ECE303 – Communication Networks

Jonathan Lam

February 9, 2020

Contents

1 Computer Networks and the Internet

1.1 What is the Internet?

We can think of the Internet:

- Physically, as a network of communication links connecting hosts to each other
- Functionally, as an infrastructure providing services to applications

1.2 Network edge

end systems/hosts devices connected to the internet (and not facilitating the Internet's connections); i.e., compute devices; i.e., they "host" applications; divide into client and server based on usage

communication links a network of communication links join the hosts

packet switch usually routers (usually in network core) and link-layer switches (access networks)

route/path the sequence of communication links and packet switches taken by a path from one host to another

Internet Service Provider (ISP) provide access to the internet; are a network of packet switches and communication links

Internet Engineering Task Force (IETF) manages internet standards and RFCs

Request For Comments (RFC) define protocols

distributed application applications that require connecting to another host; "distributed" because run on multiple computers; only run on edge devices (compute devices)

protocol defines the format and order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event

network access anything that takes an end device to the first router ("edge router")

1.3 Network access

DSL and cable two major types of broadband residential access; DSL (digital subscriber line) happens over a telephone network, so that the telephone company (telco) is the ISP; the signal gets sent to the central office (CO), which multiplexes the signal (DSLAM, DSL Access Multiplexer), which is connected to the network core and converts the analog frequencies into digital ones; cable uses the same infrastructure as cable television; CMTS (cable modem termination system) is similar to DSLAM; cable modem is a shared broadcast medium, so total bandwidth is limited

HFC hybrid fiber coax; a common implementation of cable systems

asymmetric transmission rates typically, download is allocated higher bandwidth than upload

FTTH Fiber To The Home; e.g., FIOS; fast, one-to-one w/ CO

satelliate, dial-up alternative methods for Internet access

physical data transmission media twisted-pair copper wire, coaxial cable, multimode fiber-optic cable, terrestrial/satellite radio spectrum

guided/unguided data transmission media wires: guided: WLAN/satellite: unguided

unshielded twisted pair (UTP) cheapest form of wire; commonly used in indoor wiring, but not as good as shielded

1.4 Network core

packet speed packets are transmitted over each link at its full transmission speed (i.e., they are atomic, not broken up or mixed with other packets)

store-and-forward packets are sent one at a time, only after fully finished receiving (b/c may need to process) (i.e., it builds entire packet in some buffer)

queueing delays packets must wait in output buffer/queue until communication link is done transmitting other packets

packet loss output buffer full

forwarding table in a router; maps (parts of) destination IPs to outbound links; get automatically set by routing protocols

circuit a communication link on the path between two hosts which maintain their state for a connection; a.o.t. packet switching; has a guaranteed constant transmission rate

frequency/time-division multiplexing (FDM/TDM) different frequency bands are reserved (full time, partial bandwidth) for a circuit or time is divided into frames with dedicated time slots (partial time, full bandwidth)

circuit switching benefits/downfalls over packet switching it has "silent periods" because of reserved pieces not being used; also some time to set up the circuit; it has the ability for real-time services; it is more costly to implement

ISP tiers tier-1: globally-spanning, doesn't have to pay anyone; local: connect to tier-1 or larger local ISPs

customer/provider ISPs customers pay providers to connect to them; show hierarchy of size

Points of Presence (PoP) a group of routers in the same location in the provider's network where customer ISPs can connect into the provider ISP

multi-homing when an ISP connects to multiple provider ISPs

peering when two ISPs (usually of the same level) exchange traffic without either side paying

Internet Exchange Point (IXP) a place where multiple ISPs can peer together

Content Provider Networks (CDNs) corporations with large internal networks largely separate from the rest of the Internet; allow greater control over their data and services

delays processing (examining headers); queueing (other items in queue); transmission delay (how long it takes to get all of packet onto link); propagation delay (based on physical medium's properties)

latency and throughput latency is how long it takes for a packet to reach its destination; throughput is the rate at which packets goes through (are received by the receiver) and is bounded above by the lowest bandwidth of any links along the route; access network (the "last mile") is usually the bottleneck for performance in today's Internet

1.5 Protocol layers and their service models

1.5.1 TCP/IP stack

A user application places some data into a message in some application-specific protocol. The OS manages TCP protocol and sets up the IP protocol. When traveling between hosts, while on the physical medium, physical-level protocols govern bit movement at the most basic level, and link-level protocols provide some abstraction that governs reliability and makes some decisions between any nodes in the network. At a node, the network-level protocols manage which next link to take. When the destination is reached, the transport- and application-level protocols are again managed by the host.

E.g., a NIC operates at levels 1 (sending out physical bits) and level 2 (making decisions based on MAC address); a switch also operates at levels 1 and 2; a router operates at 1-3.

application where network applications and their protocols live (e.g., HTTP, SMTP, FTP, DNS); packet of information in application layer is referred to as a "message"

transport TCP, UDP; supports application layer with connection and some reliability (TCP only); transport layer packet is a "segment"

network (IP layer) responsible for moving network-layer packets ("datagrams") between hosts, e.g., through the IP protocol and other routing protocols

link responsible for reliable movement of link-level packets ("frames") between network nodes, e.g., WiFi, Ethernet

physical protocols for moving bits along the specific physical medium

1.5.2 ISO OSI model

Open Systems Interconnection model, by the International Organization for Standardization

application

presentation provide services that allow communicating applications to interpret the meaning of data exchanged, e.g., data compression and encryption (e.g., SSL/TLS)

session for delimiting and synchronization of data exchange, such as the means to build a checkpointing and recovery scheme

transport

network

link

physical

Important idea of **data encapsulation**; at any node, any headers/packets at a higher level in the stack than what the node is implemented at is treated as data. Only the header at the level of implementation is interpreted. I.e., the **payload** of any packet comprises of the packet from the layer above (unless it is the application-layer, in which the payload is the user's data).

1.6 Networks under attack

botnet a network of malware-compromised devices that attackers use to perform coordinated attacks (e.g., DDoS)

self-replicating many malware are self-replicating

viruses vs. worms viruses require explicit user input; worms do not

DoS attacks usually by vulnerability attacks (well-crafted messages sent to the server) or bandwidth/connection flooding

packet sniffing e.g., WireShark; data over shared media (e.g., WiFi) are especially vulnerable

IP spoofing this creates the need for end-point authentication

2 Application layer

2.1 Principles of network applications

P2P architectures interesting b/c of self-scalability – each user also acts as part of the service; however, is not ISP friendly (due to asymmetric upload/download rate of residential ISPs), may have security and incentive concerns

loss-tolerant applications e.g., video streaming – not of utmost important that every bit gets through

bandwidth-sensitive vs. elastic applications the former requires a certain amount of throughput to function (e.g., media); the latter just uses whatever is available (e.g., email)

services provided by transfer protocols reliable data transfer, security provided by TCP (the latter with SSL/TLS); throughput and timing are not guaranteed by current internet protocols

2.2 Overview of the WWW and HTTP

HTTP and the transfer layer HTTP runs over TCP (not over UDP)

stateless HTTP is stateless – doesn't maintain any information about previous information sent

round-trip time (RTT) latency from client to server back to client

web cache may be implemented locally, or through a local server

conditional GET may be used to keep cache up to date; cache asks server for updates, server sends updated file or text message if not updated