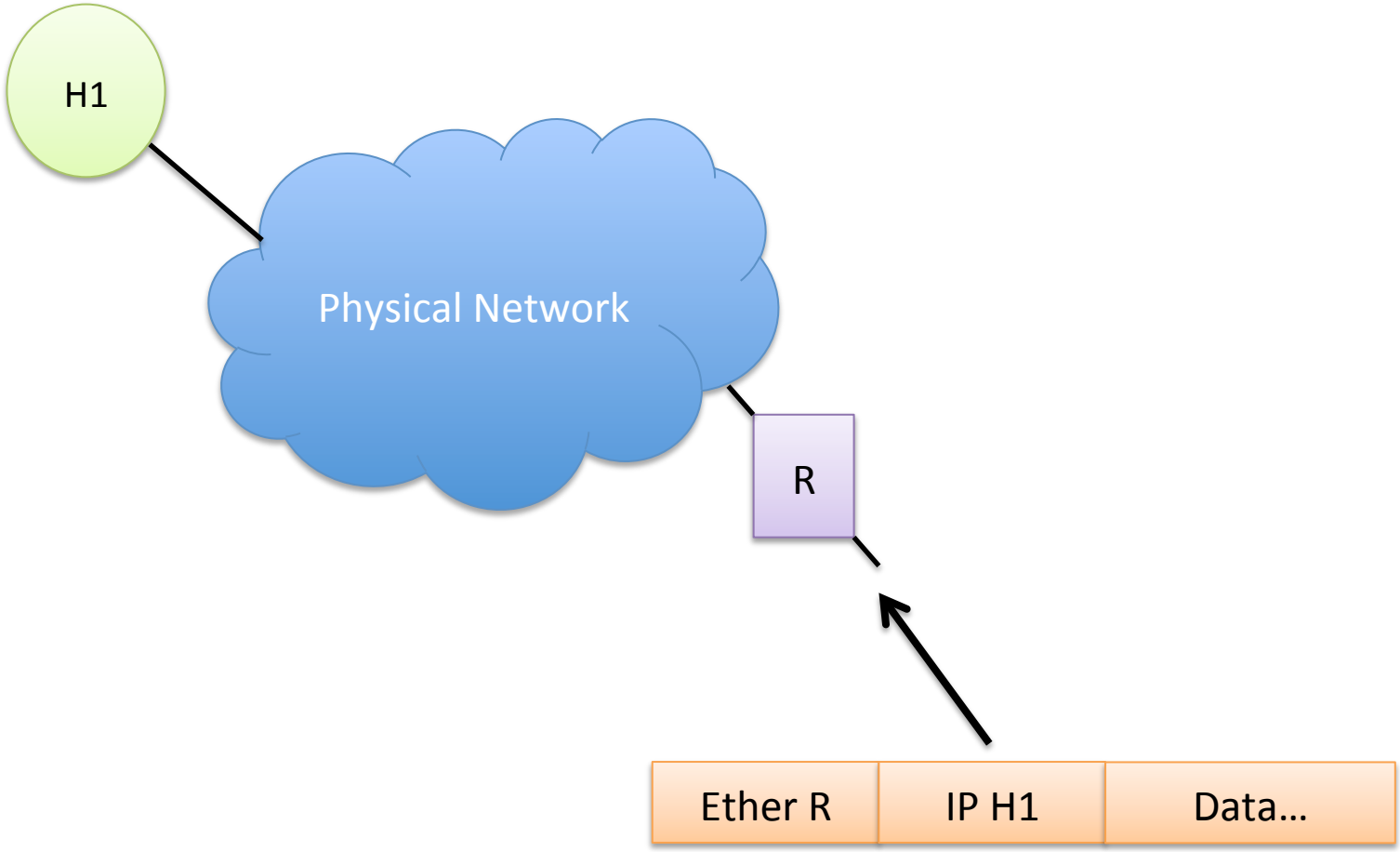
14. The modern enterprise network: what a large-scale network looks like, and emerging trends affecting it (BYOD, cloud).

15. Legal and ethical issues in defending networks.

Main Goals for Today

- Finish up Arp Spoofing from Last Time
- Basics of TCP Protocol
- Port scanning

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

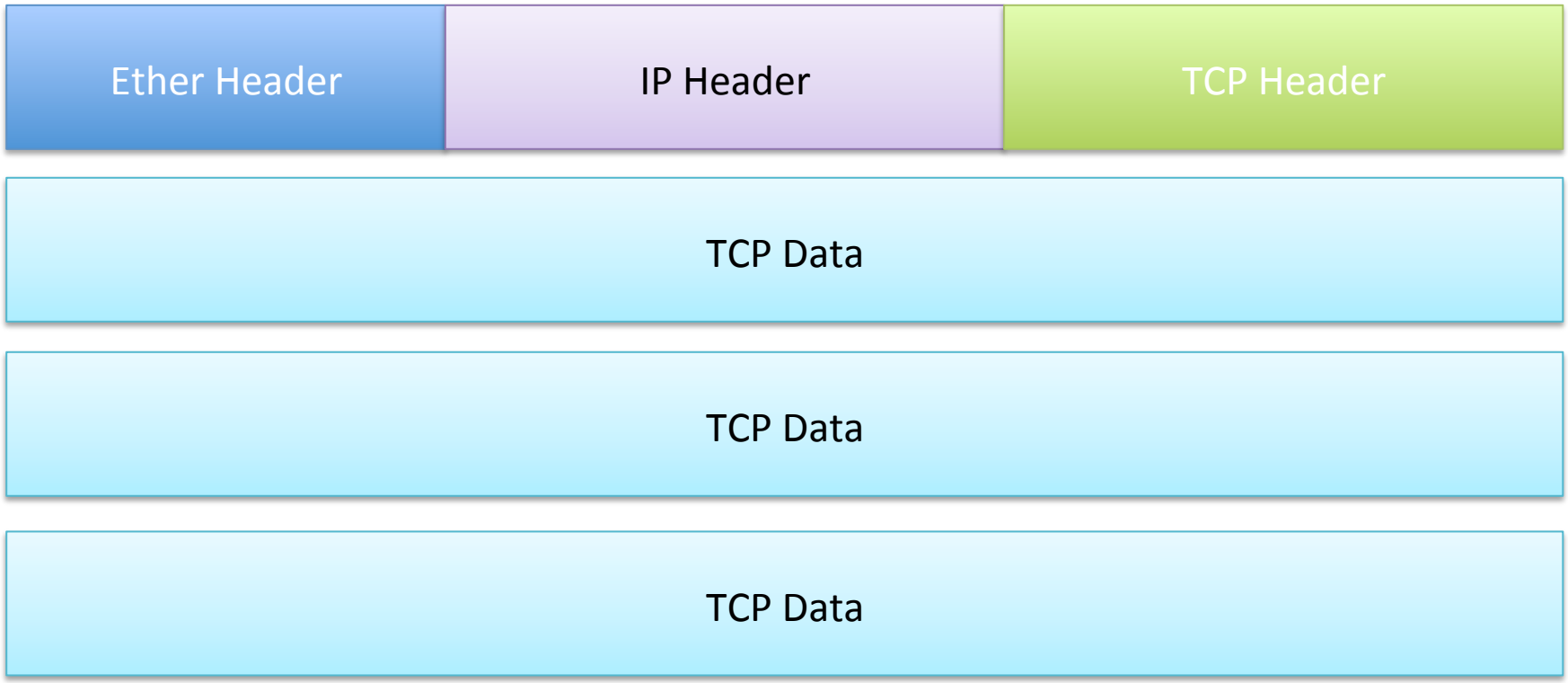
Intro to TCP

- 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

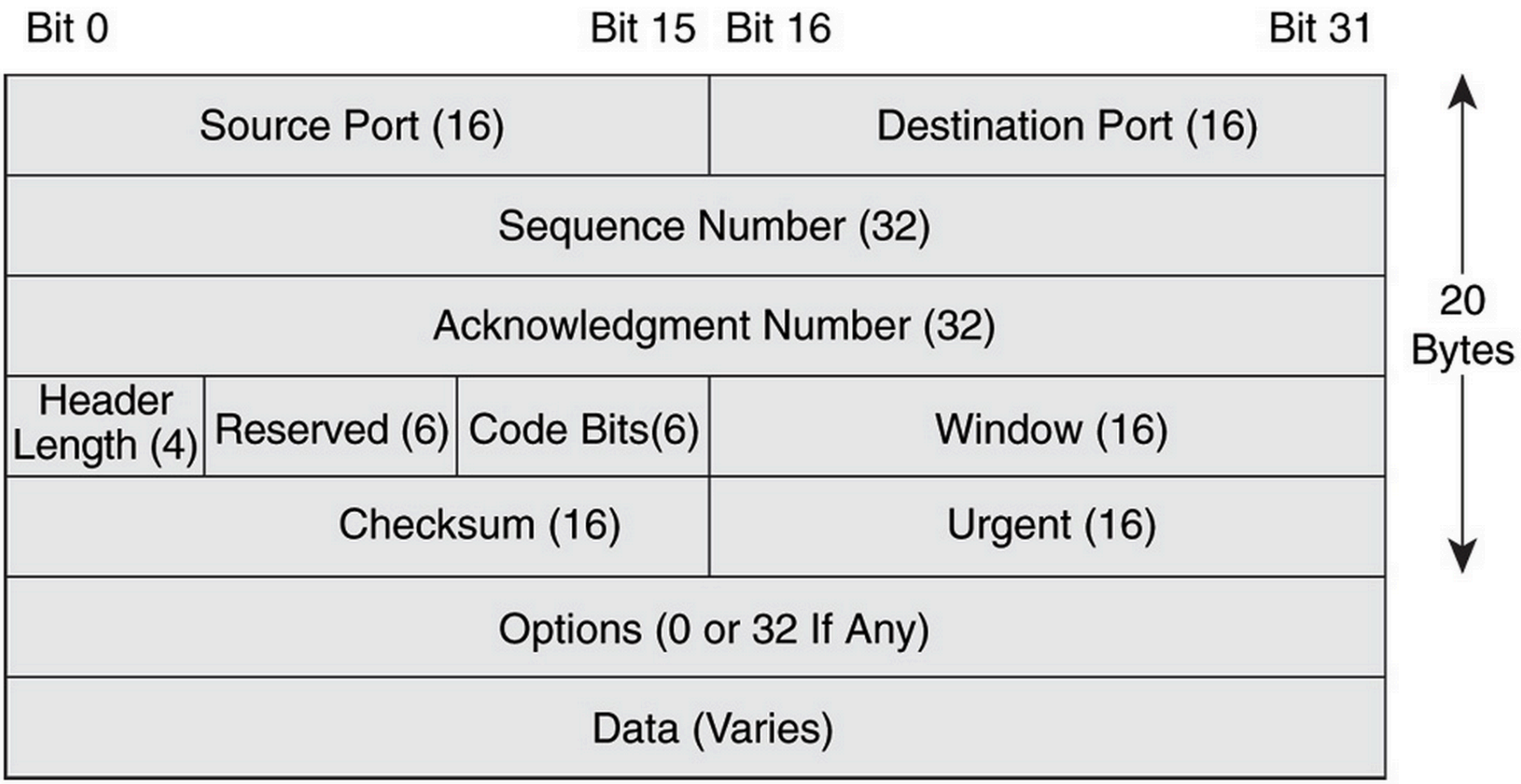
Protocol Relationship

- 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

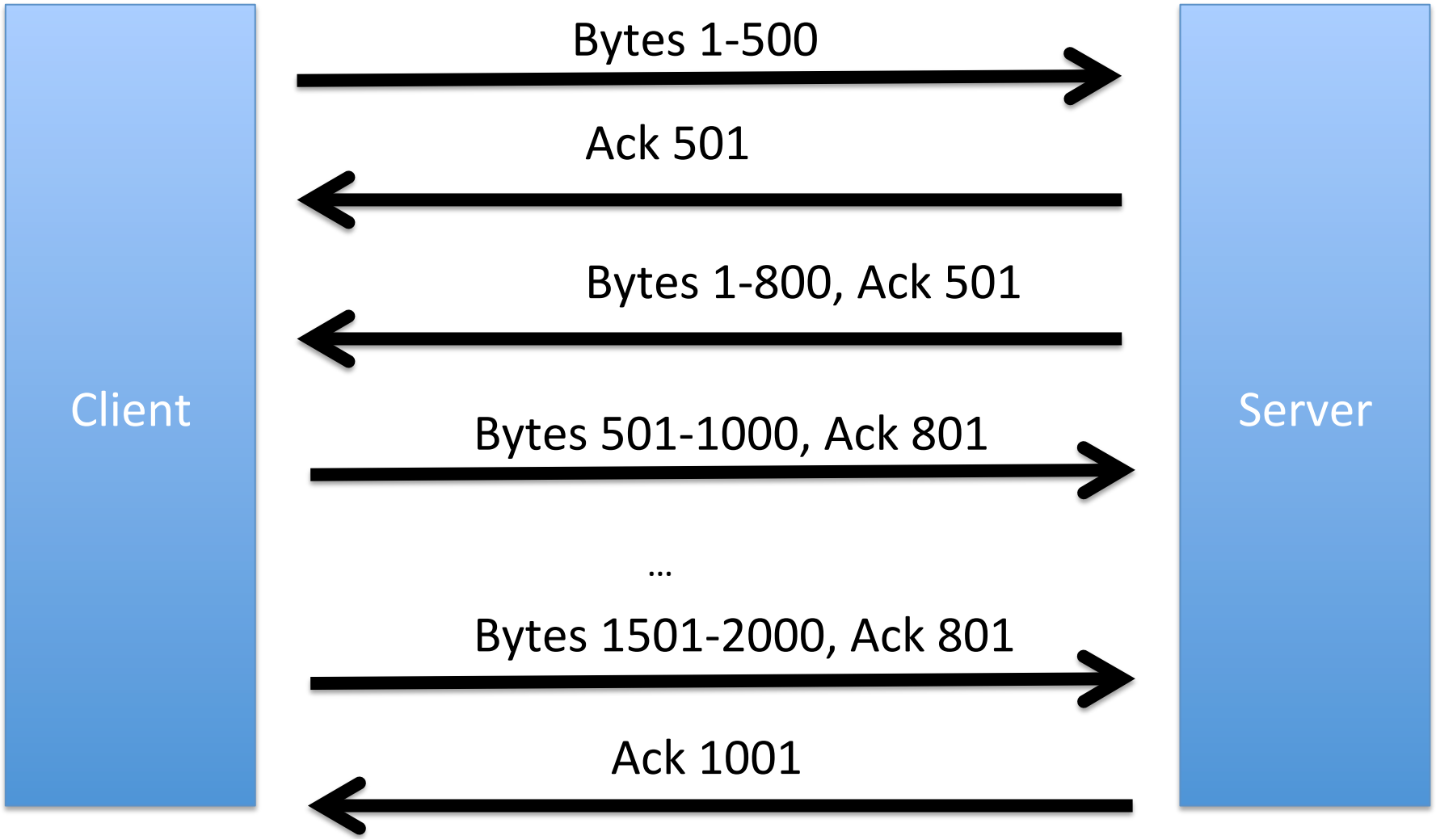
TCP Connections

- 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

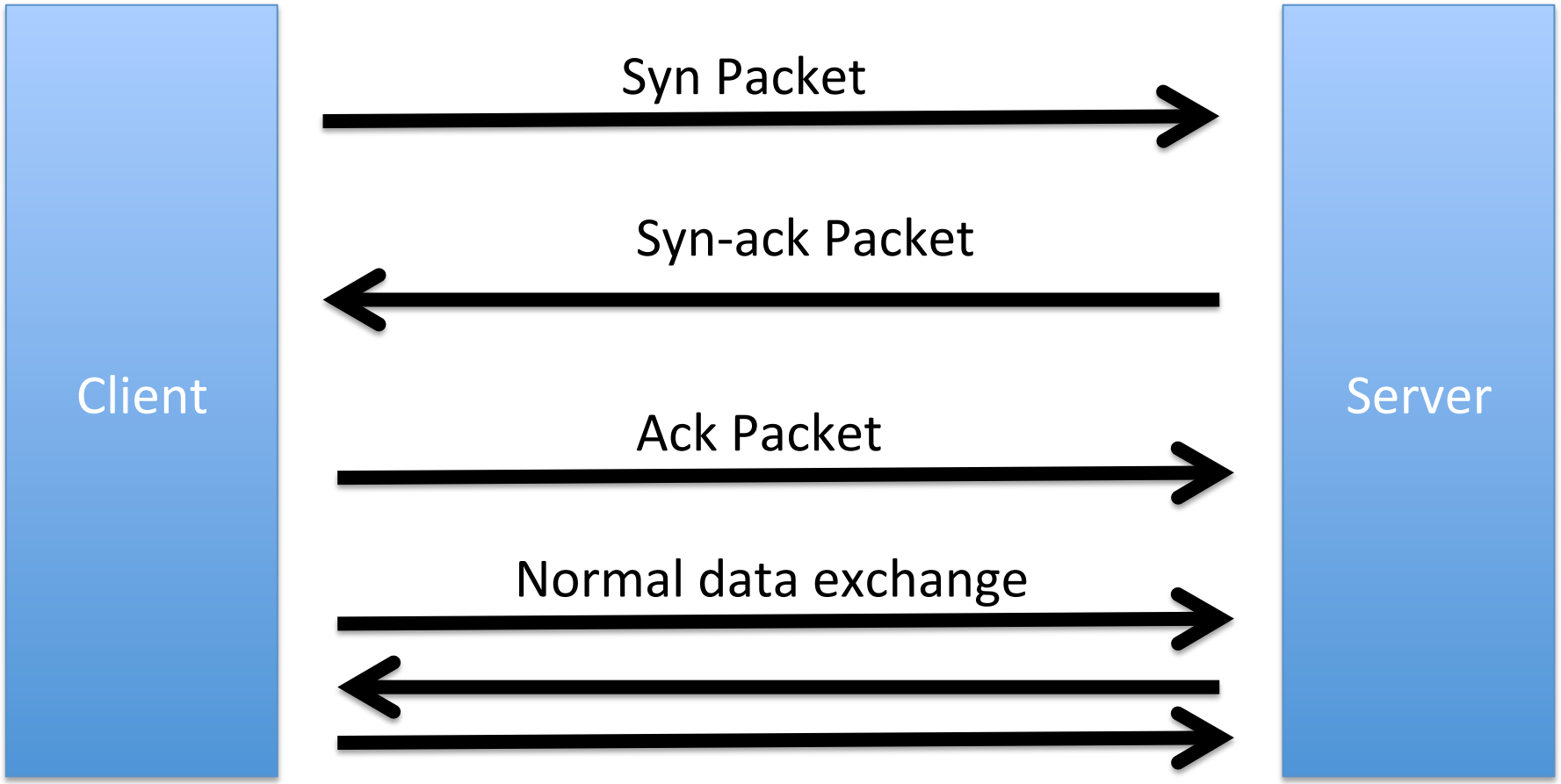
Let's work through an example



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

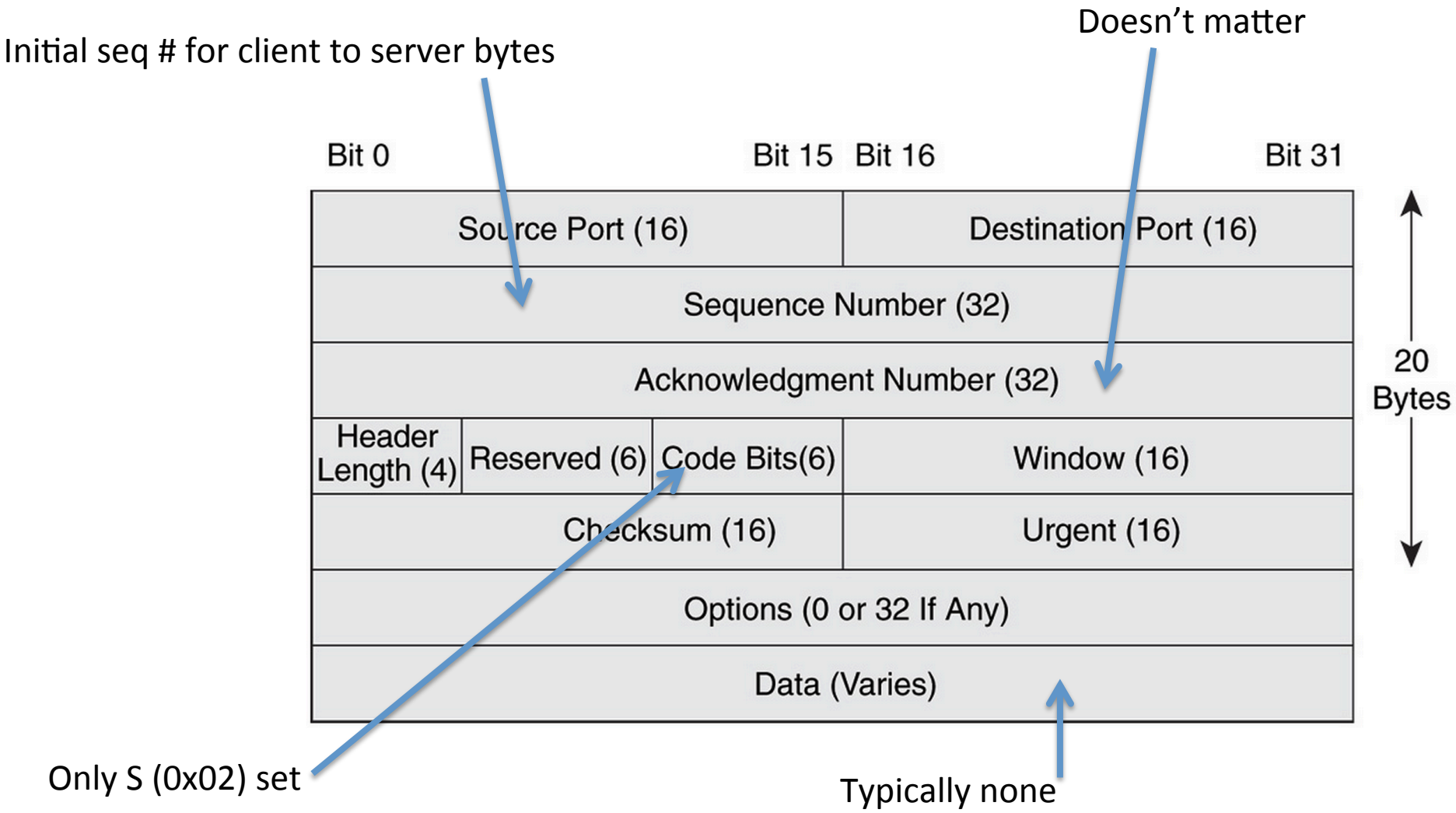
Handshake packets



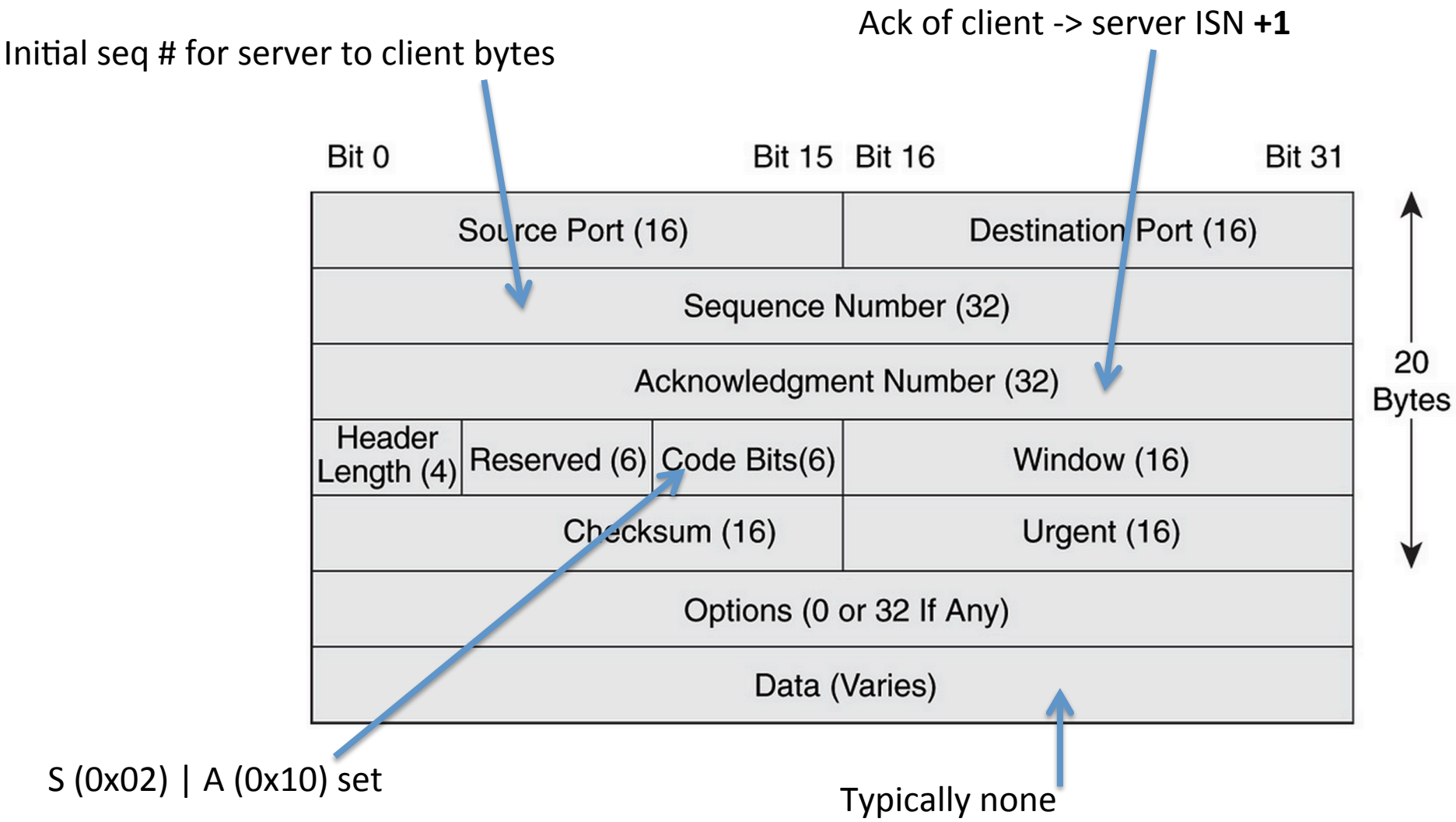
“Syn Packet”

- 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

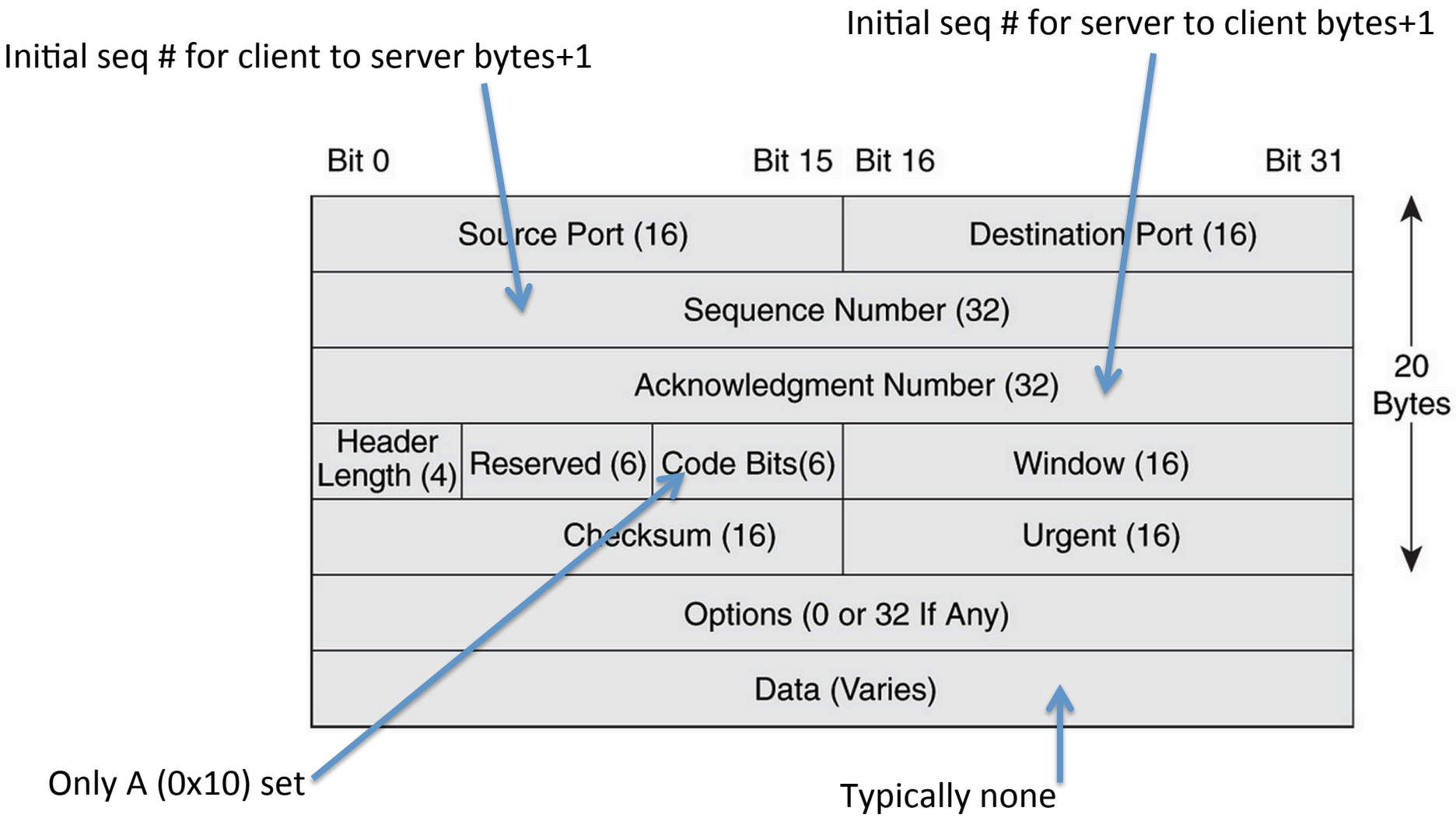
Syn Packet Layout



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