CSCI 1800 Cybersecurity and International Relations

Design and Operation of the Internet

John E. Savage

Brown University

Outline

- Internet Conceptual Layers
- Link layer
- Network layer
- Transport layer
- Denial of service
- Open Source Software
- Huawei Telecommunications Technology

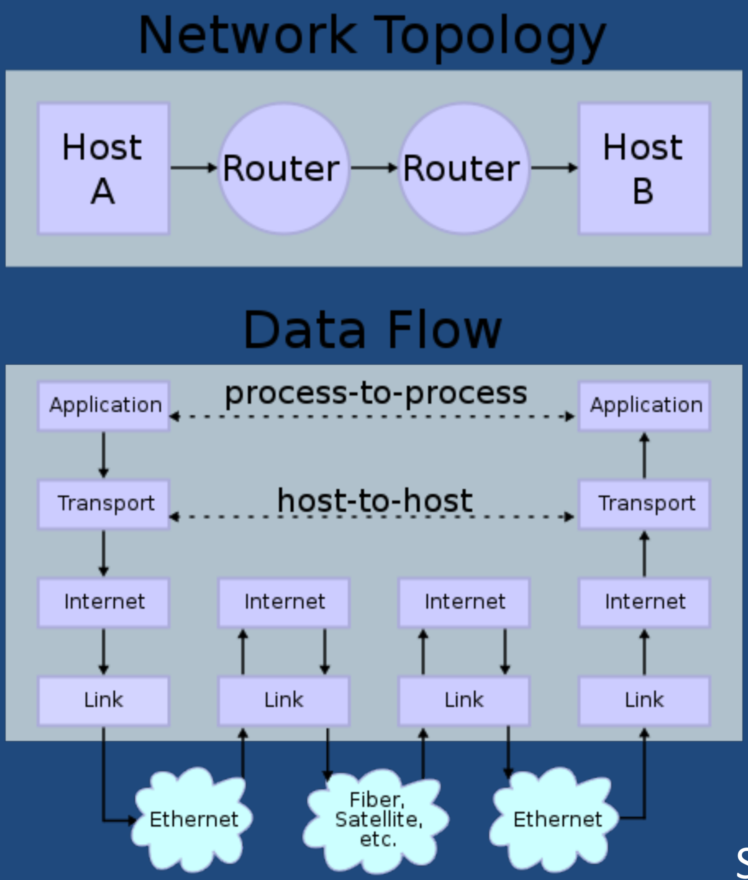
Notes on This Lecture

- It describes the operation of the Internet
- It is not necessary to commit all of it to memory
- Get the big picture and consult the notes when you need them.

The Internet

- The Internet is a collection of networks.
  - Networks connect hosts, i.e. individual computers.
  - Networks are local, area-wide, enterprise-wide, and national
- Protocols govern data transmission on networks
  - A protocol defines a way to package data
    - E.g. Include source, destination, & content and (often) error checking
  - Ethernet (1973) – link & physical layers – collision detection
  - Internet protocol (IP) (1974) – Internet layer – decomposes data streams into packets. Sends them via packet switching.
- Protocols are layered, one communicating to next
  - They simplify implementation of the Internet

Sending Data via Protocol Layers



Source: Wikipedia

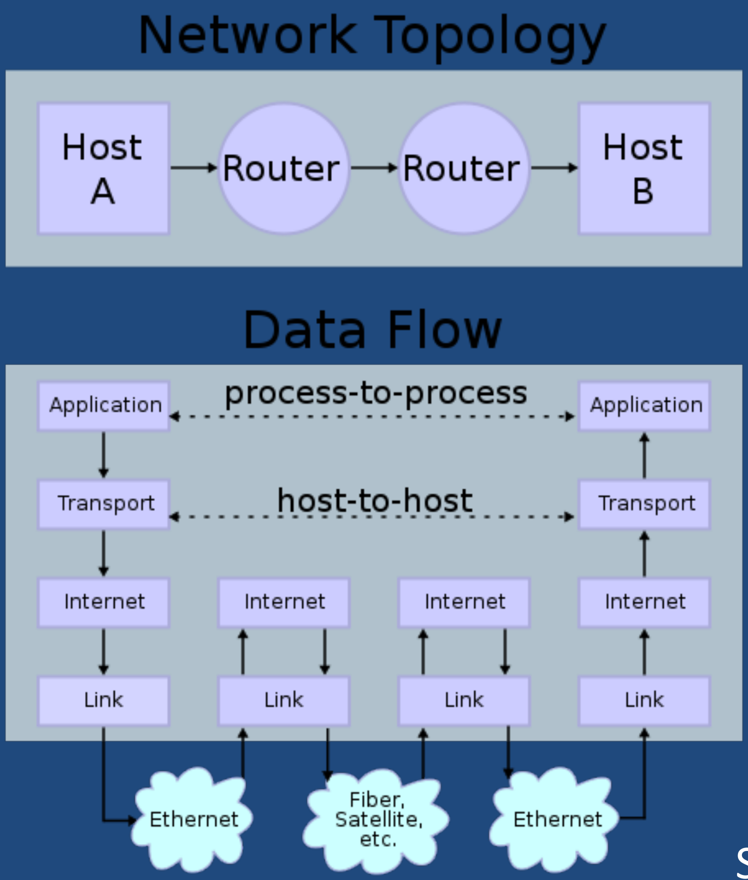
Conceptual Internet Protocol Layers

- Physical Layer
  - At level of wires, cables, radio – physical data transmission
- Link Layer
  - Logical level, organizes data into blocks, choose routes.
- Internet or network Layer
  - Makes best effort to move packets using Internet Protocol (IP)
- Transport Layer
  - TCP* (reliable) and UDP† (fast, no guarantees) protocols are here
- Application Layer
  - Application protocols such as HTTP and HTTPs for browsers, DNS for naming, SSL for secure communication, VoIP for phone

* TCP: Transmission Control Protocol

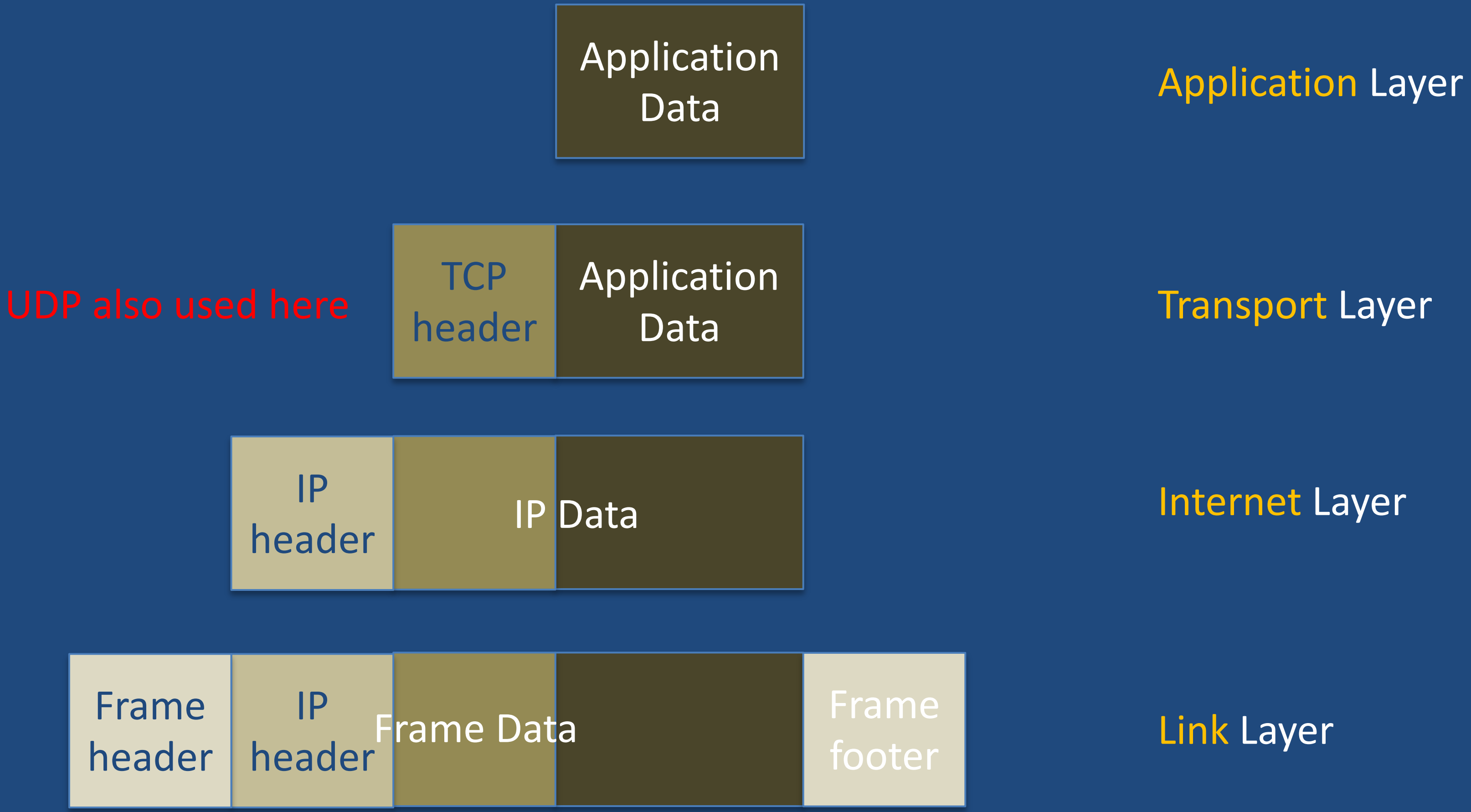
† UDP: User Datagram Protocol

Sending Data via Protocol Layers



Source: Wikipedia

Internet Packet Encapsulation by Layer



Application Data

Application Layer

UDP also used here

TCP header | Application Data

Transport Layer

IP header | IP Data

Internet Layer

Frame header | IP header | Frame Data | Frame footer

Link Layer

Network Security Goals - CIA^4

- Confidentiality
  - Keep content private
- Integrity
  - Ensure that content is not altered
- Availability
  - Ensure content is available

Big Three – CIA

- Assurance
  - Enforce data flow policies, e.g. firewall configurations, rules, etc.
- Authenticity
  - Authenticate users via signatures
- Anonymity
  - Guarantee anonymity when needed

Ethernet – At the Link Layer

- Data organized into frames. Each has
  - Header of 175 bytes (8 bits/byte)
  - Payload of 46 to 1,500 bytes
  - Footer contains a 4-byte checksum
    - What is the role of the checksum?

- Operation: If a host wants to send a frame:
  - Waits until no signals heard & transmits one bit of one frame
  - Listens for collisions between its bit and bits of others.
    - *If collision detected*, wait a random time and retransmit
    - *If no collisions detected* during packet transit time, success.
  - Transmits remaining bits in frame in same manner.

Ethernet Hubs and Switches

- Ethernet hub connects multiple hosts
  - All hosts hear messages sent by others

- Ethernet switch has multiple hubs connecting multiple hosts.
  - Only hosts on hub can hear one another.
  - Messages are sent from host on one hub to host on another hub by *switching* packets to that hub.

Media Access Control Addresses

- Each device has a network interface, the place where connects to a network.
  - Each network interface has a MAC address.
  - A MAC address is generally a *unique* 48-bit string assigned by a manufacturer.
  - Although on modern computers, a MAC address can be changed under software control.
- MAC addresses are used by Ethernet switches.

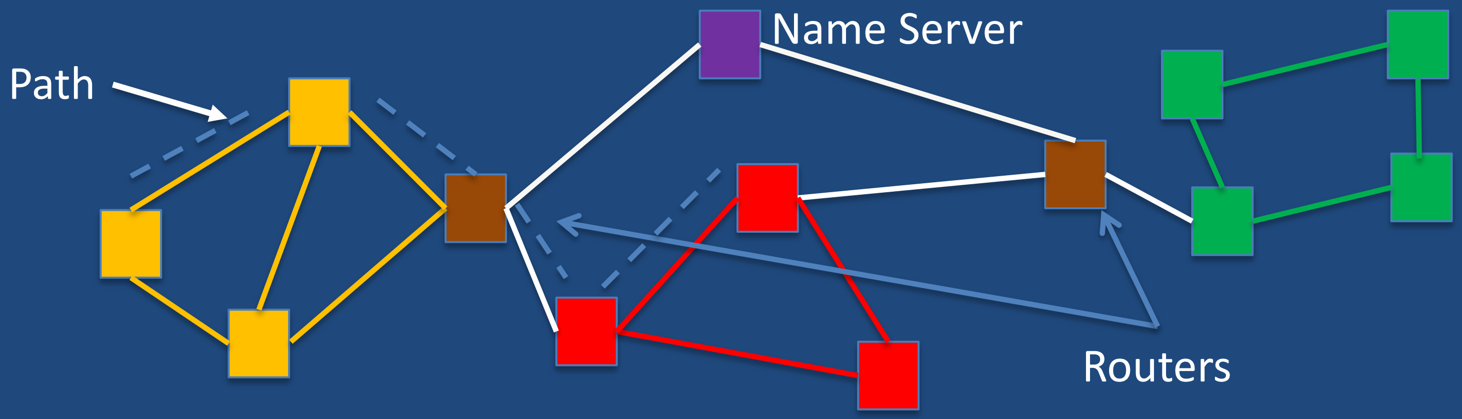
Address Resolution Protocol (ARP)

- ARP – link-layer protocol on local area network (LAN)
- To send a packet to an IP address on the LAN:
  a. If sender knows local address (usually MAC), send to it.
  b. If not, sender broadcasts IP address on LAN asking owner to reply with its MAC address. Then go to a.
- Spoofing of ARP is possible to create MTM attack
  - When Alice makes request intended for Bob, Eve responds with her MAC address before Bob responds
  - When Bob makes a request intended for Alice, Eve responds with her MAC address before she responds
  - Now communication between Alice & Bob is via Eve

The Internet Protocol (IP)

- IP makes best effort to send packets between source and destination addresses.
- Addresses are 32-bits (IPv4) or 128-bits (IPv6).

$2^{32} = 4 \cdot 2^{30}$ or about $4 \cdot 10^9$ $2^{128} = 64 \cdot 2^{120}$ or about $64 \cdot 10^{36}$



Packet Transmission

- ARP used to send packets within local area net (LAN)
- Packets for an IP address on remote LAN are sent to LAN Internet gateway, then to remote LAN.
- Gateways are also called routers.
- Routers use routing tables to direct packets.
  - For each IP address, a table specifies a neighbor to receive the packet.
  - To prevent looping, each packet has a time-to-live (TTL) value. It is decreased by one each time it passes through a router. When TTL = 0, packet is discarded.

Packet Routing

- Routers quickly drop, deliver or forward packets.
  - Drop if TTL =0, deliver if dest. is on LAN; forward if not
- Packet forwarding protocol is via one of these:
  - Open Shortest Path First (OSPF) or
  - Border Gateway Protocol (BGP)
- BGP also routes packets between autonomous systs

- Note: A LAN hub/switch is simple. A router is not. It is complex & must handle complex routing policies.

Format of IPv4 Packets

2^{16} = 65,536 ports

	4 bits	4 bits	8 bits	3 bits	13 bits	
Bit Offset	**0-3**	**4-7**	**8-15**	**16-18**	**19-31**	
0	Version	Header Length	Service Type	Total Length		Header
32	Identification			Flags	Fragment Offset	
64	Time to Live		Protocol	Header Checksum		
96	Source Address					
128	Destination Address					
160	(Options)					
160+	Data Data Data Data Data					Payload

Format of IP Packets

- Header checksum identifies transmission errors
  – Checksum recomputed every time TTL decremented.
- IPv4 address – 4 bytes or 32 bits, eg 128.148.32.5
  – A byte (8-bits) specifies an integer in range [0-255].
- IPv6 address – 8 sets 4 hexadecimals or 128 bits
  – Hexadecimals: [0,1,2,...,9,a,b,...,f] (16 chars, 4 bits)
  – e.g. 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Refresher on Binary Numbers

Decimal Numbers	Binary Representation
	2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0
0	0 0 0 0 0 0 0 0
1	0 0 0 0 0 0 0 1
2	0 0 0 0 0 0 1 0
3	0 0 0 0 0 0 1 1
4	0 0 0 0 0 1 0 0
5	0 0 0 0 0 1 0 1
6	0 0 0 0 0 1 1 0
7	0 0 0 0 0 1 1 1
8	0 0 0 0 1 0 0 0
16	0 0 0 1 0 0 0 0
128	1 0 0 0 0 0 0 0
…	…
255	1 1 1 1 1 1 1 1

More on Format of IP Packets

- A domain or prefix defines a block of IP addresses that is associated with a subnetwork or autonomous system (AS).
- A domain is specified thus: (IP address)/(integer) and assigned to an autonomous system.
  - E.g. 128.148.32.5/24 specifies the IPv4 addresses beginning with the first 24 address bits of 128.148.32.5
  - What are the first 24 bits? 10000000 10110000 00100000 --------
- The domain contains the addresses 128.148.32.0, 128.148.32.1, …, 128.148.32.255.
- Since there are 2^8 = 256 choices for the last 8 = 32-24 bits, this prefix defines 256 addresses in the subnetwork.

Conceptual Internet Layers

- Physical Layer
  - At level of wires, cables, radio – physical data transmission
- Link Layer
  - Logical level, organizes data into blocks, choose routes.
- Internet or network Layer
  - Makes best effort to move packets using Internet Protocol (IP)
- Transport Layer
  - TCP (reliable) and UDP (no guarantees) protocols are here
- Application Layer
  - Applications protocols are here. They include HTTP and HTTPs for browsers, DNS for naming, SMTP & IMAP for email, SSL for secure communication, and VoIP for phone service

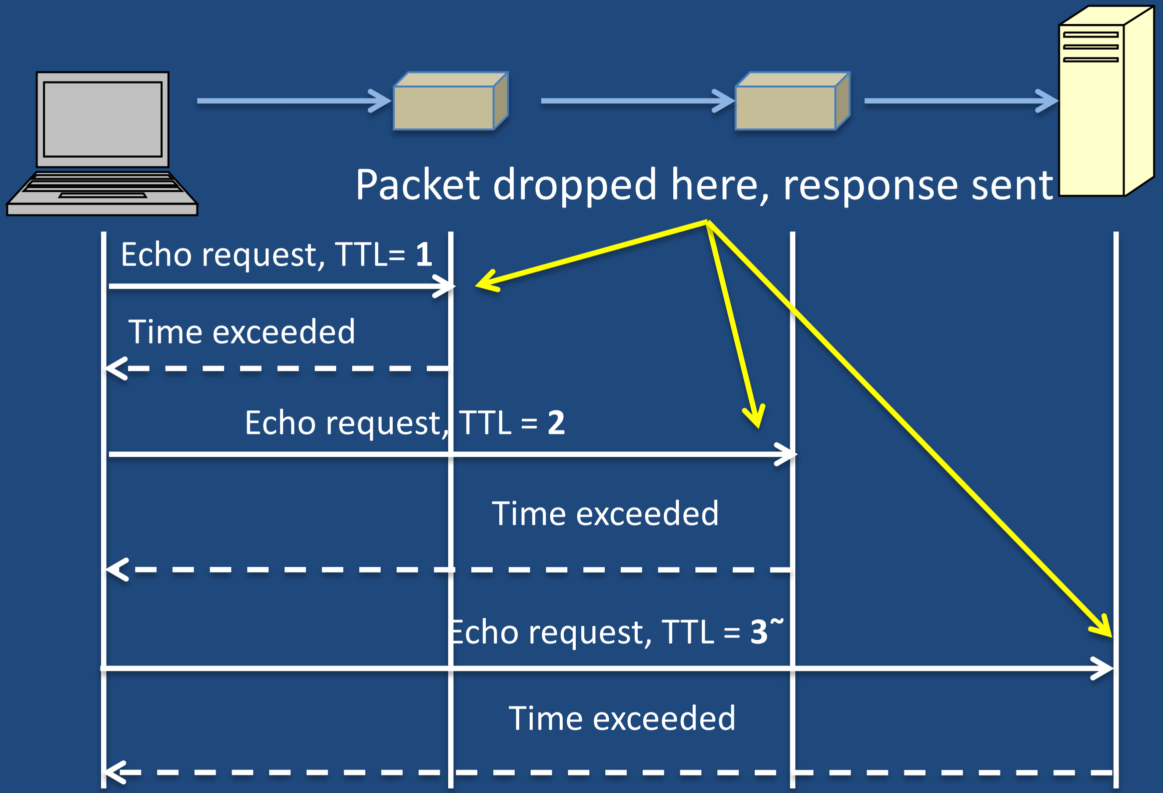
Internet Control Message Protocol

- ICMP is network layer protocol for testing and error notification. Message types:
  - Echo request – asks destination to acknowledge
  - Echo response – acknowledges receipt of packet
  - Time exceeded – sends notification that TTL = 0
  - Destination unreachable – packet not delivered
- Ping uses ICMP to tell if machine reachable
  - It repeatedly sends an ICMP packet to an IP address

```
 PING princeton.edu (140.180.223.22): 56 data bytes
 64 bytes from Princeton.EDU (140.180.223.22): icmp_seq=1 ttl=243 time=11.3 ms
 64 bytes from Princeton.EDU (140.180.223.22): icmp_seq=2 ttl=243 time=12.2 ms
…
```

Traceroute

- Traceroute uses ICMP to trace path from source to destination.


Packet dropped here, response sent
Echo request, TTL= **1**
Time exceeded
Echo request, TTL = **2**
Time exceeded
Echo request, TTL = **3**˜
Time exceeded

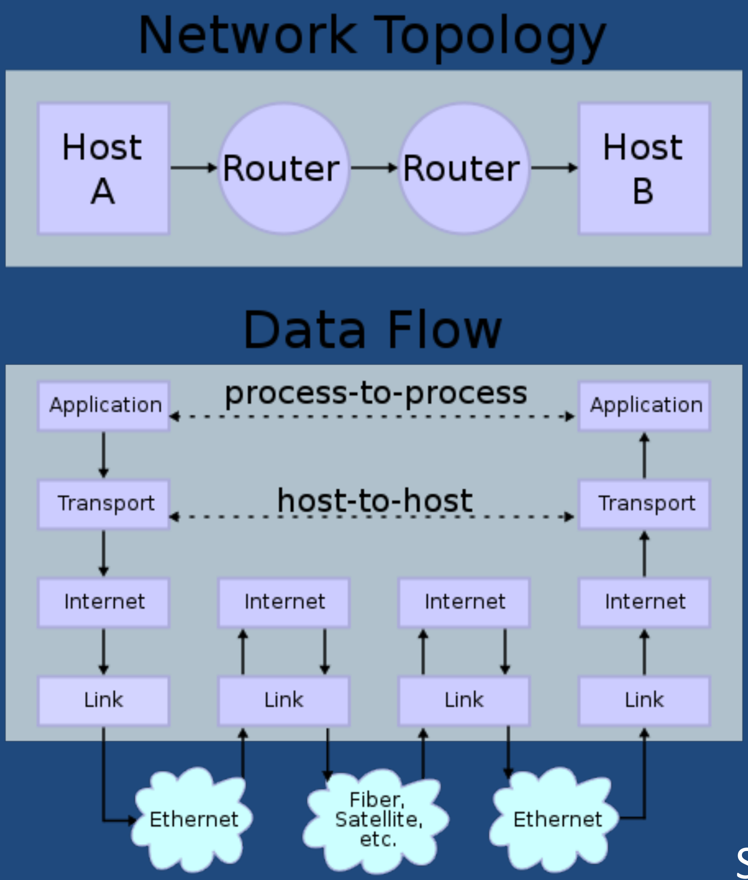
Traceroute Example

```
•   traceroute to princeton.edu (140.180.223.22), 30 hops max, 60 byte packets
•    1  10.116.52.1 (10.116.52.1)  1.414 ms  1.515 ms  1.716 ms
•    2  commodus-int.cs.brown.edu (10.116.1.5)  0.171 ms  0.160 ms  0.150 ms
•    3  138.16.160.253 (138.16.160.253)  1.897 ms  1.898 ms  1.905 ms
•    4  vl2062-ddmz-cit-r.net.brown.edu (10.1.18.1)  0.904 ms  0.923 ms  0.907 ms
•    5  lsb-inet-r-230.net.brown.edu (128.148.230.6)  0.969 ms  0.961 ms  1.198 ms
•    6  131.109.202.1 (131.109.202.1)  1.885 ms  1.825 ms  2.112 ms
•    7  bostonlight.oshean.org (198.7.255.1)  3.248 ms  3.566 ms  3.565 ms
•    8  nox300gw1-oshean-re.nox.org (192.5.89.125)  3.541 ms  3.506 ms  3.490 ms
•    9  i2-re-nox300gw1.nox.org (192.5.89.222)  7.809 ms  8.164 ms  8.105 ms
•   10  216.27.100.5 (216.27.100.5)  10.280 ms  10.218 ms  10.197 ms
•   11  remote1.princeton.magpi.net (216.27.98.114)  11.261 ms  11.253 ms  11.226 ms
•   12  core-87-router.Princeton.EDU (128.112.12.130)  11.919 ms  12.503 ms  12.150 ms
•   13  Princeton.EDU (140.180.223.22)  11.505 ms  11.498 ms  11.489 ms
```

IP Spoofing

- Host/router can change Source Address in a packet.
  - Can be used in denial of service attack.
  - If ICMPs are sent to many destinations with the same spoofed source address, all will respond to spoofed source, swamping it.
- Coping with IP spoofing:
  - Routers should drop a packet entering a domain with source address from inside that domain.
  - Should also drop leaving packets whose source is outside
  - If routers log packets passing through them, which is not always done, can trace spoofed packets back to a source.

Protocol Layers Again



Source: Wikipedia

Transport Layer Protocols

- They connect process at a port of local IP address to a process at a port of a remote IP address. 2^{16} ports.
- TCP and UDP are primary protocols at this layer.
- Transmission Control Protocol (TCP) provides reliable packet stream between ports. Repeat packets if lost.
  - What should it be used for? files, web pages, email
- User Datagram Protocol (UDP) provides best-effort communication between ports. Send it and forget it
  - Used for VoIP and apps where lost bytes not important.

TCP Packet Format

2^{16} = 65,536 ports

16 bits

Bit Offset	0-3	4-7	8-15	16-18	19-31
0	Source Port			Destination Port	
32	Sequence Number (Seq)				
64	Acknowledgement Number (Ack)				
96	Offset	Reserved Flags		Window Size	
128	Checksum			Urgent Pointer	
160	Options				
>= 160	Data Data Data …				

Header

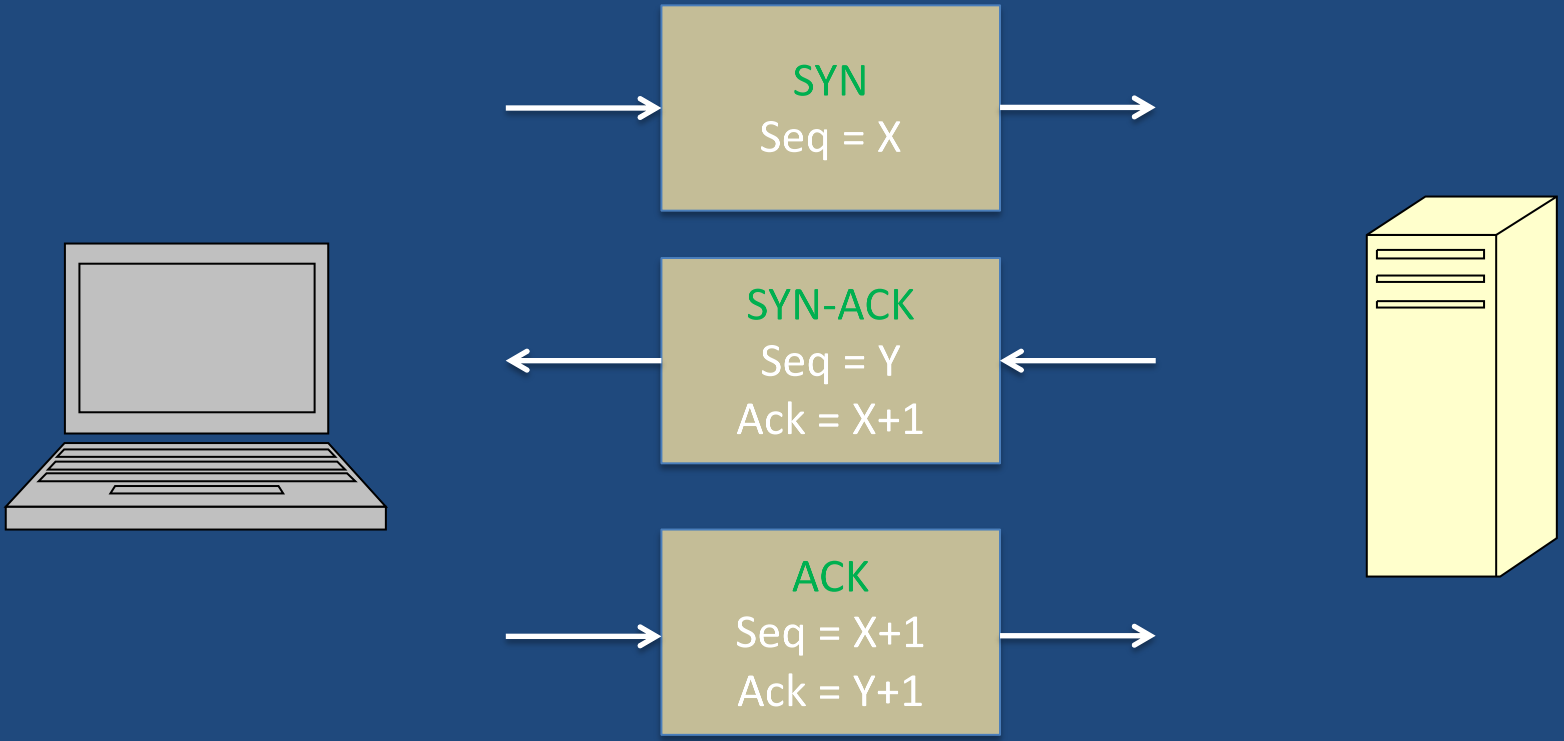
Payload

Port 80 for HTTP, 21 for FTP, 22 for SSH, for example.

Transmission Control Protocol (TCP)

- TCP/IP connects to destination using three-way handshake.
  - Each packet has a sequence number so that packets can be assembled in order.
  - If a packet is not acknowledged during a congestion window (a reasonable round-trip time) it is repeated. Thus, copies of packets can be in network.
  - The sender uses flow control (adjusts window) to avoid overwhelming the receiver.
  - If payload checksum fails, receiver rejects packet.

Three-Way TCP Handshake



SYN
Seq = X

SYN-ACK
Seq = Y
Ack = X+1

ACK
Seq = X+1
Ack = Y+1

TCP Three-Way Handshake

- Establishes connection between source/dest.

1. Source S sends destination D a packet with SYN flag on and random sequence number Seq = X.
2. D sends S a packet with both SYN and ACK flags on adds a random sequence number Seq = Y, and an acknowledgement number Ack = X+1. (S checks X)
3. S sends D a packet with SYN flag off, ACK flag on, Seq = X+1 and Ack = Y+1. (D compares Ack to Y.)

If successfully completed, TCP connection is made.

- Random values for X and Y help defeat attacks.

User Datagram Protocol (UDP)

- Header includes source and destination ports, length, checksum, and payload
- Designed for speed, not accuracy.
- Used for time-sensitive tasks such as
  - DNS and Voice over IP (VoIP)

Network Address Translator (NAT)

- NAT used when insufficient IPv4 addresses available
- A NAT is hardware that maps one external IP address into multiple internal IP addresses.
- Each internal IP address is assigned a unique port number of the external IP address.
- When packet sent back to the IP address, its port number is used to lookup is internal IP address.
  - The packet IP address is changed to the internal one.
- A NAT hides internal IP addresses – protects against random hits

Denial of Service (Flooding) Attacks

- Because bandwidth is limited, many packets directed to a client, can overwhelm client.
  - ICMP attacks
  - SYN flood attacks
  - Optimistic TCP attacks
  - Distributed denial of service (DDoS) attacks
    - Denial of service from many sites, such as botnet.
- Can defend against DDoS via IP tracebacks or more sophisticated automatic techniques.

ICMP Attacks

- Ping Flood Attack – attacker floods victim with pings (ICMP packets)
  - Attacker can be much more powerful than victim.
- SMURF attack – attacker sends ICMP packet with spoofed address to network broadcast site.
  - All sites on network respond to spoofed site.

SYN Flood Attacks

- Attacker opens many TCP sessions by sending SYN packets to a victim without replying to SYN/ACK packets from the victim.
- Victim keeps list of SYN seq numbers in memory so that it can synchronize sessions.
- If too many sessions are opened, victim's memory fills up, blocking other TCP sessions.
  - Routers can be redesigned to avoid this.

Open Source Software (OSS)

- Proprietary software is kept confidential
  - E.g. Apple iPhone software is proprietary. Google Android phone software is OSS
- OSS is software available for use by others
  - It can be used in products, modified and shared.
  - Some OSS licenses require that a copy of modified code be placed in the OSS repository.
- Internet applications rely heavily on OSS

Open Source Software (OSS)

- A debate is ongoing whether OSS is a good idea
- Pluses:
  - OSS allows software engineers to write code quickly
  - Publicity may lead to catching more bugs
- Minuses:
  - Untrained engineers will not find bugs
  - Bugs in OSS that is widely used can create crises when discovered
    - E.g. Heartbleed OpenSSL bug introduced 2012, found 2014

Huawei Communication Technology

- The US government does not want Huawei 5G telecommunications hardware and software in US networks nor those of partner countries
- 5G offers very high data rates but signals don't penetrate thick walls.
- Security concerns:
  - Huawei systems could be used for espionage
    - Their code is of poor quality and vulnerable
    - China's National Intelligence Law requires cooperation
  - They could disable networks during conflict

Review

- Internet Conceptual Layers
- Link layer
- Network layer
- Transport layer
- Denial of service
- Open Source Software
- Huawei Telecommunications Technology