Computer Networking

Michaelmas/Lent Term
M/W/F 11:00-12:00
LT1 in Gates Building

Slide Set 1
Andrew W. Moore
andrew.moore@cl.cam.ac.uk
2016-2017

Computer Networking UROP
• Assessed Practicals for Computer Networking.
  – so supervisors can set/use work
  – so we can have a Computer Networking tick
    running over summer 2016
    Talk to me.

Part 2 projects for 16-17
• Fancy doing something at scale or speed?
  Talk to me.
Topic 1 Foundation

- Administrivia
- Networks
- Channels
- Multiplexing
- Performance: loss, delay, throughput

Course Administration

Commonly Available Texts
- Computer Networking: A Top-Down Approach
  Kurose and Ross, 7th edition 2016, Addison-Wesley
  (6th and 5th edition is also commonly available)
- Computer Networks: A Systems Approach
  Peterson and Davie, 5th edition 2011, Morgan-Kaufman

Other Selected Texts (non-representative)
- Internetworking with TCP/IP, vol. I + II
  Comer & Stevens, Prentice Hall
  Stevens, Fenner & Rudoff, Prentice Hall

Thanks

- Slides are a fusion of material from Brad Smith, Ian Leslie, Richard Black, Jim Kurose, Keith Ross, Larry Peterson, Bruce Davie, Jen Rexford, Ion Stoica, Vern Paxson, Scott Shenker, Frank Kelly, Stefan Savage, Jon Crowcroft, Mark Handley, Sylvia Ratnasamy, and Adam Greenhalgh (and to those others I’ve forgotten, sorry.)
- Supervision material is drawn from Stephen Kell, Andy Rice, and the fantastic TA teams of 144 and 168
- I want practicals too.... 😊
- Finally thanks to the Part 1b students past and Andrew Rice for all the tremendous feedback.

What is a network?

- A system of “links” that interconnect “nodes” in order to move “information” between nodes

- Yes, this is very vague

There are many different types of networks

- Internet
- Telephone network
- Transportation networks
- Cellular networks
- Supervisory control and data acquisition networks
- Optical networks
- Sensor networks

We will focus almost exclusively on the Internet

The Internet is transforming everything

- WWW
- Email
- File transfer
- Chat
- Other services

Took the dissemination of information to the next level
The Internet is big business

- Many large and influential networking companies
  - Cisco, Broadcom, AT&T, Verizon, Akamai, Huawei, ...
  - $132B+ industry (carrier and enterprise alone)

- Networking central to most technology companies
  - Google, Facebook, Intel, HP, Dell, VMware, ...

Internet research has impact

- The Internet started as a research experiment!
- 5 of 10 most cited authors work in networking
- Many successful companies have emerged from networking research(ers)

But why is the Internet interesting?

“What’s your formal model for the Internet?” — theorists
“Aren’t you just writing software for networks” — hackers
“You don’t have performance benchmarks???” — hardware folks
“Isn’t it just another network?” — old timers at AT&T
“What’s with all these TLA protocols?” — all
“But the Internet seems to be working...” — my mother

A few defining characteristics of the Internet

- The Internet ties together different networks
  - >18,000 ISP networks

A federated system

- Tied together by IP — the “Internet Protocol” — a single common interface between users and the network and between networks

A federated system

- The Internet ties together different networks
- >18,000 ISP networks

- A single, common interface is great for interoperability...
- …but tricky for business

- Why does this matter?
  - ease of interoperability is the Internet’s most important goal
  - practical realities of incentives, economics and real-world trust drive topology, route selection and service evolution
Tremendous scale

- 3.42 Billion users (46% of world population)
- 1.3+ Trillion unique URLs from 1.1 Trillion servers
- 219 Billion emails sent
- 2+ Billion smartphones
- 1.79 Billion Facebook users
- 3.4+ Billion WhatsApp messages per day
- 11.6 Billion YouTube videos watched per day
- 800 hours of YouTube video added per minute
- Network links that carry 1.5 Terabits/second

Enormous diversity and dynamic range

- Communication latency: microseconds to seconds ($10^6$)
- Bandwidth: 1Kbits/second to 100 Gigabits/second ($10^7$)
- Technology: optical, wireless, satellite, copper
- Endpoint devices: from sensors and cell phones to datacenters and supercomputers
- Applications: social networking, file transfer, skype, live TV, gaming, remote medicine, backup, IM
- Users: the governing, governed, operators, malicious, naive, savvy, embarrassed, paranoid, addicted, cheap ...

Constant Evolution

1970s:
- 56kilobits/second "backbone" links
- <100 computers, a handful of sites in the US (and one UK)
- Telnet and file transfer are the "killer" applications

Today
- 100+Gigabits/second backbone links
- 10B+ devices, all over the globe
- 20M Facebook apps installed per day

Asynchronous Operation

- Fundamental constraint: speed of light
- Consider:
  - How many cycles does your 3GHz CPU in Cambridge execute before it can possibly get a response from a message it sends to a server in Palo Alto?
    - Cambridge to Palo Alto: 8,609 km
    - Traveling at 300,000 km/s: 28.70 milliseconds
    - Then back to Cambridge: 2 x 28.70 = 57.39 milliseconds
    - 3,000,000,000 cycles/sec * 0.00005739 = 172,179,999 cycles!
- Thus, communication feedback is always dated

Prone to Failure

- To send a message, all components along a path must function correctly
  - software, modem, wireless access point, firewall, links, network interface cards, switches,…
  - Including human operators
- Consider: 50 components, that work correctly 99% of time -> 39.5% chance communication will fail
- Plus, recall
  - scale -> lots of components
  - asynchrony -> takes a long time to hear (bad) news
  - federation (internet) -> hard to identify fault or assign blame

An Engineered System

- Constrained by what technology is practical
  - Link bandwidths
  - Switch port counts
  - Bit error rates
  - Cost
  - …
Recap: The Internet is...

- A complex federation
- Of enormous scale
- Dynamic range
- Diversity
- Constantly evolving
- Asynchronous in operation
- Failure prone
- Constrained by what's practical to engineer
- Too complex for theoretical models
- "Working code" doesn't mean much
- Performance benchmarks are too narrow

Performance – not just bits per second

Second order effects
- Image/Audio quality

Other metrics...
- Network efficiency (good-put versus throughput)
- User Experience? (World Wide Wait)
- Network connectivity expectations
- Others?

Channels Concept
(This channel definition is very abstract)

- Peer entities communicate over channels
- Peer entities provide higher-layer peers with higher-layer channels

A channel is that into which an entity puts symbols and which causes those symbols (or a reasonable approximation) to appear somewhere else at a later point in time.

Example Physical Channels

These example physical channels are also known as Physical Media

Twisted Pair (TP)
- Two insulated copper wires
  - Category 3: traditional phone wires, 10 Mbps Ethernet
  - Category 6: 1000 Mbps Ethernet
- Shielded (STP)
- Unshielded (UTP)

Coaxial cable:
- Two concentric copper conductors
- Bidirectional
- Baseband:
  - Single channel on cable
  - Legacy Ethernet
- Broadband:
  - Multiple channels on cable
  - HFC (Hybrid Fiber Coax)

Fiber optic cable:
- High-speed operation
- Point-to-point transmission
- Low error rate
- Immune to electromagnetic noise

More Physical media: Radio

- Bidirectional and multiple access
- Propagation environment effects:
  - Reflection
  - Obstruction by objects
  - Interference

Radio link types:
- Terrestrial microwave
  - e.g. 45 Mbps channels
  - LAN (e.g., WiFi)
  - 1-10 Mbps, 54 Mbps, 200 Mbps
- Wide-area (e.g., cellular)
  - 4G cellular: ~ 4 Mbps
- Satellite
  - Kbps to 45 Mbps channel (or multiple smaller channels)
  - 270 ms end-to-end delay
  - Geosynchronous versus low altitude
Nodes and Links

Channels = Links
Peer entities = Nodes

Properties of Links (Channels)

- Bandwidth (capacity): "width" of the links
  - number of bits sent or received per unit time (bits/sec or bps)
- Latency (delay): "length" of the link
  - propagation time for data to travel along the link (seconds)
- Bandwidth-Delay Product (BDP): "volume" of the link
  - amount of data that can be "in flight" at any time
  - propagation delay = bits/time = total bits in link

Examples of Bandwidth-Delay

- Same city over a slow link:
  - BW = 100Mbps
  - Latency = 0.1ms
  - BDP = 10,000 bits = 1.25KBytes
- Cross-country over fast link:
  - BW = 10Gbps
  - Latency = 10ms
  - BDP = 10^8 bits = 12.5GBytes

Packet Delay

**Sending a 100B packet from A to B?**

- Time to transmit 100 bytes = 800 ms
- Time when the last bit reaches B = 800 ms + 1/10 ms

**Sending 100B packets from A to B?**

- Time to transmit 100 bytes = 800 ms
- The last bit reaches B at
  - Time = (800 ms) + (800 ms) + (800 ms) + 1 ms

Packet Delay: The "pipe" view

Sending 100B packets from A to B?
Packet Delay: The "pipe" view

Sending 100B packets from A to B?

- 1Mbps, 10ms (BDP=10,000)

- 1Mbps, 5ms (BDP=5,000)

- 10Mbps, 1ms (BDP=10,000)

What if we used 200Byte packets??

- 1Mbps, 10ms (BDP=10,000)

Recall Nodes and Links

A

B

What if we have more nodes?

One link for every node?

Need a scalable way to interconnect nodes

Solution: A switched network

Nodes share network link resources

How is this sharing implemented?

Two forms of switched networks

- Circuit switching (used in the POTS: Plain Old Telephone system)
- Packet switching (used in the Internet)
Circuit switching

Idea: source reserves network capacity along a path

(1) Node A sends a reservation request
(2) Interior switches establish a connection — i.e., “circuit”
(3) A starts sending data
(4) A sends a “teardown circuit” message

Old Time Multiplexing

Time-Division Multiplexing/Demultiplexing

• Time divided into frames; frames into slots
• Relative slot position inside a frame determines to which conversation data belongs
  — e.g., slot 0 belongs to orange conversation
• Slots are reserved (released) during circuit setup (teardown)
• If a conversation does not use its circuit capacity is lost!

Circuit Switching: FDM and TDM

Frequency Division Multiplexing

Example: 4 users

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Radio 2 88.9 MHz</th>
<th>Radio 3 91.1 MHz</th>
<th>Radio 4 93.3 MHz</th>
<th>Radio X 95.5 MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

Time Division Multiplexing

<table>
<thead>
<tr>
<th>Radio Schedule</th>
<th>News, Sports, Weather, Local, News, Sports...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>0, 1, 2, 3, 4</td>
</tr>
<tr>
<td>Time</td>
<td>0, 1, 2, 3, 4</td>
</tr>
</tbody>
</table>

Timing in Circuit Switching

Timing in Circuit Switching


circuit switching: pros and cons

• Pros
  – guaranteed performance
  – fast transfer (once circuit is established)

• Cons
Timing in Circuit Switching

Circuit switching: pros and cons

- **Pros**
  - guaranteed performance
  - fast transfers (once circuit is established)

- **Cons**
  - wastes bandwidth if traffic is “bursty”
  - connection setup time is overhead

Circuit switching

Circuit switching doesn’t “route around failure”
Circuit switching: pros and cons

• Pros
  – guaranteed performance
  – fast transfers (once circuit is established)

• Cons
  – wastes bandwidth if traffic is “bursty”
  – connection setup time is overhead
  – recovery from failure is slow

Numerical example

• How long does it take to send a file of 640,000 bits from host A to host B over a circuit-switched network?
  – All links are 1.536 Mbps
  – Each link uses TDM with 24 slots/sec
  – 500 msec to establish end-to-end circuit

Let’s work it out!

1/24 * 1.536 Mb/s = 64 kb/s

640,000 / 64kb/s = 10s

10s + 500ms = 10.5s

Two forms of switched networks

• Circuit switching (e.g., telephone network)
• Packet switching (e.g., Internet)

Packet Switching

• Data is sent as chunks of formatted bits (Packets)
• Packets consist of a “header” and “payload”
  – payload is the data being carried
  – header holds instructions to the network for how to handle packet (think of the header as an API)

Packet Switching

• Data is sent as chunks of formatted bits (Packets)
• Packets consist of a “header” and “payload”
• Switches “forward” packets based on their headers
Switches forward packets

Timing in Packet Switching

What about the time to process the packet at the switch?
- We’ll assume it’s relatively negligible (mostly true)

Timing in Packet Switching

Could the switch start transmitting as soon as it has processed the header?
- Yes! This would be called a "cut through" switch

Timing in Packet Switching

We will always assume a switch processes forwards a packet after it has received it entirely. This is called "store and forward" switching.

Packet Switching

- Data is sent as chunks of formatted bits (Packets)
- Packets consist of a “header” and “payload”
- Switches “forward” packets based on their headers
- Each packet travels independently — no notion of packets belonging to a “circuit”
Packet Switching

- Data is sent as chunks of formatted bits (Packets)
- Packets consist of a “header” and “payload”
- Switches “forward” packets based on their headers
- Each packet travels independently
- No link resources are reserved in advance. Instead, packet switching leverages **statistical multiplexing** (stat muxing)

Multiplexing

Sharing makes things efficient (cost less)
- One airplane/train for 100’s of people
- One telephone for many calls
- One lecture theatre for many classes
- One computer for many tasks
- One network for many computers
- One datacenter many applications

Three Flows with Bursty Traffic

<table>
<thead>
<tr>
<th>Data Rate 1</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Rate 2</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Rate 3</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When Each Flow Gets 1/3rd of Capacity

Frequent Overloading

<table>
<thead>
<tr>
<th>Data Rate 1</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Rate 2</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Rate 3</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When Flows Share Total Capacity

No Overloading

Statistical multiplexing relies on the assumption that not all flows burst at the same time.

**Very similar to insurance, and has same failure case**

Three Flows with Bursty Traffic

<table>
<thead>
<tr>
<th>Data Rate 1</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Rate 2</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Rate 3</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Three Flows with Bursty Traffic

Data Rate 1

Data Rate 2

Data Rate 3

Time

Capacity

Data Rate 1 + 2 + 3 >> Capacity

What do we do under overload?

Statistical multiplexing: pipe view

No Overload

Statistical multiplexing: pipe view

Queue overload into Buffer

Transient Overload
Not such a rare event
Statistical multiplexing: pipe view

Transient Overload
Not such a rare event

Queue overload into Buffer

Buffer absorbs transient bursts

Statistical multiplexing: pipe view

Transient Overload
Not such a rare event

Queue overload into Buffer

Statistical multiplexing: pipe view

Transient Overload
Not such a rare event

Queue overload into Buffer

Statistical multiplexing: pipe view

What about persistent overload?
Will eventually drop packets

Queue overload into Buffer
Queues introduce queuing delays

- Recall, packet delay = transmission delay + propagation delay (*)
- With queues (statistical multiplexing) packet delay = transmission delay + propagation delay + queuing delay (*)
- Queuing delay caused by “packet interference”
- Made worse at high load
  - less “idle time” to absorb bursts
  - think about traffic jams at rush hour or rail network failure

Queuing delay

- R = link bandwidth (bps)
- L = packet length (bits)
- a = average packet arrival rate

![Queuing delay graph]

“Real” Internet delays and routes

```
traceroute: rio.cl.cam.ac.uk to munnari.oz.au
(tracepath to path is extra)
```

![Traceroute diagram]

Internet structure: network of networks

- a packet passes through many networks!

![Internet structure diagram]
Internet structure: network of networks

- "Tier-2" ISPs: smaller (often regional) ISPs
  - Connect to one or more tier-1 ISPs, possibly other tier-2 ISPs

Tier-1 ISPs: e.g., Sprint

Packet Switching

- Data is sent as chunks of formatted bits (Packets)
- Packets consist of a "header" and "payload"
- Switches "forward" packets based on their headers
- Each packet travels independently
- No link resources are reserved in advance. Instead packet switching leverages statistical multiplexing
  - allows efficient use of resources
  - but introduces queues and queuing delays

Packet switching versus circuit switching

Packet switching may (does!) allow more users to use network

- 1 Mb/s link
- each user:
  - 100 kb/s when "active"
  - active 10% of time
- circuit-switching:
  - 10 users
- packet switching:
  - with 35 users, probability > 10 active at same time is less than 0.0004

Packet switching versus circuit switching

Q: how did we get value 0.0004?

- 1 Mb/s link
- each user:
  - 100 kb/s when "active"
  - active 10% of time
- circuit-switching:
  - 10 users
- packet switching:
  - with 35 users, probability > 10 active at same time is less than 0.0004

HINT: Binomial Distribution
## Circuit switching: pros and cons

- **Pros**
  - guaranteed performance
  - fast transfers (once circuit is established)

- **Cons**
  - wastes bandwidth if traffic is "bursty"
  - connection setup adds delay
  - recovery from failure is slow

## Packet switching: pros and cons

- **Cons**
  - no guaranteed performance
  - header overhead per packet
  - queues and queuing delays

- **Pros**
  - efficient use of bandwidth (stat. muxing)
  - no overhead due to connection setup
  - resilient – can 'route around trouble'

## Summary

- A sense of how the basic ‘plumbing’ works
  - links and switches
  - packet delays= transmission + propagation + queuing + (negligible) per-switch processing
  - statistical multiplexing and queues
  - circuit vs. packet switching
Topic 2 – Architecture and Philosophy

- Abstraction
- Layering
- Layers and Communications
- Entities and Peers
- What is a protocol?
- Protocol Standardization
- The architects process
  - How to break system into modules
  - Where modules are implemented
  - Where is state stored
- Internet Philosophy and Tensions

Abstraction Concept

A mechanism for breaking down a problem

**what not how**

- eg Specification versus implementation
- eg Modules in programs

Allows replacement of implementations without affecting system behavior

**Vertical versus Horizontal**

“Vertical” what happens in a box “How does it attach to the network?”

“Horizontal” the communications paths running through the system

**Hint:** paths are build on top of (“layered over”) other paths

Computer System Modularity

Partition system into modules & abstractions:

- Well-defined interfaces give flexibility
  - **Hides** implementation - can be freely changed
  - Extend functionality of system by adding new modules
- E.g., libraries encapsulating set of functionality
- E.g., programming language + compiler abstracts away how the particular CPU works ...

Computer System Modularity (cnt’ d)

- Well-defined interfaces hide information
  - Isolate **assumptions**
  - Present high-level **abstractions**
- But can impair performance!
- Ease of implementation vs worse performance

Network System Modularity

Like software modularity, but:

- Implementation is distributed across many machines (routers and hosts)
- Must decide:
  - How to break system into modules
    - **Layering**
  - Where modules are implemented
    - **End-to-End Principle**
  - Where state is stored
    - **Fate-sharing**

Layering Concept

- A restricted form of abstraction: system functions are divided into layers, one built upon another
- Often called a **stack**; but not a data structure!

<table>
<thead>
<tr>
<th>Layering Concept</th>
<th>Table 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>thoughts</td>
<td></td>
</tr>
<tr>
<td>speaking 1</td>
<td></td>
</tr>
<tr>
<td>speaking 2</td>
<td></td>
</tr>
<tr>
<td>speaking 3</td>
<td></td>
</tr>
<tr>
<td>T KHz analog</td>
<td></td>
</tr>
<tr>
<td>speaking 5</td>
<td></td>
</tr>
<tr>
<td>4 K Hz samples</td>
<td></td>
</tr>
<tr>
<td>D/A, A/D</td>
<td></td>
</tr>
<tr>
<td>companding</td>
<td></td>
</tr>
<tr>
<td>multiplexing</td>
<td></td>
</tr>
<tr>
<td>framing</td>
<td></td>
</tr>
<tr>
<td>modulation</td>
<td></td>
</tr>
<tr>
<td>Analog signal</td>
<td></td>
</tr>
</tbody>
</table>
Layers and Communications

- Interaction only between adjacent layers
- Layer n uses services provided by layer n-1
- Layer n provides service to layer n+1
- Bottom layer is physical media
- Top layer is application

Entities and Peers

**Entity** – a thing (an independent existence)

Entities interact with the layers above and below

Entities communicate with peer entities
  - same level but different place (e.g., different person, different box, different host)

Communications between peers is supported by entities at the lower layers

Entities usually do something useful

- Encryption – Error correction – Reliable Delivery
- Nothing at all is also reasonable

Not all communications is end-to-end

Examples for things in the middle

- IP Router – Mobile Phone Cell Tower
- Person translating French to English

Entities and Peers

Layering and Embedding

In Computer Networks we often see higher-layer information embedded within lower-layer information

- Such embedding can be considered a form of layering
- Higher-layer information is generated by stripping off headers and trailers of the current layer
- E.g., an IP entity only looks at the IP headers

*BUT* embedding is not the only form of layering

Layering is to help understand a communications system

NOT determine implementation strategy

Layering and Embedding

Distributing Layers Across Network

- Layers are simple if only on a single machine
  - Just stack of modules interacting with those above/below

- But we need to implement layers across machines
  - Hosts
  - Routers (switches)

- What gets implemented where?
**What Gets Implemented on Host?**
- Bits arrive on wire, must make it up to application
  - Therefore, all layers must exist at the host

**What Gets Implemented on a Router?**
- Bits arrive on wire
  - Physical layer necessary
- Packets must be delivered to next-hop
  - Datalink layer necessary
- Routers participate in global delivery
  - Network layer necessary
- Routers don’t support reliable delivery
  - Transport layer (and above) not supported

**What Gets Implemented on Switches?**
- Switches do what routers do, except they don’t participate in global delivery, just local delivery
- They only need to support Physical and Datalink
  - Don’t need to support Network layer
- Won’t focus on the router/switch distinction
  - When I say switch, I almost always mean router
  - Almost all boxes support network layer these days
  - Routers have switches but switches do not have routers

**The Internet Hourglass**
- There is just one network-layer protocol, IP.
  - The “narrow waist” facilitates interoperability.

**Internet protocol stack versus OSI Reference Model**

**ISO/OSI reference model**
- **presentation**: allow applications to interpret meaning of data, e.g., encryption, compression, machine-specific conventions
- **session**: synchronization, checkpointing, recovery of data exchange
- Internet stack “missing” these layers!
  - these services, if needed, must be implemented in application
  - needed?
What is a protocol?

Human protocols:
- "what's the time?"
- "I have a question"
- introductions
... specific msgs sent
... specific actions taken when msgs received, or other events

Network protocols:
- machines rather than humans
- all communication activity in Internet governed by protocols

Protocols define format, order of msgs sent and received among network entities, and actions taken on msg transmission, receipt.

So many Standards Problem

- Many different packet-switching networks
- Each with its own Protocol
- Only nodes on the same network could communicate

INTERnet Solution

- Gateways

Alternative to Standardization?

- Have one implementation used by everyone
- Open-source projects
  - Which has had more impact, Linux or POSIX?
- Or just sole-sourced implementation
  - Skype, many P2P implementations, etc.
A Multitude of Apps Problem

- Re-implement every application for every technology?
- No! But how does the Internet design avoid this?

Solution: Intermediate Layers

- Introduce intermediate layers that provide set of abstractions for various network functionality and technologies
  - A new app/media implemented only once
  - Variation on “add another level of indirection”

Remember that slide!

- The relationship between architectural principles and architectural decisions is crucial to understand

Internet Design Goals (Clark ‘88)

- Connect existing networks
- Robust in face of failures
- Support multiple types of delivery services
- Accommodate a variety of networks
- Allow distributed management
- Easy host attachment
- Cost effective
- Allow resource accountability

Real Goals

- Build something that works!
- Connect existing networks
- Robust in face of failures
- Support multiple types of delivery services
- Accommodate a variety of networks
- Allow distributed management
- Easy host attachment
- Cost effective
- Allow resource accountability

In the context of the Internet
Three Observations

- Each layer:
  - Depends on layer below
  - Supports layer above
  - Independent of others

- Multiple versions in layer
  - Interfaces differ somewhat
  - Components pick which lower-level protocol to use

- But only one IP layer
  - Unifying protocol

Layering Crucial to Internet’s Success

- Reuse

- Hides underlying detail

- Innovation at each level can proceed in parallel

- Pursued by very different communities

What are some of the drawbacks of protocols and layering?

- Layer N may duplicate lower layer functionality
  - e.g., error recovery to retransmit lost data

- Information hiding may hurt performance
  - e.g., packet loss due to corruption vs. congestion

- Headers start to get really big
  - e.g., typical TCP+IP+Ethernet is 54 bytes

- Layer violations when the gains too great to resist
  - e.g., TCP-over-wireless

- Layer violations when network doesn’t trust ends
  - e.g., firewalls

Placing Network Functionality

- Hugely influential paper: “End-to-End Arguments in System Design” by Saltzer, Reed, and Clark (’84)
  - articulated as the “End-to-End Principle” (E2E)

- Endless debate over what it means

- Everyone cites it as supporting their position (regardless of the position!)

Basic Observation

- Some application requirements can only be correctly implemented end-to-end
  - reliability, security, etc.

- Implementing these in the network is hard
  - every step along the way must be fail proof

- Hosts
  - Can satisfy the requirement without network’s help
  - Will/must do so, since they can’t rely on the network
Example: Reliable File Transfer

- Solution 1: make each step reliable, and string them together to make reliable end-to-end process
- Solution 2: end-to-end check and retry

Discussion

- Solution 1 is incomplete
  - What happens if any network element misbehaves?
  - Receiver has to do the check anyway!

- Solution 2 is complete
  - Full functionality can be entirely implemented at application layer with no need for reliability from lower layers

- Is there any need to implement reliability at lower layers?

Summary of End-to-End Principle

- Implementing functionality (e.g., reliability) in the network
  - Doesn’t reduce host implementation complexity
  - Does increase network complexity
  - Probably increases delay and overhead on all applications even if they don’t need the functionality (e.g., VoIP)

- However, implementing in the network can improve performance in some cases
  - e.g., consider a very lossy link

“Only-if-Sufficient” Interpretation

- Don’t implement a function at the lower levels of the system unless it can be completely implemented at this level

  - Unless you can relieve the burden from hosts, don’t bother

“Only-if-Necessary” Interpretation

- Don’t implement anything in the network that can be implemented correctly by the hosts

- Make network layer absolutely minimal
  - This E2E interpretation trumps performance issues
  - Increases flexibility, since lower layers stay simple

“Only-if-Useful” Interpretation

- If hosts can implement functionality correctly, implement it in a lower layer only as a performance enhancement

  - But do so only if it does not impose burden on applications that do not require that functionality
We have some tools:

- Abstraction
- Layering
- Layers and Communications
- Entities and Peers
- Protocol as motivation
- Examples of the architects process
- Internet Philosophy and Tensions
**Topic 3: The Data Link Layer**

**Our goals:**
- understand principles behind data link layer services:
  - (these are methods & mechanisms in your networking toolbox)
  - error detection, correction
  - sharing a broadcast channel: multiple access
  - link layer addressing
  - reliable data transfer, flow control:
- instantiation and implementation of various link layer technologies
  - Wired Ethernet (aka 802.3)
  - Wireless Ethernet (aka 802.11 WiFi)
- Algorithms
  - Binary Exponential Backoff
  - Spanning Tree

**Link Layer: Introduction**

**Some terminology:**
- hosts and routers are nodes
- communication channels that connect adjacent nodes along communication path are links
  - wired links
  - wireless links
  - LANs
- layer-2 packet is a frame, encapsulates datagram

**Link Layer (Channel) Services**

- framing, link access:
  - encapsulate datagram into frame, adding header, trailer
  - channel access if shared medium
  - “MAC” addresses used in frame headers to identify source, dest
  - different from IP address!
- reliable delivery between adjacent nodes
  - we see some of this again in the Transport Topic
  - seldom used on low bit-error link (fiber, some twisted pair)
  - wireless links: high error rates
- Q: why both link-level and end-end reliability?

**Link Layer (Channel) Services - 2**

- flow control:
  - pacing between adjacent sending and receiving nodes
- error detection:
  - errors caused by signal attenuation, noise.
  - receiver detects presence of errors:
    - signals sender for retransmission or drops frame
- error correction:
  - receiver identifies and corrects bit error(s) without resorting to retransmission
- half-duplex and full-duplex
  - with half duplex, nodes at both ends of link can transmit, but not at same time

**Where is the link layer implemented?**

- in each and every host
- link layer implemented in “adaptor” (aka network interface card NIC)
  - Ethernet card, PCMCI card, 802.11 card
  - implements link, physical layer
- attaches into host’s system buses
- combination of hardware, software, firmware

**Adaptors Communicating**

- sending side:
  - encapulates datagram in frame
  - encodes data for the physical layer
  - adds error checking bits, provide reliability, flow control, etc.
- receiving side:
  - decodes data from the physical layer
  - looks for errors, provide reliability, flow control, etc.
  - extracts datagram, passes to upper layer at receiving side
Coding – a channel function

Change the representation of data.

Given Data \[\xrightarrow{\text{Encoding}}\] Changed Data

Decoding

1. Encryption: MyPasswd \[\xrightarrow{\text{<>}}\] AA$$$$ff
2. Error Detection: AA$$$$ff \xrightarrow{\text{<>}} AA$$$$ffff
3. Compression: AA$$$$ffff \xrightarrow{\text{<>}} A2$4f4
4. Analog: A2$4f4 \xrightarrow{\text{<>}}

Coding

Change the representation of data.

Given Data \[\xrightarrow{\text{Encoding}}\] Changed Data

Decoding

1. Encryption: MyPasswd \[\xrightarrow{\text{<>}}\] AA$$$$ff
2. Error Detection: AA$$$$ff \xrightarrow{\text{<>}} AA$$$$ffff
3. Compression: AA$$$$ffff \xrightarrow{\text{<>}} A2$4f4
4. Analog: A2$4f4 \xrightarrow{\text{<>}}

Line Coding Examples

Non-Return-to-Zero (NRZ) [Baud = bit-rate]

Data to send

Line Coding – Block Code example

Block coding transfers data with a fixed overhead: 20% less information per Baud in the case of 4B/5B.

So to send data at 100Mbps; the line rate (the Baud rate) must be 125Mbps.

1Gbps uses an 8b/10b codec; encoding entire bytes at a time but with 25% overhead.
Line Coding Scrambling – with secrecy

Step 1
Scrambling Sequence
Communications Channel
Message XOR Sequence
Message

Step 2

Scrambling Sequence
Scrambling Sequence
Message XOR Sequence
Message

Step 3
Don’t ever reuse Scrambling sequence, ever. <<< this is quite important

Line Coding Scrambling – no secrecy

Scrambling Sequence
Communications Channel
Message XOR Sequence
Message

Scrambling Sequence

This is a diagram of line coding and scrambling. The process involves encoding messages into a scrambled format for secure transmission. The diagrams illustrate the steps involved in scrambling and unscrambling messages, emphasizing the importance of not reusing the scrambling sequence to maintain security.

Line Coding Examples (Hybrid)

...1001111011101000100111101000111010110111011110100...
...1001111011101000100111101000111010110111011110100..

Inserted bits marking “start of frame/block/sequence”
Scramble / Transmit / Unscramble

...010001110110110101000100111101101000101101010010011101011101001001011101111000...

Identify (and remove) “start of frame/block/sequence”
This gives you the Byte delineations for free

64b/66b combines a scrambler and a framer. The start of frame is a pair of bits 01 or 10: 10 means “this frame contains data and control” – control could be configuration information, length of encoded data or simply “this line is idle” (no data at all)

Multiple Access Mechanisms

Each dimension is orthogonal (so may be trivially combined)
There are other dimensions too; can you think of them?
Code Division Multiple Access (CDMA) (not to be confused with CSMA!)

- used in several wireless broadcast channels (cellular, satellite, etc) standards
- unique “code” assigned to each user; i.e., code set partitioning
- all users share same frequency, but each user has own “chipping” sequence (i.e., code) to encode data
- encoded signal = (original data) XOR (chipping sequence)
- decoding: inner-product of encoded signal and chipping sequence
- allows multiple users to “coexist” and transmit simultaneously with minimal interference (if codes are orthogonal)

CDMA Encode/Decode

sender adds code

channel output $Z_{m,n}$

received input

receiver removes code

Coding Examples summary

- Common Wired coding
  - Block codecs: table-lookups
  - fixed overhead, inline control signals
  - Scramblers: shift registers
  - overhead free

Like earlier coding schemes and error correction/detection; you can combine these
- e.g., 10Gb/s Ethernet may use a hybrid

CDMA (Code Division Multiple Access)
- coping intelligently with competing sources
- Mobile phones

Error Detection and Correction

How to use coding to deal with errors in data communication?

Basic Idea:
1. Add additional information to a message.
2. Detect an error and re-send a message.
   Or, fix an error in the received message.
How to use coding to deal with errors in data communication?

Basic Idea:
1. Add additional information to a message.
2. Detect an error and re-send a message.
   Or, fix an error in the received message.

Error Detection and Correction

Error Detection

EDC = Error Detection and Correction bits (redundancy = overhead)
D = Data protected by error checking, may include header fields

- Error detection not 100% reliable!
- Protocol may miss some errors, but rarely
- Larger EDC field yields better detection and correction

![Diagram of error detection and correction](image)

Error Detection Code

Sender: Y = generateCheckBit(X); send(XY);
Receiver: receive(X1Y1); Y2 = generateCheckBit(X1); if (Y1 != Y2) ERROR; else NOERROR.

Noise

Problem: This simple parity cannot detect two-bit errors.

Error Detection Code: Parity

Add one bit, such that the number of 1’s is even.

Internet checksum

Goal: detect “errors” (e.g., flipped bits) in transmitted packet
(note: used at transport layer only)

Sender:
- treat segment contents as sequence of 16 bit integers
- checksum: addition (1’s complement sum) of segment contents
- sender puts checksum value into UDP checksum field

Receiver:
- compute checksum of received segment
- check if computed checksum equals checksum field value:
  - NO - error detected
  - YES - no error detected. But maybe errors nonetheless?
**Error Detection Code: CRC**

- CRC means “Cyclic Redundancy Check”.
- More powerful than parity.
  - It can detect various kinds of errors, including 2-bit errors.
- More complex: multiplication, binary division.
- Parameterized by n-bit divisor P.
  - Example: 3-bit divisor 101.
  - Choosing good P is crucial.

**CRC with 3-bit Divisor 101**

```plaintext
1111
1001

CRC
Parity

11
10

101

Multiplication by \(2^3\)
\(D2 = D \cdot 2^3\)

Binary Division by 101
CheckBit = \(D2 \mod 101\)

Add three 0's at the end

Example: 3-bit divisor 101.

**The divisor (P) – Secret sauce of CRC**

- If the divisor were 100, instead of 101, data 1111 and 1001 would give the same check bit 00.
- Mathematical analysis about the divisor:
  - Last bit should be 1.
  - Should contain at least two 1’s.
  - Should be divisible by 11.
- ATM, HDLC, Ethernet each use a CRC with well-chosen fixed divisors

Divisor analysis keeps mathematicians in jobs
(a branch of pure math: combinatorial mathematics)

FYI: in K&R P is called the Generator: \(G\)

**Checksumming: Cyclic Redundancy Check recap**

- view data bits, \(D\), as a binary number
- choose \(r+1\) bit pattern (generator), \(P\)
- goal: choose \(r\) CRC bits, \(R\), such that
  - \(<D, R>\) exactly divisible by \(G\) (modulo 2)
  - receiver knows \(G\), divides \(<D, R>\) by \(G\). If non-zero remainder: error detected!
  - can detect all burst errors less than \(r+1\) bits
- widely used in practice (Ethernet, 802.11 WiFi, ATM)

**CRC Another Example – this time with long division**

Want:
\[ D \cdot 2^r \text{ XOR } R = nP \]

equivalently:
\[ D \cdot 2^r = nP \text{ XOR } R \]

equivalently:
if we divide \(D \cdot 2^r\) by \(P\), want remainder \(R\)

\[ R = \text{remainder}\left(\frac{D \cdot 2^r}{P}\right) \]

FYI: in K&R P is called the Generator: \(G\)

**Error Detection Code becomes….**

**Sender:**
\[ Y = \text{generateCheckBit}(X); \]
\[ \text{send}(XY); \]

**Receiver:**
\[ \text{receive}(X1Y1); \]
\[ Y2 = \text{generateCheckBit}(X1); \]
\[ \text{if} \ (Y1 \neq Y2) \text{ ERROR}; \]
\[ \text{else NOERROR} \]
**Forward Error Correction (FEC)**

**Sender:**
\[ Y = \text{generateCheckBit}(X); \]
\[ \text{send}(XY); \]

**Receiver:**
\[ Y = \text{generateCheckBit}(X); \]
\[ \text{receive}(X1Y1); \]
\[ Y2 = \text{generateCheckBit}(X1); \]
\[ \text{if } (Y1 \neq Y2) \text{ FIXERROR}(X1Y1); \]
\[ \text{else NOERROR}; \]

---

**Basic Idea of Forward Error Correction**

Replace erroneous data by its “closest” error-free data.

**Error Detection vs Correction**

**Error Correction:**
- Cons: More check bits. False recovery.
- Pros: No need to re-send.

**Error Detection:**
- Cons: Need to re-send.
- Pros: Less check bits.

**Usage:**
- Correction: A lot of noise. Expensive to re-send.
- Detection: Less noise. Easy to re-send.
- Can be used together.

---

**Multiple Access Links and Protocols**

Two types of “links”:  
- point-to-point  
  - point-to-point link between Ethernet switch and host  
- broadcast (shared wire or medium)  
  - old-fashioned wired Ethernet (here be dinosaurs – extinct)  
  - upstream HFC (Hybrid Fiber-Coax – the Coax may be broadcast)  
  - Home plug / Powerline networking  
  - 802.11 wireless LAN

**Multiple Access protocols**

- single shared broadcast channel  
- two or more simultaneous transmissions by nodes: interference  
  - collision if node receives two or more signals at the same time  
    multiple access protocol
  - distributed algorithm that determines how nodes share channel, i.e., determine when node can transmit
  - communication about channel sharing must use channel itself!  
    - no out-of-band channel for coordination
Ideal Multiple Access Protocol

Broadcast channel of rate $R$ bps
1. when one node wants to transmit, it can send at rate $R$
2. when $M$ nodes want to transmit, each can send at average rate $R/M$
3. fully decentralized:
   – no special node to coordinate transmissions
   – no synchronization of clocks, slots
4. simple

MAC Protocols: a taxonomy

Three broad classes:
- **Channel Partitioning**
  - divide channel into smaller "pieces" (time slots, frequency, code)
  - allocate piece to node for exclusive use
- **Random Access**
  - channel not divided, allow collisions
  - "recover" from collisions
- **"Taking turns"**
  - nodes take turns, but nodes with more to send can take longer turns

Channel Partitioning MAC protocols: TDMA
(time travel warning – we mentioned this earlier)

**TDMA:** time division multiple access
- access to channel in "rounds"
- each station gets fixed length slot (length = pkt trans time) in each round
- unused slots go idle
- example: station LAN, 1,3,4 have pkt, slots 2,5,6 idle

Channel Partitioning MAC protocols: FDMA
(time travel warning – we mentioned this earlier)

**FDMA:** frequency division multiple access
- channel spectrum divided into frequency bands
- each station assigned fixed frequency band
- unused transmission time in frequency bands go idle
- example: station LAN, 1,3,4 have pkt, frequency bands 2,5,6 idle

“Taking Turns” MAC protocols

Channel partitioning MAC protocols:
- share channel efficiently and fairly at high load
- inefficient at low load: delay in channel access, 1/N bandwidth allocated even if only 1 active node!

Random access MAC protocols
- efficient at low load: single node can fully utilize channel
- high load: collision overhead

“taking turns” protocols
- look for best of both worlds!

Polling:
- master node “invites” slave nodes to transmit in turn
- typically used with “dumb” slave devices
- concerns:
  - polling overhead
  - latency
  - single point of failure (master)
“Taking Turns” MAC protocols

Token passing:
- control token passed from one node to next sequentially.
- token message concerns:
  - token overhead
  - latency
  - single point of failure (token)
- concerns fixed in part by a slotted ring (many simultaneous tokens)

Random Access MAC Protocols

- When node has packet to send
  - Transmit at full channel data rate
  - No a priori coordination among nodes
- Two or more transmitting nodes \(\Rightarrow\) collision
  - Data lost
- Random access MAC protocol specifies:
  - How to detect collisions
  - How to recover from collisions
- Examples
  - ALOHA and Slotted ALOHA
  - CSMA, CSMA/CD, CSMA/CA (wireless)

Key Ideas of Random Access

- Carrier sense
  - Listen before speaking, and don’t interrupt
  - Checking if someone else is already sending data
  - ... and waiting till the other node is done
- Collision detection
  - If someone else starts talking at the same time, stop
  - Realizing when two nodes are transmitting at once
  - ... by detecting that the data on the wire is garbled
- Randomness
  - Don’t start talking again right away
  - Waiting for a random time before trying again

CSMA (Carrier Sense Multiple Access)

- CSMA: listen before transmit
  - If channel sensed idle: transmit entire frame
  - If channel sensed busy, defer transmission
- Human analogy: don’t interrupt others!
- Does this eliminate all collisions?
  - No, because of nonzero propagation delay

ATM

In TDM a sender may only use a pre-allocated slot

In ATM a sender transmits labeled cells whenever necessary

ATM = Asynchronous Transfer Mode – an ugly expression
think of it as ATDM = Asynchronous Time Division Multiplexing
That’s a variant of PACKET SWITCHING to the rest of us – just like Ethernet
but using fixed length slots/packets/cells

Use the media when you need it, but
ATM had virtual circuits and these needed setup...
Worse ATM had an utterly irrational size

CSMA Collisions

Propagation delay: two nodes may not hear each other’s before sending.

Would slots hurt or help?

CSMA reduces but does not eliminate collisions

Biggest remaining problem?
Collisions still take full slot!
How do you fix that?
CSMA/CD (Collision Detection)

- CSMA/CD: carrier sensing, deferral as in CSMA
  - Collisions detected within short time
  - Colliding transmissions aborted, reducing wastage
- Collision detection easy in wired LANs:
  - Compare transmitted, received signals
- Collision detection difficult in wireless LANs:
  - Reception shut off while transmitting (well, perhaps not)
  - Not perfect broadcast (limited range) so collisions local
  - Leads to use of collision avoidance instead (later)

CSMA/CD Collision Detection

B and D can tell that collision occurred.

Note: for this to work, need restrictions on minimum frame size and maximum distance. Why?

Limits on CSMA/CD Network Length

- Latency depends on physical length of link
  - Time to propagate a packet from one end to the other
- Suppose A sends a packet at time t
  - And B sees an idle line at a time just before t + d
  - ... so B happily starts transmitting a packet
- B detects a collision, and sends jamming signal
  - But A can’t see collision until t + 2d

Performance of CSMA/CD

- Time wasted in collisions
  - Proportional to distance d
- Time spend transmitting a packet
  - Packet length p divided by bandwidth b
- Rough estimate for efficiency (K some constant)
  \[ E \approx \frac{p}{b + Kd} \]
  - Note:
    - For large packets, small distances, E ~ 1
    - As bandwidth increases, E decreases
    - That is why high-speed LANs are all switched

Benefits of Ethernet

- Easy to administer and maintain
- Inexpensive
- Increasingly higher speed
- Evolvable!

Evolution of Ethernet

- Changed everything except the frame format
  - From single coaxial cable to hub-based star
  - From shared media to switches
  - From electrical signaling to optical
- Lesson #1
  - The right interface can accommodate many changes
  - Implementation is hidden behind interface
- Lesson #2
  - Really hard to displace the dominant technology
  - Slight performance improvements are not enough
Ethernet: CSMA/CD Protocol

- **Carrier sense:** wait for link to be idle
- **Collision detection:** listen while transmitting
  
  - No collision: transmission is complete
  - Collision: abort transmission & send jam signal
- **Random access:** binary exponential back-off
  
  - After collision, wait a random time before trying again
  - After mth collision, choose K randomly from (0, ..., 2^m - 1)
  - ... and wait for K*512 bit times before trying again
    - Using min packet size as “slot”
    - If transmission occurring when ready to send, wait until end of transmission (CSMA)

The Wireless Spectrum

Metrics for evaluation / comparison of wireless technologies

- Bitrate or Bandwidth
- Range: PAN, LAN, MAN, WAN
- Two-way / One-way
- Multi-Access / Point-to-Point
- Digital / Analog
- Applications and industries
- Frequency – Affects most physical properties:
  
  Distance (free-space loss)
  Penetration, Reflection, Absorption
  Energy proportionality
  Policy: Licensed / Deregulated
  Line of Sight (Fresnel zone)

  - Size of antenna
    - Determined by wavelength – $\lambda = \frac{V}{f}$

Wireless Communication Standards

- Cellular (800/900/1700/1900MHz):
  
  - 2G: GSM / CDMA / GPRS / EDGE
  - 3G: CDMA2000/UMTS/HSDPA/EVDO
  - 4G: LTE, WiMax
- IEEE 802.11 (aka WiFi):
  
  - b: 2.4GHz band, 11Mbps (~4.5 Mbps operating rate)
  - g: 2.4GHz, 54-108Mbps (~19 Mbps operating rate)
  - a: 5.0GHz band, 54-108Mbps (~25 Mbps operating rate)
  - n: 2.4/5Ghz, 150-600Mbps (4x4 mimo).
- IEEE 802.15 – lower power wireless:
  
  - 802.15.1: 2.4GHz, 2.1 Mbps (Bluetooth)
  - 802.15.4: 2.4GHz, 250 Kbps (Sensor Networks)

What Makes Wireless Different?

- Broadcast and multi-access medium...
  
  - err, so....

- BUT, Signals sent by sender don’t always end up at receiver intact

  - Complicated physics involved, which we won’t discuss
  - But what can go wrong?

Path Loss / Path Attenuation

- **Free Space Path Loss:**

  $$L_{FSPL} = \left(\frac{4\pi d}{\lambda}\right)^2$$

  - $d =$ distance
  - $\lambda =$ wavelength
  - $f =$ frequency
  - $c =$ speed of light

  - Reflection, Diffraction, Absorption
  - Terrain contours (Urban, Rural, Vegetation).
  - Humidity
Multipath Effects

- Signals bounce off surface and interfere with one another
- Self-interference

Interference from Other Sources

- **External Interference**
  - Microwave is turned on and blocks your signal
  - Would that affect the sender or the receiver?
- **Internal Interference**
  - Hosts within range of each other collide with one another’s transmission
  - We have to tolerate path loss, multipath, etc., but we can try to avoid internal interference

Wireless Bit Errors

- The lower the SNR (Signal/Noise) the higher the Bit Error Rate (BER)
- We could make the signal stronger...
- Why is this not always a good idea?
  - Increased signal strength requires more power
  - Increases the interference range of the sender, so you interfere with more nodes around you
    - And then they increase their power....
- Local link-layer Error Correction schemes can correct some problems

Let’s focus on **802.11**
aka - WiFi ...
What makes it special?

Deregulation > Innovation > Adoption > Lower cost = Ubiquitous technology

JUST LIKE ETHERNET – not lovely but sufficient

802.11 Architecture

- Designed for limited area
- AP’s (Access Points) set to specific channel
- Broadcast beacon messages with SSID (Service Set Identifier) and MAC Address periodically
- Hosts scan all the channels to discover the AP’s
  - Host associates with AP

Wireless Multiple Access Technique?

- **Carrier Sense**
  - Sender can listen before sending
  - What does that tell the sender?
- **Collision Detection**
  - Where do collisions occur?
  - How can you detect them?
A and C can both send to B but can’t hear each other
– A is a hidden terminal for C and vice versa
– Carrier Sense will be ineffective

Exposed node: B sends a packet to A; C hears this and decides not to send a packet to D (despite the fact that this will not cause interference)
– Carrier sense would prevent a successful transmission.

Key Points
• No concept of a global collision
  – Different receivers hear different signals
  – Different senders reach different receivers
• Collisions are at receiver, not sender
  – Only care if receiver can hear the sender clearly
  – It does not matter if sender can hear someone else
  – As long as that signal does not interfere with receiver
• Goal of protocol:
  – Detect if receiver can hear sender
  – Tell senders who might interfere with receiver to shut up

Basic Collision Avoidance
• Since can’t detect collisions, we try to avoid them
• Carrier sense:
  – When medium busy, choose random interval
  – Wait that many idle timeslots to pass before sending
• When a collision is inferred, retransmit with binary exponential backoff (like Ethernet)
  – Use ACK from receiver to infer “no collision”
  – Use exponential backoff to adapt contention window

CSMA/CA -MA with Collision Avoidance
• Before every data transmission
  – Sender sends a Request to Send (RTS) frame containing the length of the transmission
  – Receiver respond with a Clear to Send (CTS) frame
  – Sender sends data
  – Receiver sends an ACK; now another sender can send data
• When sender doesn’t get a CTS back, it assumes collision

CSMA/CA, can’t
• If other nodes hear RTS, but not CTS: send
  – Presumably, destination for first sender is out of node’s range...
CSMA/CA, con’t

If other nodes hear RTS, but not CTS: send
  – Presumably, destination for first sender is out of node’s range…
  – Can cause problems when a CTS is lost
• When you hear a CTS, you keep quiet until scheduled transmission is over (hear ACK)

Preventing Collisions Altogether
• Frequency Spectrum partitioned into several channels
  – Nodes within interference range can use separate channels
  – Now A and C can send without any interference!
• Most cards have only 1 transceiver
  – Not Full Duplex: Cannot send and receive at the same time
  – Aggregate Network throughput doubles

CSMA/CD vs CSMA/CA (without RTS/CTS)

<table>
<thead>
<tr>
<th>Wired – listen and talk</th>
<th>Wireless – talk OR listen</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Listen for others</td>
<td>1. Listen for others</td>
</tr>
<tr>
<td>3. Send message (and listen)</td>
<td>a. increase your BEB</td>
</tr>
<tr>
<td>4. Collision?</td>
<td>b. sleep</td>
</tr>
<tr>
<td>a. JAM</td>
<td>c. goto 1.</td>
</tr>
<tr>
<td>b. increase your BEB</td>
<td></td>
</tr>
<tr>
<td>c. sleep</td>
<td></td>
</tr>
<tr>
<td>d. goto 1.</td>
<td></td>
</tr>
</tbody>
</table>

Changing the rules: an 802.11 feature

Rate Adaptation
(for a variety of out-of-context reasons often unused)
• base station, mobile dynamically change transmission rate
  (physical layer modulation technique) as mobile moves, SNR varies

\[ \text{SNR} = \begin{cases} 
  \text{BER decreases, BER increases as node moves away from base station} \\
  \text{When BER becomes too high, switch to lower transmission rate but with lower BER} 
\end{cases} \]
Summary of MAC protocols

- **channel partitioning**, by time, frequency or code
  - Time Division, Frequency Division
- **random access** (dynamic),
  - ALOHA, S-ALOHA, CSMA, CSMA/CD
  - carrier sensing: easy in some technologies (wire), hard in others (wireless)
  - CSMA/CD used in Ethernet
  - CSMA/CA used in 802.11
- **taking turns**
  - polling from central site, token passing
  - Bluetooth, FDDI, IBM Token Ring

MAC Addresses

- MAC (or LAN or physical or Ethernet) address:
  - function: get frame from one interface to another physically-connected interface (same network)
  - 48 bit MAC address (for most LANs)
    - burned in NIC ROM, nowadays usually software settable and set at boot time

LAN Address (more)

- MAC address allocation administered by IEEE
- manufacturer buys portion of MAC address space (to assure uniqueness)
- analogy:
  (a) MAC address: like Social Security Number
  (b) IP address: like postal address
- MAC flat address → portability
  - can move LAN card from one LAN to another
- IP hierarchical address NOT portable
  - address depends on IP subnet to which node is attached

Hubs

...physical-layer ["dumb"] repeaters:
- bits coming in one link go out all other links at same rate
- all nodes connected to hub can collide with one another
- no frame buffering
- no CSMA/CD at hub: host NICs detect collisions

Switch

(like a Hub but smarter)

- link-layer device: smarter than hubs, take active role
  - store, forward Ethernet frames
  - examine incoming frame’ s MAC address, selectively forward frame to one-or-more outgoing links when frame is to be forwarded on segment, uses CSMA/CD to access segment
- transparent
  - hosts are unaware of presence of switches
- plug-and-play, self-learning
  - switches do not need to be configured
Switch: allows multiple simultaneous transmissions

- hosts have dedicated, direct connection to switch
- switches buffer packets
- Ethernet protocol used on each incoming link, but no collisions; full duplex
  - each link is its own collision domain
- switching: A-to-A' and B-to-B' simultaneously, without collisions
  - not possible with dumb hub

Switch: self-learning (recap)

- switch learns which hosts can be reached through which interfaces
  - when frame received, switch “learns” location of sender: incoming LAN segment
  - records sender/location pair in switch table

Switch Table

- Q: how does switch know that A' reachable via interface 4, B' reachable via interface 5?
- A: each switch has a switch table, each entry:
  - (MAC address of host, interface to reach host, time stamp)
  - looks like a routing table!
- Q: how are entries created, maintained in switch table?
  - something like a routing protocol?

Switch: frame filtering/forwarding

When frame received:

1. record link associated with sending host
2. index switch table using MAC dest address
3. if entry found for destination
   then {
     if dest on segment from which frame arrived
        then drop the frame
     else forward the frame on interface indicated
   }
   else flood

Interconnecting switches

- switches can be connected together

Q: sending from A to G - how does S1 know to forward frame destined to F via S3 and S5?
A: self learning! (works exactly the same as in single-switch case – flood/forward/drop)
Flooding Can Lead to Loops
- Flooding can lead to forwarding loops
  - E.g., if the network contains a cycle of switches
  - “Broadcast storm”

Solution: Spanning Trees
- Ensure the forwarding topology has no loops
  - Avoid using some of the links when flooding
  - … to prevent loop from forming
- Spanning tree
  - Sub-graph that covers all vertices but contains no cycles
  - Links not in the spanning tree do not forward frames

Graph Has Cycles!
Graph Has No Cycles!

What Do We Know?
- Shortest paths to (or from) a node form a tree
- So, algorithm has two aspects:
  - Pick a root
  - Compute shortest paths to it
- Only keep the links on shortest-path

Constructing a Spanning Tree
- Switches need to elect a root
  - The switch w/ smallest identifier (MAC addr)
- Each switch determines if each interface is on the shortest path from the root
  - Excludes it from the tree if not
- Messages (Y, d, X)
  - From node X
  - Proposing Y as the root
  - And the distance is d

Steps in Spanning Tree Algorithm
- Initially, each switch proposes itself as the root
  - Switch sends a message out every interface
  - … proposing itself as the root with distance 0
  - Example: switch X announces (X, 0, X)
- Switches update their view of the root
  - Upon receiving message (Y, d, Z) from Z, check Y’s id
  - If new id smaller, start viewing that switch as root
- Switches compute their distance from the root
  - Add 1 to the distance received from a neighbor
  - Identify interfaces not on shortest path to the root
  - … and exclude them from the spanning tree
- If root or shortest distance to it changed, “flood” updated message (Y, d+1, X)

Example From Switch #4’s Viewpoint
- Switch #4 thinks it is the root
  - Sends (4, 0, 4) message to 2 and 7
- Then, switch #4 hears from #2
  - Receives (2, 0, 2) message from 2
  - … and thinks that #2 is the root
  - And realizes it is just one hop away
- Then, switch #4 hears from #7
  - Receives (2, 1, 7) from 7
  - And realizes this is a longer path
  - So, prefers its own one-hop path
  - And removes 4-7 link from the tree
Example From Switch #4’s Viewpoint

• Switch #2 hears about switch #1
  – Switch 2 hears (1, 1, 3) from 3
  – Switch 2 starts treating 1 as root
  – And sends (1, 2, 2) to neighbors

• Switch #4 hears from switch #2
  – Switch 4 starts treating 1 as root
  – And sends (1, 3, 4) to neighbors

• Switch #4 hears from switch #7
  – Switch 4 receives (1, 3, 7) from 7
  – And realizes this is a longer path
  – So, prefers its own three-hop path
  – And removes 4-7 link from the tree

Robust Spanning Tree Algorithm

• Algorithm must react to failures
  – Failure of the root node
    • Need to elect a new root, with the next lowest identifier
  – Failure of other switches and links
    • Need to recompute the spanning tree

• Root switch continues sending messages
  – Periodically reannouncing itself as the root (1, 0, 1)
  – Other switches continue forwarding messages

• Detecting failures through timeout (soft state)
  – If no word from root, times out and claims to be the root
  – Delay in reestablishing spanning tree is major problem
  – Work on rapid spanning tree algorithms…

Topic 3: Summary

• principles behind data link layer services:
  – error detection, correction
  – sharing a broadcast channel: multiple access
  – link layer addressing

• instantiation and implementation of various link layer technologies
  – Ethernet
  – switched LANS
  – WiFi

• algorithms
  – Binary Exponential Backoff
  – Spanning Tree
Topic 4: Network Layer

Our goals:
- understand principles behind network layer services:
  - network layer service models
  - forwarding versus routing (versus switching)
  - how a router works
  - routing (path selection)
  - IPv6
- For the most part, the Internet is our example – again.

Addressing (at a conceptual level)
- Assume all hosts have unique IDs
- No particular structure to those IDs
- Later in topic I will talk about real IP addressing
- Do I route on location or identifier?
- If a host moves, should its address change?
  - If not, how can you build scalable Internet?
  - If so, then what good is an address for identification?

Packets (at a conceptual level)
- Assume packet headers contain:
  - Source ID, Destination ID, and perhaps other information

Switches/Routers
- Multiple ports (attached to other switches or hosts)
- Ports are typically duplex (incoming and outgoing)

A Variety of Networks
- ISPs: carriers
  - Backbone
  - Edge
  - Border (to other ISPs)
- Enterprises: companies, universities
  - Core
  - Edge
  - Border (to outside)
- Datacenters: massive collections of machines
  - Top-of-Rack
  - Aggregation and Core
  - Border (to outside)
Switches forward packets

Forwarding Table

<table>
<thead>
<tr>
<th>Destination</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLASGOW</td>
<td>4</td>
</tr>
<tr>
<td>OXFORD</td>
<td>5</td>
</tr>
<tr>
<td>EDINBURGH</td>
<td>2</td>
</tr>
</tbody>
</table>

Forwarding Decisions

- When packet arrives...
  - Must decide which outgoing port to use
  - In single transmission time
  - Forwarding decisions must be **simple**
- Routing state dictates where to forward packets
  - Assume decisions are **deterministic**
- **Global routing state** means collection of routing state in each of the routers
  - Will focus on where this routing state comes from
  - But first, a few preliminaries....

Forwarding vs Routing

- Forwarding: “data plane”
  - Directing a data packet to an outgoing link
  - Individual router using routing state
- Routing: “control plane”
  - Computing paths the packets will follow
  - Routers talking amongst themselves
  - Jointly creating the routing state
- Two very different timescales....

Router definitions

- N = number of external router “ports”
- R = speed (“line rate”) of a port
- Router capacity = N x R

Networks and routers

Examples of routers (core)

**Cisco CRS**

- R=10/40/100 Gbps
- NR = 922 Tbps
- Netflix: 0.7GB per hour (1.5Mb/s)
- ~600 million concurrent Netflix users

72 racks, >1MW
Examples of routers (edge)

Cisco ASR
- \( R = 1/10/40 \text{ Gbps} \)
- \( NR = 120 \text{ Gbps} \)

Examples of routers (small business)

Cisco 3945E
- \( R = 10/100/1000 \text{ Mbps} \)
- \( NR < 10 \text{ Gbps} \)

What's inside a router?

1. Processes packets on their way in
2. Processes packets before they leave
3. Transfers packets from input to output ports
4. Input and Output for the same port are on one physical linecard

What's inside a router?

1. Implement IGP and BGP protocols; compute routing tables
2. Push forwarding tables to the line cards

What's inside a router?

1. Linecards (input)
2. Interconnect (Switching) Fabric
3. Linecards (output)
4. Route/Control Processor
5. Constitutes the control plane
6. Constitutes the data plane

Context + Terminology

- "End hosts"
- "Border Routers"
- "Border Routers"
- "End points"
- "Interior Routers"

"Autonomous System (AS)" or "Domain"
Region of a network under a single administrative entity

"Route" or "Path"
Internet routing protocols are responsible for constructing and updating the forwarding tables at routers.

Routing Protocols

- Routing protocols implement the core function of a network
  - Establish paths between nodes
  - Part of the network's "control plane"

- Network modeled as a graph
  - Routers are graph vertices
  - Links are edges
  - Edges have an associated "cost"
    - e.g., distance, loss

- Goal: compute a "good" path from source to destination
  - "good" usually means the shortest (least cost) path

Internet Routing

- Internet Routing works at two levels
- Each AS runs an intra-domain routing protocol that establishes routes within its domain
  - (AS – region of network under a single administrative entity)
  - Link State, e.g., Open Shortest Path First (OSPF)
  - Distance Vector, e.g., Routing Information Protocol (RIP)
- ASes participate in an inter-domain routing protocol that establishes routes between domains
  - Path Vector, e.g., Border Gateway Protocol (BGP)

Addressing (for now)

- Assume each host has a unique ID (address)
- No particular structure to those IDs
- Later in course will talk about real IP addressing

Outline

- Link State
- Distance Vector
- Routing: goals and metrics (if time)
Link State Routing

- Each node maintains its local "link state" (LS)
  - i.e., a list of its directly attached links and their costs

Dijkstra’s Shortest Path Algorithm

- INPUT:
  - Network topology (graph), with link costs

- OUTPUT:
  - Least cost paths from one node to all other nodes

- Iterative: after $k$ iterations, a node knows the least cost path to its $k$ closest neighbors

Example

Notation

- $c(i,j)$: link cost from node $i$ to $j$; cost is infinite if not direct neighbors; $\geq 0$

- $D(v)$: total cost of the current least cost path from source to destination $v$

- $p(v)$: $v$'s predecessor along path from source to $v$

- $S$: set of nodes whose least cost path definitively known
**Dijkstra’s Algorithm**

1. **Initialization:**
   - $c(i,j)$: link cost from node $i$ to $j$
   - $D(v)$: current cost source to $v$
   - $p(v)$: $v$’s predecessor along path from source to $v$
   - $S$: set of nodes whose least cost path definitively known

2. Set $S = \{A\}$.
3. For all nodes $v$:
   - If $v$ adjacent to $A$:
     - Then $D(v) = c(A,v)$.
   - Else $D(v) = \infty$.

4. Loop:
   - Find $w$ not in $S$ such that $D(w)$ is a minimum.
   - Add $w$ to $S$.
   - Update $D(v)$ for all $v$ adjacent to $w$ and not in $S$.
   - If $D(w) + c(w,v) < D(v)$ then:
     - Update $D(v)$ for all $v$ adjacent to $w$ and not in $S$.
     - $D(v) = D(w) + c(w,v)$; $p(v) = w$.
   - Until all nodes in $S$.

---

**Example: Dijkstra’s Algorithm**

**Initialization:**
- $S = \{A\}$.
- For all nodes $v$:
  - If $v$ adjacent to $A$:
    - Then $D(v) = c(A,v)$.
  - Else $D(v) = \infty$.
- Until all nodes in $S$:...

**Loop:**
- Find $w$ not in $S$ s.t. $D(w)$ is a minimum.
- Add $w$ to $S$.
- Update $D(v)$ for all $v$ adjacent to $w$ and not in $S$.
- If $D(w) + c(w,v) < D(v)$ then:
  - Update $D(v)$ for all $v$ adjacent to $w$ and not in $S$.
  - $D(v) = D(w) + c(w,v)$; $p(v) = w$.
- Until all nodes in $S$.

**Example: Dijkstra’s Algorithm**

**Initialization:**
- $S = \{A\}$.
- For all nodes $v$:
  - If $v$ adjacent to $A$:
    - Then $D(v) = c(A,v)$.
  - Else $D(v) = \infty$.
- Until all nodes in $S$:

**Loop:**
- Find $w$ not in $S$ s.t. $D(w)$ is a minimum.
- Add $w$ to $S$.
- Update $D(v)$ for all $v$ adjacent to $w$ and not in $S$.
- If $D(w) + c(w,v) < D(v)$ then:
  - Update $D(v)$ for all $v$ adjacent to $w$ and not in $S$.
  - $D(v) = D(w) + c(w,v)$; $p(v) = w$.
- Until all nodes in $S$.

---

**Example: Dijkstra’s Algorithm**

**Initialization:**
- $S = \{A\}$.
- For all nodes $v$:
  - If $v$ adjacent to $A$:
    - Then $D(v) = c(A,v)$.
  - Else $D(v) = \infty$.
- Until all nodes in $S$:

**Loop:**
- Find $w$ not in $S$ s.t. $D(w)$ is a minimum.
- Add $w$ to $S$.
- Update $D(v)$ for all $v$ adjacent to $w$ and not in $S$.
- If $D(w) + c(w,v) < D(v)$ then:
  - Update $D(v)$ for all $v$ adjacent to $w$ and not in $S$.
  - $D(v) = D(w) + c(w,v)$; $p(v) = w$.
- Until all nodes in $S$.

---

**Example: Dijkstra’s Algorithm**

**Initialization:**
- $S = \{A\}$.
- For all nodes $v$:
  - If $v$ adjacent to $A$:
    - Then $D(v) = c(A,v)$.
  - Else $D(v) = \infty$.
- Until all nodes in $S$:

**Loop:**
- Find $w$ not in $S$ s.t. $D(w)$ is a minimum.
- Add $w$ to $S$.
- Update $D(v)$ for all $v$ adjacent to $w$ and not in $S$.
- If $D(w) + c(w,v) < D(v)$ then:
  - Update $D(v)$ for all $v$ adjacent to $w$ and not in $S$.
  - $D(v) = D(w) + c(w,v)$; $p(v) = w$.
- Until all nodes in $S$.
Example: Dijkstra’s Algorithm

Step | S (w) | D(B) | D(C) | D(D) | D(E) | D(F)
---|---|---|---|---|---|---
0 | A | 2.2 | 5.2 | 1.2 | 1.2 | 1.2
1 | AD | 4.4 | 2.2 | 2.2 | 2.2 | 2.2
2 | ADE | 3.6 | 4.6 | 4.6 | 4.6 | 4.6
3 | ADEB | 5.8 | 5.8 | 5.8 | 5.8 | 5.8
4 | ADEBC | 6.10 | 6.10 | 6.10 | 6.10 | 6.10

Loop
9. Find w not in S such that D(w) is a minimum.
10. Add w to S.
11. Update D(v) for all v adjacent to w not in S.
12. If D(v) + c(w,v) < D(v) then
13. D(v) = D(w) + c(w,v); p(v) = w;
14. Until all nodes in S.

The Forwarding Table

- Running Dijkstra at node A gives the shortest path from A to all destinations.
- We then construct the forwarding table.

<table>
<thead>
<tr>
<th>Destination</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>(A,B)</td>
</tr>
<tr>
<td>C</td>
<td>(A,D)</td>
</tr>
<tr>
<td>D</td>
<td>(A,D)</td>
</tr>
<tr>
<td>E</td>
<td>(A,D)</td>
</tr>
<tr>
<td>F</td>
<td>(A,D)</td>
</tr>
</tbody>
</table>

Issue #1: Scalability

- How many messages needed to flood link state messages?
  - O(N x E), where N is #nodes; E is #edges in graph
- Processing complexity for Dijkstra’s algorithm?
  - O(N^2), because we check all nodes w not in S at each iteration and have O(N) iterations
  - more efficient implementations: O(N log(N))
- How many entries in the LS topology database? O(E)
- How many entries in the forwarding table? O(N)
Issue #2: Transient Disruptions

- Inconsistent link-state database
  - Some routers know about failure before others
  - The shortest paths are no longer consistent
- Can cause transient forwarding loops

![Diagram of network with inconsistent paths and loops]

Distance Vector

Learn-By-Doing

Let’s try to collectively develop distance-vector routing from first principles

Experiment

- Your job: find the (route to) the youngest person in the room
- Ground Rules
  - You may not leave your seat, nor shout loudly across the class
  - You may talk with your immediate neighbors (N-S-E-W only)
    (hint: “exchange updates” with them)
- At the end of 5 minutes, I will pick a victim and ask:
  - who is the youngest person in the room? (date & name)
  - which one of your neighbors first told you this info?

Go!
Distance Vector Routing

• Each router knows the links to its neighbors
  – Does not flood this information to the whole network
• Each router has provisional “shortest path” to every other router
  – E.g.: Router A: “I can get to router B with cost 11”
• Routers exchange this distance vector information with their neighboring routers
  – Vector because one entry per destination
• Iterative process converges to set of shortest paths

A few other inconvenient truths

• What if we use a non-additive metric?
  – E.g., maximal capacity
• What if routers don’t use the same metric?
  – I want low delay, you want low loss rate?
• What happens if nodes lie?

Can You Use Any Metric?

• I said that we can pick any metric. Really?
• What about maximizing capacity?

What Happens Here?

Problem: “cost” does not change around loop

Additive measures avoid this problem!

No agreement on metrics?

• If the nodes choose their paths according to different criteria, then bad things might happen
• Example
  – Node A is minimizing latency
  – Node B is minimizing loss rate
  – Node C is minimizing price
• Any of those goals are fine, if globally adopted
  – Only a problem when nodes use different criteria
• Consider a routing algorithm where paths are described by delay, cost, loss
**What Happens Here?**

Cares about price, then loss
Cares about delay, then price
Cares about loss, then delay

**Must agree on loop-avoiding metric**

- When all nodes minimize same metric
- And that metric increases around loops
- Then process is guaranteed to converge

**What happens when routers lie?**

- What if a router claims a 1-hop path to everywhere?
- All traffic from nearby routers gets sent there
- How can you tell if they are lying?
- Can this happen in real life?
  – It has, several times...

**Link State vs. Distance Vector**

- Core idea
  – LS: tell all nodes about your immediate neighbors
  – DV: tell your immediate neighbors about (your least cost distance to) all nodes

**Message complexity**

- LS: $O(N^2)$ messages;
  – $N$ is #nodes
- DV: $O(\text{#Iterations} \times E)$
  – where #Iterations is ideally $O(\text{network diameter})$ but varies due to routing loops or the count-to-infinity problem

**Processing complexity**

- LS: $O(N^2)$
- DV: $O(\text{#Iterations} \times N)$

**Link State vs. Distance Vector**

- LS: each node learns the complete network map; each node computes shortest paths independently and in parallel
- DV: no node has the complete picture; nodes cooperate to compute shortest paths in a distributed manner

→ LS has higher messaging overhead
→ LS has higher processing complexity
→ LS is less vulnerable to looping

**Robustness:** what happens if router malfunctions?

- LS:
  – node can advertise incorrect link cost
  – each node computes only its own table
- DV:
  – node can advertise incorrect path cost
  – each node’s table used by others; error propagates through network
Routing: Just the Beginning

• Link state and distance-vector are the deployed routing paradigms for intra-domain routing

• Inter-domain routing (BGP)
  — more Part II (Principles of Communications)
  — A version of DV

What are desirable goals for a routing solution?

• “Good” paths (least cost)
• Fast convergence after change/failures
  — no/rare loops
• Scalable
  — #messages
  — table size
  — processing complexity
• Secure
• Policy
• Rich metrics (more later)

Delivery models

• What if a node wants to send to more than one destination?
  — broadcast: send to all
  — multicast: send to all members of a group
  — anycast: send to any member of a group

• What if a node wants to send along more than one path?

Metrics

• Propagation delay
• Congestion
• Load balance
• Bandwidth (available, capacity, maximal, bw)
• Price
• Reliability
• Loss rate
• Combinations of the above

In practice, operators set abstract “weights” (much like our costs); how exactly is a bit of a black art

From Routing back to Forwarding

• Routing: “control plane”
  — Computing paths the packets will follow
  — Routers talking amongst themselves
  — Jointly creating the routing state

• Forwarding: “data plane”
  — Directing a data packet to an outgoing link
  — Individual router using routing state

• Two very different timescales....
Per-packet processing in an IP Router

1. Accept packet arriving on an incoming link.
2. Lookup packet destination address in the forwarding table, to identify outgoing port(s).
3. Manipulate packet header: e.g., decrement TTL, update header checksum.
4. Send packet to the outgoing port(s).
5. Buffer packet in the queue.
6. Transmit packet onto outgoing link.

Generic Router Architecture

Forwarding tables

Naive approach:
One entry per address

<table>
<thead>
<tr>
<th>Entry</th>
<th>Destination</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.0.0.0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0.0.0.1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>255.255.255.255</td>
<td>12</td>
</tr>
</tbody>
</table>

Improved approach:
Group entries to reduce table size

<table>
<thead>
<tr>
<th>Entry</th>
<th>Destination</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.0.0.0 – 127.255.255.255</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>128.0.0.0 – 128.255.255.255</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>192.0.0.0 – 192.255.255.255</td>
<td>12</td>
</tr>
</tbody>
</table>

IP addresses as a line

Longest Prefix Match (LPM)

<table>
<thead>
<tr>
<th>Entry</th>
<th>Destination</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cambridge</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Oxford</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Europe</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>USA</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>Everywhere (default)</td>
<td>5</td>
</tr>
</tbody>
</table>
Longest Prefix Match (LPM)

<table>
<thead>
<tr>
<th>Entry</th>
<th>Destination</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cambridge</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Oxford</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Europe</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>USA</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>Everywhere</td>
<td>5</td>
</tr>
</tbody>
</table>

Matching entries:
- Europe
- Everywhere

Universities
Continents
Planet

To: France
Data

Implementing Longest Prefix Match

<table>
<thead>
<tr>
<th>Entry</th>
<th>Destination</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cambridge</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Oxford</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Europe</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>USA</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>Everywhere</td>
<td>5</td>
</tr>
</tbody>
</table>

Most specific
Least specific

Router Architecture Overview

Two key router functions:
- run routing algorithms/protocol (RIP, OSPF, BGP)
- forwarding datagrams from incoming to outgoing link

Switching Via Memory

First generation routers:
- traditional computers with switching under direct control of CPU
- packet copied to system’s memory
- speed limited by memory bandwidth (2 bus crossings per datagram)
Switching Via a Bus

- datagram from input port memory to output port memory via a shared bus
- **bus contention**: switching speed limited by bus bandwidth
- Lots of ports?? speed up the bus no contention bus speed = 2 * port speed x port count
- 32 Gbps bus, Cisco 5600: sufficient speed for access routers

Switching Via An Interconnection Network

- overcome bus bandwidth limitations
- Banyan networks, other interconnection nets initially developed to connect processors in multiprocessor stages
- advanced design: fragmenting datagram into fixed length cells, switch cells through the fabric.
- Cisco CRS-1: switches 1.2 Tbps through the interconnection network

Output Ports

- **Buffering** required when datagrams arrive from fabric faster than the transmission rate
- **Scheduling discipline** chooses among queued datagrams for transmission  ➔ Who goes next?

Output port queueing

- buffering when arrival rate via switch exceeds output line speed
- **queuing (delay) and loss due to output port buffer overflow!**

Input Port Queuing

- Fabric slower than input ports combined -> queueing may occur at input queues
- Head-of-the-Line (HOL) blocking: queued datagram at front of queue prevents others in queue from moving forward
- **queueing delay and loss due to input buffer overflow!**

Buffers in Routers

- So how large should the buffers be?

Buffer size matters

- End-to-end delay
  - Transmission, propagation, and queueing delay
  - The only variable part is queueing delay
- Router architecture
  - Board space, power consumption, and cost
  - On chip buffers: higher density, higher cost
  - Optical buffers: all-optical routers

You are now touching the edge of the research zone…..
Rule-of-thumb – Intuition

- If an ACK is received: \( W \leftarrow W + 1/W \)
- If a packet is lost: \( W \leftarrow W/2 \)

Small Buffers – Intuition

- Synchronized Flows
  - Aggregate window has same dynamics
  - Therefore buffer occupancy has same dynamics
  - Rule-of-thumb still holds.

- Many TCP Flows
  - Independent, desynchronized
  - Central limit theorem says the aggregate becomes Gaussian
  - Variance (buffer size) decreases as \( N \) increases

IPv4 Packet Structure

- 20 Bytes of Standard Header, then Options
- 4-bit Version
- 4-bit Header Length
- 8-bit Type of Service (TOS)
- 16-bit Total Length (Bytes)
- 16-bit Identification
- 3-bit Flags
- 13-bit Fragment Offset
- 8-bit Time to Live (TTL)
- 8-bit Protocol
- 16-bit Header Checksum
- 32-bit Source IP Address
- 32-bit Destination IP Address
- Options (if any)
- Payload
(Packet) Network Tasks One-by-One

- Read packet correctly
- Get packet to the destination
- Get responses to the packet back to source
- Carry data
- Tell host what to do with packet once arrived
- Specify any special network handling of the packet
- Deal with problems that arise along the path

Reading Packet Correctly

- Version number (4 bits)
  - Indicates the version of the IP protocol
  - Necessary to know what other fields to expect
  - Typically “4” (for IPv4), and sometimes “6” (for IPv6)
- Header length (4 bits)
  - Number of 32-bit words in the header
  - Typically “5” (for a 20-byte IPv4 header)
  - Can be more when IP options are used
- Total length (16 bits)
  - Number of bytes in the packet
  - Maximum size is 65,535 bytes ($2^{16} - 1$)
  - Though underlying links may impose smaller limits

Getting Packet to Destination and Back

- Two IP addresses
  - Source IP address (32 bits)
  - Destination IP address (32 bits)
- Destination address
  - Unique identifier/locator for the receiving host
  - Allows each node to make forwarding decisions
- Source address
  - Unique identifier/locator for the sending host
  - Recipient can decide whether to accept packet
  - Enables recipient to send a reply back to source

Telling Host How to Handle Packet

- Protocol (8 bits)
  - Identifies the higher-level protocol
  - Important for demultiplexing at receiving host
- Most common examples
  - E.g., “6” for the Transmission Control Protocol (TCP)
  - E.g., “17” for the User Datagram Protocol (UDP)

Special Handling

- Type-of-Service (8 bits)
  - Allow packets to be treated differently based on needs
  - E.g., low delay for audio, high bandwidth for bulk transfer
  - Has been redefined several times
- Options

Potential Problems

- Header Corrupted: Checksum
- Loop: TTL
- Packet too large: Fragmentation
Pop quiz question: What happens when a fragment is lost?

- Checksum (16 bits)
  - Particular form of checksum over packet header
- If not correct, router discards packets
  - So it doesn’t act on bogus information
- Checksum recalculated at every router
  - Why?
  - Why include TTL?
  - Why only header?

Example

98

100

4000 byte datagram

MTU = 1500 bytes

1480 bytes in data field

102

Storage

IP Fragmentation & Reassembly

- network links have MTU (max transfer size) - largest possible link level frame.
- different link types, different MTUs
- large IP datagram divided ["fragmented"] within net
  - one datagram becomes several datagrams
  - "reassembled" only at final destination
- IP header bits used to identify, order related fragments
- IPv6 does things differently...

Fragmentation
(some assembly required)

- Fragmentation: when forwarding a packet, an Internet router can split it into multiple pieces ("fragments") if too big for next hop link
- Must reassemble to recover original packet
  - Need fragmentation information (32 bits)
  - Packet identifier, flags, and fragment offset

101

Preventing Loops
(aka Internet Zombie plan)

- Forwarding loops cause packets to cycle forever
  - As these accumulate, eventually consume all capacity
- Time-to-Live (TTL) Field (8 bits)
  - Decrementated at each hop, packet discarded if reaches 0
  - ...and “time exceeded” message is sent to the source
  - Using “ICMP” control message; basis for traceroute

103

IP Fragmentation and Reassembly

Example

One large datagram becomes several smaller datagrams

104

Fragmentation Details

- Identifier (16 bits): used to tell which fragments belong together
- Flags (3 bits):
  - Reserved (RF): unused bit
  - Don’t Fragment (DF); instruct routers to not fragment the packet even if it won’t fit
  - Instead, they drop the packet and send back a “Too Large” ICMP control message
  - Forms the basis for “Path MTU Discovery”
- More (MF): this fragment is not the last one
- Offset (13 bits): what part of datagram this fragment covers in 8-byte units

Pop quiz question: What happens when a fragment is lost?

Pop quiz question: Why do frags use offset and not a frag number?
Options

- End of Options List
- No Operation (padding between options)
- Record Route
- Strict Source Route
- Loose Source Route
- Timestamp
- Tracert
- Router Alert
- ...

IP Addressing: introduction

- IP address: 32-bit identifier for host, router interface
- Interface: connection between host/router and physical link
  - router’s typically have multiple interfaces
  - host typically has one interface
- IP addresses associated with each interface

Subnets

- IP address:
  - subnet part (high order bits)
  - host part (low order bits)
- What’s a subnet?
  - device interfaces with same subnet part of IP address
  - can physically reach each other without intervening router

DHCP client-server scenario

Goal: allow host to dynamically obtain its IP address from network server when it joins network
Can renew its lease on address in use
Allows reuse of addresses (only hold address while connected an "on")
Support for mobile users who want to join network (more shortly)

IP addresses: how to get one?

Q: How does a host get its IP address?

A: hard-coded by system admin in a file
  - Windows: control-panel > network > configuration > tcp/ip > properties
  - UNIX: /etc/rc.config (circa 1980's your mileage will vary)
  - DHCP: Dynamic Host Configuration Protocol: dynamically get address from as server
    - "plug-and-play"

DHCP ACK: sent to client when address is allocated from server
DHCP Offer: sent to client when address is allocated from server
DHCP packet
  - Source 1: 0.0.0.0
  - Source 2: 255.255.255.255, 67
  - Destination: 68

ISP’s block

Organization 0: 11001000 00010111 00010000 00000000
Organization 1: 11010000 0010111 00100000 00000000
Organization 2: 11010000 0011011 0010100 00000000
Organization 3: 11010000 00110111 0010100 00000000
Organization 4: 11010000 00110111 0010100 00000000

DHCP ACK: sent to client when address is allocated from server
DHCP Offer: sent to client when address is allocated from server
DHCP packet
  - Source 1: 0.0.0.0
  - Source 2: 255.255.255.255, 67
  - Destination: 68

IP addresses: how to get one?

Q: How does network get subnet part of IP address?
A: gets allocated portion of its provider ISP’s address space
Hierarchical addressing: route aggregation

Hierarchical addressing allows efficient advertisement of routing information:

Organization 0
- 200.23.16.0/23
- 200.23.18.0/23
- 200.23.20.0/23
- 200.23.30.0/23

ISP-R-Us

Fly-By-Night-ISP

Send me anything with addresses beginning 200.23.16.0/20

Send me anything with addresses beginning 200.23.18.0/23

Send me anything with addresses beginning 199.31.0.0/23

Internet

Hierarchical addressing: more specific routes

ISPs-R-Us has a more specific route to Organization 1

Organization 0
- 200.23.15.0/23

Organization 2
- 200.23.19.0/23

Organization 7
- 200.23.18.0/23

ISP-R-Us

Fly-By-Night-ISP

Send me anything with addresses beginning 200.23.16.0/20

Send me anything with addresses beginning 199.31.0.0/23

Internet

IP addressing: the last word...

Q: How does an ISP get a block of addresses?
A: ICANN: Internet Corporation for Assigned Names and Numbers
- allocates addresses
- manages DNS
- assigns domain names, resolves disputes

NAT: Network Address Translation

Implementation: NAT router must:
- outgoing datagrams: replace (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #)
  - remote clients/servers will respond using (NAT IP address, new port #) as destination address
- remember (in NAT translation table) every (source IP address, port #) to (NAT IP address, new port #) translation pair
- incoming datagrams: replace (NAT IP address, new port #) in dest fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table

NAT: Network Address Translation

Motivation: local network uses just one IP address as far as outside world is concerned:
- range of addresses not needed from ISP: just one IP address for all devices
- can change addresses of devices in local network without notifying outside world
- can change ISP without changing addresses of devices in local network
- devices inside local net not explicitly addressable, visible by outside world (a security plus).
NAT: Network Address Translation

1. client wants to connect to server with address 10.0.0.1
   - server address 10.0.0.1 local to LAN (client can’t use it as destination addr)
   - only one externally visible NATed address: 138.76.29.7

2. solution: statically configure NAT to forward incoming connection requests at given port to server
   - e.g., (138.76.29.7, port 2500) always forwarded to 10.0.0.1 port 25000

NAT traversal problem

- solution 2: Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol. Allows NATed host to:
  - learn public IP address
  - add/remove port mappings (with lease times)

  i.e., automate static NAT port map configuration

NAT traversal problem

- solution 3: relaying (used in Skype)
  - NATed client establishes connection to relay
  - external client connects to relay
  - relay bridges packets between to connections

NAT traversal problem

• NAT is controversial:
  - routers should only process up to layer 3
  - violates end-to-end argument (?)
  - NAT possibility must be taken into account by app designers, e.g., P2P applications
  - address shortage should instead be solved by IPv6

NAT traversal problem

1. 16-bit port-number field:
   - 60,000 simultaneous connections with a single LAN-side address!

2. NAT is controversial:
   - routers should only process up to layer 3
   - violates end-to-end argument (?)
   - NAT possibility must be taken into account by app designers, e.g., P2P applications
   - address shortage should instead be solved by IPv6

Remember this? Traceroute at work...

traceroute: rio.cl.cam.ac.uk to munnari.oz.au
[tracepath on p.1 similar]
Traceroute and ICMP

- Source sends series of UDP segments to dest
  - First has TTL=1
  - Second has TTL=2, etc.
  - Unlikely port number
- When nth datagram arrives to nth router:
  - Router discards datagram
  - And sends to source an ICMP message (type 11, code 0)
  - Message includes name of router & IP address
- When ICMP message arrives, source calculates RTT
- Traceroute does this 3 times
  - Stopping criterion
- UDP segment eventually arrives at destination host
- Destination returns ICMP "host unreachable" packet (type 3, code 3)
- When source gets this ICMP, stops.

ICMP: Internet Control Message Protocol

- used by hosts & routers to communicate network-level information
  - error reporting: unreachable host, network, port, protocol
  - echo request/reply (used by ping)
  - network-layer "above" IP:
    - ICMP msgs carried in IP datagrams
  - ICMP message: type, code plus first 8 bytes of IP datagram causing error

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>echo reply (ping)</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>dest, network unreachable</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>dest protocol unreachable</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>dest port unreachable</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>dest network unknown</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>source quench (congestion control - not used)</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>echo request (ping)</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>route advertisement</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>router discovery</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>TTL expired</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>bad IP header</td>
</tr>
</tbody>
</table>

Gluing it together:
How does my Network (address) interact with my Data-Link (address)?

Switches vs. Routers Summary

- both store-and-forward devices
  - routers: network layer devices (examine network layer headers)
  - switches are link layer devices
- routers maintain routing tables, implement routing algorithms
- switches maintain switch tables, implement filtering, learning algorithms

MAC Addresses (and IPv4 ARP) or How do I glue my network to my data-link?

- 32-bit IP address:
  - network-layer address
  - used to get datagram to destination IP subnet
- MAC (or LAN or physical or Ethernet) address:
  - function: get frame from one interface to another physically-connected interface (same network)
  - 48 bit MAC address (for most LANs)
    - burned in NIC ROM, also (commonly) software settable

LAN Addresses and ARP

Each adapter on LAN has unique LAN address
Address Resolution Protocol

- Every node maintains an ARP table
  - <IP address, MAC address> pair
- Consult the table when sending a packet
  - Map destination IP address to destination MAC address
  - Encapsulate and transmit the data packet
- But: what if IP address not in the table?
  - Sender broadcasts: "Who has IP address 1.2.3.156?"
  - Receiver responds: "MAC address 58-23-D7-FA-20-B0"
  - Sender caches result in its ARP table

Example: A Sending a Packet to B

How does host A send an IP packet to host B?

1. A sends packet to R.
2. R sends packet to B.

Host A Decides to Send Through R

- Host A constructs an IP packet to send to B
  - Source 111.111.111.111, destination 222.222.222.222
- Host A has a gateway router R
  - Used to reach destinations outside of 111.111.111.0/24
  - Address 111.111.111.110 for R learned via DHCP/config

R Decides how to Forward Packet

- Router R's adaptor receives the packet
  - R extracts the IP packet from the Ethernet frame
  - R sees the IP packet is destined to 222.222.222.222
- Router R consults its forwarding table
  - Packet matches 222.222.222.0/24 via other adaptor
Key Ideas in Both ARP and DHCP

- **Broadcasting**: Can use broadcast to make contact
  - Scalable because of limited size
- **Caching**: remember the past for a while
  - Store the information you learn to reduce overhead
  - Remember your own address & other host's addresses
- **Soft state**: eventually forget the past
  - Associate a time-to-live field with the information
  - ... and either refresh or discard the information
  - Key for robustness in the face of unpredictable change

Why Not Use DNS-Like Tables?

- When host arrives:
  - Assign it an IP address that will last as long it is present
  - Add an entry into a table in DNS-server that maps MAC to IP addresses
- Answer:
  - Names: explicit creation, and are plentiful
  - Hosts: come and go without informing network
    - Must do mapping on demand
    - Addresses: not plentiful, need to reuse and remap
    - Soft-state enables dynamic reuse

No More IPv4 Addresses

- IPv4 address space in terms of /8's
No More IPv4 Addresses

- 20 /8’s on April 10, 2010

- 13 /8’s on May 8, 2010

IPv6

- Motivated (prematurely) by address exhaustion
  – Address field *four* times as long

- Steve Deering focused on simplifying IP
  – Got rid of all fields that were not absolutely necessary
  – “Spring Cleaning” for IP

- Result is an elegant, if unambitious, protocol

Larger Address Space

- IPv4 = 4,294,967,295 addresses
- IPv6 = 340,282,366,920,938,463,374,607,432,768,211,456 addresses
- 4x in number of bits translates to huge increase in address space!
Other Significant Protocol Changes

- Increased minimum MTU from 576 to 1280
- No enroute fragmentation... fragmentation only at source
- Header changes
  - Replace broadcast with multicast

### IPv4

<table>
<thead>
<tr>
<th>Field</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Address</td>
<td>Identification</td>
</tr>
<tr>
<td>Destination</td>
<td>Options</td>
<td>Fragment Offset</td>
</tr>
</tbody>
</table>

Legend:
- Exists in IPv4
- Exists not kept in IPv6
- Name and position changed in IPv6
- New field in IPv6

### IPv6

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Source Address</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Destination Address</td>
</tr>
</tbody>
</table>

IPv6 Address Notation

- RFC 5952
- 128-bit IPv6 addresses are represented in:
  - Eight 16-bit segments
  - Hexadecimal (non-case sensitive) between 0000 and FFFF
  - Separated by colons
- Example:
  - 3ffe:1944:0100:0000:0000:1000:0123:0000
- Two rules for dealing with 0’s
  - One Hex digit = 4 bits

0’s Rule 1 – Leading 0’s

- The leading zeroes in any 16-bit segment do not have to be written.
- Example
  - 3ffe:1944:0100:0000:0000:0123:0000:0000
  - 3ffe:1944:0100:0000:0000:1000:0123:0000

Legend:
- IPv4
- IPv6

Roundup: Why IPv6?

- Larger address space
- Auto-configuration
- Cleanup
- Eliminate fragmentation
- Eliminate checksum
- Pseudo-header (w/o Hop Limit) covered by transport layer
- Flow label
- Increase minimum MTU from 576 to 1280
- Replace broadcasts with multicast

No Checksum!

- Provided by transport layer, if needed
- Ala TCP, includes pseudo-header
- Pseudo-header doesn’t include Hop Limit
  - No per-hop re-computation!
  - Allows end-to-end implementation (transport layer)
- UDP checksum required (wasn’t in IPv4) rfc6936: No more zero
- Pseudo-header added to ICMPv6 checksum
O’s Rule 1 – Leading 0’s

- Can only apply to leading zeros... otherwise ambiguous results

- Example
  -  3ffe : 1944 : 100 : a : 0 : bc : 2500 : d0b

- Could be either
  -  3ffe : 1944 : 0100 : 000a : 0000 : 00bc : 2500 : d0b
  -  3ffe : 1944 : 1000 : a000 : 0000 : bc00 : 2500 : d0b
  - Which is correct?

O’s Rule 2 – Double Colon

- Any single, contiguous string of 16-bit segments consisting of all zeroes can be represented with a double colon.

  ff02 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0005

  ff02 : 0 : 0 : 0 : 0 : 0 : 0 : 5

  ff02 : : 5

O’s Rule 2 – Double Colon

- Only a single contiguous string of all-zero segments can be represented with a double colon.

- Example:
  -  2001 : d02 : 0000 : 0000 : 0014 : 0000 : 0000 : 0095

- Both of these are correct
  -  2001 : d02 :: 14 : 0 : 0 : 95
  - OR
  -  2001 : d02 : 0 : 0 : 14 :: 95

Network Prefixes

- In IPv4, network portion of address can by identified by either
  - Netmask: 255.255.255.0
  - Bitcount: /24

- Only use bitcount with IPv6

  3ffe:1944:100:a::/64
Special IPv6 Addresses

- Default route: \texttt{::/0}
- Unspecified Address: \texttt{::/128}
  - Used in SLAAC (coming later)
- Loopback/Local Host: \texttt{::1/128}
  - No longer a /8 of addresses but a single address

Types of IPv6 Addresses

- RFC 4291—“IPv6 Addressing Architecture”
- Global Unicast
  - Globally routable IPv6 addresses
- Link Local Unicast
  - Addresses for use on a given subnet
- Unique Local Unicast
  - Globally unique address for local communication
- Multicast
- Anycast
  - A unicast address assigned to interfaces belonging to different nodes

Global Unicast Addresses

- Globally routable addresses
  - RFC 3587
    - 3 parts
      - 48 bit global routing prefix
        - Hierarchically-structured value assigned to a site
      - Further broken down into Registry, ISP Prefix, and Site Prefix fields
      - 16 bit Subnet ID
        - Identifier of a subnet within a site
      - 64(!) bit Interface ID
        - Identify an interface on a subnet
        - Motivated by expected use of MAC addresses (IEEE EUI-64 identifiers) in SLAAC...
        - Except GLAs that start with '000... binary
      - Used for, e.g., “IPv4-Mapped IPv6 Addresses” (RFC 4082)

Subnetting Global Unicast Addresses

- Each site can identify \(2^{31} (65,535)\) subnets
  - 2340:1111:AAAA1:1111/64
  - 2340:1111:AAAA2:1111/64
  - 2340:1111:AAAA3:1111/64
  - 2340:1111:AAAA4:1111/64
  - ...
- Subnet has address space of \(2^{31}... an IAS of IASs!
- Can extend the subnet ID into the interface ID portion of the address...
  - Sacrifice ability to use EUI-64 style of SLAAC...
  - Maybe not a bad thing... more later
These are huge numbers!!

- Assume average /16's allocated to ISPs and /22's allocated to sites in IPv4
- And this keeps assumption of /64 subnets!

### IPv6 Address Space

<table>
<thead>
<tr>
<th>Description</th>
<th>Range</th>
<th>Count</th>
<th>Scale vs IPv4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total # ISPs</td>
<td>/3 - /12</td>
<td>2^5 = 512M</td>
<td>9,382</td>
</tr>
<tr>
<td>Total # Sites</td>
<td>/3 - /48</td>
<td>2^4 = 4T</td>
<td>1.2M</td>
</tr>
<tr>
<td>Sites/ISP</td>
<td>/48 - /64</td>
<td>2^2 = 64K</td>
<td>1,024</td>
</tr>
</tbody>
</table>

### Problem with /64 Subnets

- Scanning a subnet becomes a DoS attack!
  - Creates IPv6 version of 2^64 ARP entries in routers
  - Exhaust address-translation table space
  
  **So now we have:**
  
  - `ping6 ff02::1` All nodes in broadcast domain
  - `ping6 ff02::2` All routers in broadcast domain

### Types of IPv6 Addresses

- **Unallocated** ("Reserved by IETF")
  - /7's: FF00::/8
  - /8's: 8000::/6
  - /9's: FE00::/4
  - /10's: F800::/2
  - /11's: FF00::
  - /12's: F800::

  *Accounts for a bit more than 2^{125} of the address space.*

- **Global Unicast**
  - FE80::/64
  - FF00::/8

  *Accounts for a bit more than 2^{127}, or more than half, of the address space!!

- **Link Local Unicast**
  - FE80::/64

- **Unique Local Unicast**
  - FE80::/64

- **Multicast**
- **Anycast**

<table>
<thead>
<tr>
<th>Global Unicast</th>
<th>FE80::/64</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Local Unicast</td>
<td>FE80::/64</td>
</tr>
<tr>
<td>Unique Local Unicast</td>
<td>FE80::/64</td>
</tr>
<tr>
<td>Multicast</td>
<td>FE80::/64</td>
</tr>
<tr>
<td>Anycast</td>
<td>FE80::/64</td>
</tr>
</tbody>
</table>

### Types of IPv6 Addresses

- **RFC 4291**:
  - "IPv6 Addressing Architecture"

- **Global Unicast**
  - Globally routable IPv6 addresses

- **Link Local Unicast**
  - Addresses for use on a given site

- **Unique Local Unicast**
  - Globally unique address for local communication

- **Multicast**

- **Anycast**
  - A unicast address assigned to interfaces belonging to different nodes

### Link-Local Addresses

- **11111110 10.../binary (FE80::/64)**
  - According to RFC 4291 bits 11-64 should be 0s... so really FE80::/64?

  **For use on a single link:**
  - Automatic address configuration
  - Neighbor discovery (IPv6 ARP)
  - When no routers are present
  - Routers must not forward

  **Addresses “chicken-or-egg” problem... need an address to get an address.**

  **Address assignment done unilaterally by node (later)**

  **IPv4 has link-local address (169.254/16, RFC 3927)**
  - Only used if no globally routable addresses available

- **Networks**
  - 128/14

- **Router-Link Interfaces**
  - 128/13

- **Link-Local Addresses**
  - FE80::/64

- **Neighbor Discovery**
  - For addressing links using RFC 4861

- **Static Routing**
  - Used for IPv6 networks

- **Wireless**
  - Used for IPv6 networks

- **IPv6 Address**
  - FE80::/64

- **Neighbor Discovery**
  - For addressing links using RFC 4861
Types of IPv6 Addresses

- RFC 4291 – "IPv6 Addressing Architecture"
- Global Unicast
  - Globally routable IPv6 addresses
- Link Local Unicast
  - Addresses for use on a given subnet
- Unique Local Unicast
  - Globally unique address for local communication
- Multicast
- Anycast
  - A unicast address assigned to interfaces belonging to different nodes

Unique Local Addresses

- 4 parts
  - "L" bit always 1
  - Global ID (40 bits) randomly generated to enforce the idea that these addresses are not to be globally routed or aggregated
  - Subnet ID (16 bits) same as globally Unique Subnet ID
  - Interface ID (64 bits) same as globally Unique Interface ID

Multicast Addresses

- '11111111...' binary (FF00::/8)
- Equivalent to IPv4 multicast (224.0.0.0/8)
- 3 parts
  - Flag (4 bits)
  - Scope (4 bits)

Reserved Multicast Addresses

- All nodes
  - FF01::1 – interface-local; used for loopback multicast transmissions
  - FF02::1 – link-local; replaces IPv4 broadcast address (all 1's host)
- All routers
  - FF02:: (interface-local), FF02:: (link-local)
- Solicited-Node multicast
  - Used in Neighbor Discovery Protocol (later)
  - FF02::FF00:0/104 [FF02::FF00:::]
  - Construct by replacing ‘XX:XXXX’ above with low-order 24 bits of a node's unicast or anycast address
  - Example
    - For unicast address 4017:0:11:0:0:0:0:0
    - Solicited-Node multicast is FF02::FF1E:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0
**Types of IPv6 Addresses**

- RFC 4291 – “IPv6 Addressing Architecture”
- **Global Unicast**
  - Globally routable IPv6 addresses
- **Link Local Unicast**
  - Addresses for use on a given subnet
- **Unique Local Unicast**
  - Globally unique address for local communication
- **Multicast**
  - **Anycast**
    - A unicast address assigned to interfaces belonging to different nodes

**Anycast Addresses**

- Allocated from unicast address space
  - Syntactically indistinguishable from unicast addresses
- An address assigned to more than one node
- Anycast traffic routed to the “nearest” host with the anycast address
- Typically used for a service (e.g. local DNS servers)
- Nodes must be configured to know an address is anycast
  - Don’t do Duplicate Address Detection
  - Advertise a route?

**A Node’s Required Addresses**

- Link-local address for each interface
- Configured unicast or anycast addresses
- Loopback address
- All-Nodes multicast interface and link addresses
- Solicited-Node multicast for each configured unicast and anycast address
- Multicast addresses for all groups the node is a member of
- Routers must add
  - Subnet-Router anycast address for each interface
  - Subnet prefix with all 0’s host part
  - All-Routers multicast address

**Roundup: IPv6 Addresses**

- “Interface ID” (host part) is 64 bits
- New addresses required by all nodes (host or router)
  - Link-local address
  - All-nodes interface-local and link-local multicast
  - Solicited-node multicast for each unicast/anycast address
- New addresses required by routers
  - All-routers interface-local, link-local and site-local multicast
  - Subnet-Router anycast for each interface?

**Assigning Address to Interfaces**

- Static (manual) assignment
  - Needed for network equipment
- DHCPv6
  - Needed to track who uses an IP address
- StateLess Address AutoConfiguration (SLAAC)
  - New to IPv6
- Describe SLAAC in the following...
SLAAC

- RFC 4862 – IPv6 Stateful Address Autoconfiguration
- Used to assign unicast addresses to interfaces
  - Link-Local Unicast
  - Global Unicast
  - Unique-Local Unicast?
- Goal is to minimize manual configuration
  - No manual configuration of hosts
  - Limited router configuration
  - No additional servers
- Use when "not particularly concerned with the exact addresses hosts use"
  - Otherwise use DHCPv6 [RFC 3315]

SLAAC Building Blocks

- Interface IDs
- Neighbor Discovery Protocol
- SLAAC Process

SLAAC Building Blocks

- Interface IDs
- Neighbor Discovery Protocol
- SLAAC Process

IEEE EUI-64 Option for Interface ID

- Use interface MAC address
- Insert FFFE to convert EUI-48 to EUI-64
- Flip Universal/Local bit to “1”
  - Section 2.5.1 RFC 4291

Privacy Option for Interface ID

- Using MAC uniquely identifies a host... security/privacy concerns!
- Microsoft defined an alternative solution for Interface IDs [RFC 4941]
- Hosts generates a random 64 bit Interface ID
SLAAC Building Blocks

- Interface IDs
- Neighbor Discovery Protocol
- SLAAC Process

NDP

- RFC 4861 – Neighbor Discovery for IPv6
- Used to
  - Determine MAC address for nodes on same subnet (ARP)
  - Find routers on same subnet
  - Determine subnet prefix and MTU
  - Determine address of local DNS server (RFC 6106)
- Uses 5 ICMPv6 messages
  - Router Solicitation (RS) – request routers to send RA
  - Router Advertisement (RA) – router’s address and subnet parameters
  - Neighbor Solicitation (NS) – request neighbor’s MAC address (ARP Request)
  - Neighbor Advertisement (NA) – MAC address for an IPv6 address (ARP Reply)
  - Redirect – inform host of a better next hop for a destination

NDP RS & RA

- Router Solicitation (RS)
  - Originated by hosts to request that a router send an RA
  - Source = unspecified (::) or link-local address,
  - Destination = All-routers multicast (FF02::2)
- Router Advertisement (RA)
  - Originated by routers to advertise their address and link-specific parameters
  - Sent periodically and in response to Router Solicitation messages
  - Source = link-local address,
  - Destination = All-routers multicast (FF02:1)

NDP NS & NA

- Neighbor Solicitation (NS)
  - Request target MAC address while providing target of source (IPv4 ARP Request)
  - Used to resolve address or verify reachability of neighbor
  - Source = unspecified or "::" (Duplicate Address Detection… next slide)
  - Destination = solicited-node multicast
- Neighbor Advertisement (NA)
  - Advertise MAC address for given IPv6 address (IPv4 ARP Reply)
  - Respond to NS or communicate MAC address change
  - Source = unspecified, destination = NS’s source or all nodes multicast (if source "::")

Duplicate Address Detection

- Duplicate Address Detection (DAD) used to verify address is unique in subnet prior to assigning it to an interface
- MUST take place on all unicast addresses, regardless of whether they are obtained through stateful, stateless or manual configuration
- MUST NOT be performed on anycast addresses
- Uses Neighbor Solicitation and Neighbor Advertisement messages
- NS sent to solicited-node multicast; if no NA received address is unique
- Solicited-node multicast: FF02::1:FF00:1/104 w/ last 24 bits of target
SLAAC Building Blocks

- Interface IDs
- Neighbor Discovery Protocol
- SLAAC Process

SLAAC Steps

- Select link-local address
- Verify "tentative" address not in use by another host with DAD
- Send RS to solicit RAs from routers
- Receive RA with
  - router address,
  - subnet MTU,
  - subnet prefix,
  - local DNS server (RFC 6106)
- Generate global unicast address
- Verify address is not in use by another host with DAD

Prefix Leases

- Prefix information contained in RA includes lifetime information
  - Preferred lifetime: when an address’s preferred lifetime expires SHOULD only be used for existing communications
  - Valid lifetime: when an address’s valid lifetime expires it MUST NOT be used as a source address or accepted as a destination address.
- Unsolicited RAs can reduce prefix lifetime values
  - Can be used to force re-addressing

Roundup: ICMPv6

- Implements router discovery and ARP functions
- ICMPv6 messages
  - Router Solicitation/Router Advertisement
  - Neighbor Solicitation/Neighbor Advertisement
  - (Next hop) Redirect
- Duplicate Address Detection (DAD)
  - verify unique link-local and global-unicast addresses
  - Uses:
    - NS/NA (i.e. gratuitous ARP)
    - Solicited node multicast address

Review - SLAAC

- Assigns link-local and global-unicast addresses
- Goals
  - Eliminate manual configuration
  - Require minimal router configuration
  - Require no additional servers
- Host part options
  - EUI-64
  - Random ("privacy") addresses
- Steps
  - Generate link-local address and verify with DAD
  - Find router - RS/RA
  - Generate global unicast address and verify with DAD
Improving on IPv4 and IPv6?

- Why include unverifiable source address?
  - Would like accountability and anonymity (now neither)
  - Return address can be communicated at higher layer
- Why packet header used at edge same as core?
  - Edge: host tells network what service it wants
  - Core: packet tells switch how to handle it
  - One is local to host, one is global to network
- Some kind of payment/responsibility field?
  - Who is responsible for paying for packet delivery?
  - Source, destination, other?
- Other ideas?

Summary Network Layer

- understand principles behind network layer services:
  - network layer service models
  - forwarding versus routing (versus switching)
  - how a router works
  - routing (path selection)
  - IPv6
- Algorithms
  - Two routing approaches (LS vs DV)
  - One of these in detail (LS)
  - ARP
Our goals:
• understand principles behind transport layer services:
  – multiplexing/demultiplexing
  – reliable data transfer
  – flow control
  – congestion control
• learn about transport layer protocols in the Internet:
  – UDP: connectionless transport
  – TCP: connection-oriented transport
  – TCP congestion control

Why a transport layer?
• IP packets are addressed to a host but end-to-end communication is between application processes at hosts
  – Need a way to decide which packets go to which applications (more multiplexing)
Why a transport layer?

• IP packets are addressed to a host but end-to-end communication is between application processes at hosts
  — Need a way to decide which packets go to which applications (mux/demux)
• IP provides a weak service model (best-effort)
  — Packets can be corrupted, delayed, dropped, reordered, duplicated
  — No guidance on how much traffic to send and when
  — Dealing with this is tedious for application developers

Role of the Transport Layer

• Communication between application processes
  — Multiplexing between application processes
  — Implemented using ports

Role of the Transport Layer

• Communication between processes
• Provide common end-to-end services for app layer [optional]
  — Reliable, in-order data delivery
  — Paced data delivery: flow and congestion-control
    • too fast may overwhelm the network
    • too slow is not efficient
• TCP and UDP are the common transport protocols
  — also SCTP, MTCP, SST, RDP, DCCP, ...

Role of the Transport Layer

• Communication between processes
• Provide common end-to-end services for app layer [optional]
• TCP and UDP are the common transport protocols
• UDP is a minimalist, no-frills transport protocol
  — only provides mux/demux capabilities
• TCP is the totus porcus protocol
  — offers apps a reliable, in-order, byte-stream abstraction
  — with congestion control
  — but no performance (delay, bandwidth, ...) guarantees
Role of the Transport Layer

• Communication between processes
  – mux/demux from and to application processes
  – implemented using ports

Context: Applications and Sockets

• Socket: software abstraction by which an application process exchanges network messages with the (transport layer in the) operating system
  – socketID = socket(..., socket.TYPE)
  – socketID.sendto(message, ...)
  – socketID.recvfrom(....)

• Two important types of sockets
  – UDP socket: TYPE is SOCK_DGRAM
  – TCP socket: TYPE is SOCK_STREAM

Ports

• Problem: deciding which app (socket) gets which packets
  – Solution: port as a transport layer identifier
    – 16 bit identifier
      – OS stores mapping between sockets and ports
        – a packet carries a source and destination port number in its transport layer header
  
• For UDP ports (SOCK_DGRAM)
  – OS stores (local port, local IP address) ↔ socket

• For TCP ports (SOCK_STREAM)
  – OS stores (local port, local IP, remote port, remote IP) ↔ socket

4 5 8-bit Type of Service (TOS) 16-bit Total Length (Bytes)
16-bit Identification 3-bit Flags 13-bit Fragment Offset
8-bit Time to Live (TTL) 8-bit Protocol 16-bit Header Checksum
32-bit Source IP Address
32-bit Destination IP Address

IP Payload

TCP or UDP header and Payload

32-bit Source IP Address
32-bit Destination IP Address

4 5 8-bit Type of Service (TOS) 16-bit Total Length (Bytes)
16-bit Identification 3-bit Flags 13-bit Fragment Offset
8-bit Time to Live (TTL) 8 = TCP 17 = UDP 16-bit Header Checksum
32-bit Source IP Address
32-bit Destination IP Address

IP Payload
Recap: Multiplexing and Demultiplexing

- Host receives IP packets
  - Each IP packet has source and destination IP address
  - Each Transport Layer header has source and destination port number

- Host uses IP addresses and port numbers to direct the message to appropriate socket

More on Ports

- Separate 16-bit port address space for UDP and TCP
- “Well known” ports (0-1023): everyone agrees which services run on these ports
  - e.g., ssh:22, http:80
  - helps client know server’s port
- Ephemeral ports (most 1024-65535): dynamically selected as the source port for a client process

UDP: User Datagram Protocol

- Lightweight communication between processes
  - Avoid overhead and delays of ordered, reliable delivery
- UDP described in RFC 768 – (1980)
  - Destination IP address and port to support demultiplexing
  - Optional error checking on the packet contents
    - (checksum field of 0 means “don’t verify checksum”)

Why a transport layer?

- IP packets are addressed to a host but end-to-end communication is between application processes at hosts
  - Need a way to decide which packets go to which applications (mux/demux)
- IP provides a weak service model (best-effort)
  - Packets can be corrupted, delayed, dropped, reordered, duplicated

Principles of Reliable data transfer

- Important in app., transport, link layers
- Top 10 list of important networking topics!
  - In a perfect world, reliable transport is easy
    - But the Internet default is best-effort
  - All the bad things best-effort can do
    - A packet is corrupted (bit errors)
    - A packet is lost
    - A packet is delayed (why?)
    - Packets are reordered (why?)
    - A packet is duplicated (why?)
Principles of Reliable data transfer

- important in app., transport, link layers
- top-10 list of important networking topics!
- characteristics of unreliable channel will determine complexity of reliable data transfer protocol (rdt)

Reliable data transfer: getting started

We’ll:
- incrementally develop sender, receiver sides of reliable data transfer protocol (rdt)
- consider only unidirectional data transfer
  - but control info will flow on both directions!
- use finite state machines (FSM) to specify sender, receiver

KR state machines – a note.

Beware
Kurose and Ross has a confusing/confused attitude to state-machines.
i’ve attempted to normalise the representation.
UPSHOT: these slides have differing information to the KR book (from which the RDT example is taken.)
in KR “actions taken” appear wide-ranging, my interpretation is more specific/relevant.

Rdt1.0: reliable transfer over a reliable channel

- underlying channel perfectly reliable
  - no bit errors
  - no loss of packets
- separate FSMs for sender, receiver:
  - sender sends data into underlying channel
  - receiver read data from underlying channel
Rdt2.0: channel with bit errors

- underlying channel may flip bits in packet
  - checksum to detect bit errors
- the question: how to recover from errors:
  - acknowledgements (ACKs): receiver explicitly tells sender that packet received is OK
  - negative acknowledgements (NAKs): receiver explicitly tells sender that packet had errors
  - sender retransmits packet on receipt of NAK
- new mechanisms in rdt2.0 (beyond rdt1.0):
  - error detection
  - receiver feedback: control msgs (ACK, NAK) receiver -> sender

Dealing with Packet Corruption

Sender | Time | Receiver
--- | --- | ---
1 | ack | 2
2 | nack | 0

rdt2.0: FSM specification

sender

receiver

Note: the sender holds a copy of the packet being sent until the delivery is acknowledged.

rdt2.0: operation with no errors

rdt2.0: error scenario

rdt2.0 has a fatal flaw!

What happens if ACK/NAK corrupted?
- sender doesn’t know what happened at receiver!
- can’t just retransmit: possible duplicate

Handling duplicates:
- sender retransmits current packet if ACK/NAK garbled
- sender adds sequence number to each packet
- receiver discards (doesn’t deliver) duplicate packet

stop and wait
Sender sends one packet, then waits for receiver response
Dealing with Packet Corruption

Data and ACK packets carry sequence numbers

<table>
<thead>
<tr>
<th>Time</th>
<th>Sender</th>
<th>Receiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

What if the ACK/NACK is corrupted?
Packet #1 or #2?

**rdt2.1:** sender, handles garbled ACK/NAKs

**Sender:**
- seq # added to pkt
- two seq. #’s (0, 1) will suffice. Why?
- must check if received ACK/NAK corrupted
- twice as many states
  - state must “remember” whether “current” pkt has a 0 or 1 sequence number

**Receiver:**
- must check if received packet is duplicate
  - state indicates whether 0 or 1 is expected pkt seq #
- note: receiver can not know if its last ACK/NAK received OK at sender

**rdt2.2:** a NAK-free protocol

- same functionality as rdt2.1, using ACKs only
- instead of NAK, receiver sends ACK for last pkt received OK
  - receiver must explicitly include seq # of pkt being ACKed
- duplicate ACK at sender results in same action as NAK: retransmit current pkt

**rdt2.2:** sender, receiver fragments

**Sender FSM fragment**

**Receiver FSM fragment**
**rdt3.0: channels with errors and loss**

New assumption: underlying channel can also lose packets (data or ACKs)
- checksum, seq #, ACKs, retransmissions will be of help, but not enough

Approach: sender waits “reasonable” amount of time for ACK
- retransmits if no ACK received in this time
- if pkt (or ACK) just delayed (not lost):
  - retransmission will be duplicate, but use of seq #’s already handles this
  - receiver must specify seq # of pkt being ACKed
- requires countdown timer

Dealing with Packet Loss

Timer-driven loss detection
Set timer when packet is sent - retransmit on timeout

Dealing with Packet Loss

Timeout

- P(1)
- P(2)
- P(3)
- P(4)
- P(5)

Dealing with Packet Loss

Timeout

- P(1)
- P(2)
- P(3)
- P(4)
- P(5)

**Performance of rdt3.0**

- rdt3.0 works, but performance stinks
- ex: 1 Gbps link, 15 ms prop. delay, 8000 bit packet:
  \[ d_{\text{prop}} = \frac{L}{R} = \frac{8000 \text{ bits}}{10^8 \text{ bps}} = 8 \text{ microseconds} \]
  \[ U_{\text{sender}} = \frac{L}{RTT + L/R} = \frac{0.008}{8000} = 0.000027 \]
- 1KB pkt every 30 msec -> 33KB/sec throughput over 1 Gbps link
- network protocol limits use of physical resources!
A Sliding Packet Window

- **window** = set of adjacent sequence numbers
  - The size of the set is the window size; assume window size is \( n \)
- General idea: send up to \( n \) packets at a time
  - Sender can send packets in its window
  - Receiver can accept packets in its window
  - Window of acceptable packets "slides" on successful reception/acknowledgement

Acknowledgements w/ Sliding Window

- Two common options
  - cumulative ACKs: ACK carries next in-order sequence number that the receiver expects

Cumulative Acknowledgements (1)

- At receiver

  - After receiving \( B+1, B+2 \)
  - Receiver sends ACK(\( B_{new}+1 \))
Cumulative Acknowledgements (2)

- At receiver

- After receiving B+4, B+5

- Receiver sends ACK(B+1)

How do we recover?

Go-Back-N (GBN)

- Sender transmits up to n unacknowledged packets
- Receiver only accepts packets in order
  - discards out-of-order packets (i.e., packets other than B+1)
- Receiver uses cumulative acknowledgements
  - i.e., sequence# in ACK = next expected in-order sequence#
- Sender sets timer for 1st outstanding ack (A+1)
- If timeout, retransmit A+1, ..., A+n

Sliding Window with GBN

- Let A be the last ack’d packet of sender without gap; then window of sender = \( \{A+1, A+2, ..., A+n\} \)

- Let B be the last received packet without gap by receiver, then window of receiver = \( \{B+1, ..., B+n\} \)

GBN Example w/o Errors

Sender Window
\[
\begin{array}{cccc}
(1, 2) & 1 & 2 & 3 \\
(2, 3, 4) & 3 & 4 & 5 \\
(3, 4, 5) & 5 & 6 & 7 \\
(4, 5, 6) & 6 & 7 & 8 \\
\end{array}
\]

Receiver Window
\[
\begin{array}{cccc}
1 & 2 & 3 & 4 \\
2 & 3 & 4 & 5 \\
3 & 4 & 5 & 6 \\
4 & 5 & 6 & 7 \\
\end{array}
\]

GBN Example with Errors

Window size = 3 packets

Sender

Receiver

GBN: sender extended FSM

state diagram
GBN: receiver extended FSM

ACK-only: always send an ACK for correctly-received packet with the highest in-order seq #
- may generate duplicate ACKs
- need only remember expectedseqnum

- out-of-order packet:
  - discard (don't buffer) -> no receiver buffering!
  - Re-ACK packet with highest in-order seq #

Acknowledgements w/ Sliding Window

- Two common options
  - cumulative ACKs: ACK carries next in-order sequence number the receiver expects
  - selective ACKs: ACK individually acknowledges correctly received packets

- Selective ACKs offer more precise information but require more complicated book-keeping
- Many variants that differ in implementation details

Selective Repeat (SR)

- Sender: transmit up to n unacknowledged packets
- Assume packet k is lost, k+1 is not
- Receiver: indicates packet k+1 correctly received
- Sender: retransmit only packet k on timeout
- Efficient in retransmissions but complex book-keeping
  - need a timer per packet

SR Example with Errors

Observations

- With sliding windows, it is possible to fully utilize a link, provided the window size (n) is large enough. Throughput is ~ (n/RTT)
  - Stop & Wait is like n = 1.
- Sender has to buffer all unacknowledged packets, because they may require retransmission
- Receiver may be able to accept out-of-order packets, but only up to its buffer limits
- Implementation complexity depends on protocol details (GBN vs. SR)

Recap: components of a solution

- Checksums (for error detection)
- Timers (for loss detection)
- Acknowledgments
  - cumulative
  - selective
- Sequence numbers (duplicates, windows)
- Sliding Windows (for efficiency)
- Reliability protocols use the above to decide when and what to retransmit or acknowledge
What does TCP do?

Most of our previous tricks + a few differences

• Sequence numbers are byte offsets
• Sender and receiver maintain a sliding window
• Receiver sends cumulative acknowledgements (like GBN)
• Sender maintains a single retransmission timer
• Receivers do not drop out-of-sequence packets (like SR)
• Introduces fast retransmit optimization that uses duplicate ACKs to trigger early retransmission
• Introduces timeout estimation algorithms

Automatic Repeat Request (ARQ)

+ Self-clocking (Automatic)  
  Next lets move from the generic to the specific....
+ Adaptive
+ Flexible  
  TCP arguably the most successful protocol in the Internet....
  its an ARQ protocol

- Slow to start / adapt consider high Bandwidth/Delay product

TCP Header

<table>
<thead>
<tr>
<th>Source port</th>
<th>Destination port</th>
<th>Sequence number</th>
<th>Acknowledgment</th>
<th>Advertised window</th>
<th>HdrLen</th>
<th>Flags</th>
<th>Urgent pointer</th>
<th>Options (variable)</th>
<th>Data</th>
</tr>
</thead>
</table>

Last time: Components of a solution for reliable transport

• Checksums (for error detection)
• Timers (for loss detection)
• Acknowledgments
  – cumulative
  – selective
• Sequence numbers (duplicates, windows)
• Sliding Windows (for efficiency)
  – Go-Back-N (GBN)
  – Selective Replay (SR)

What does TCP do?

Many of our previous ideas, but some key differences

• Checksum

TCP Header

<table>
<thead>
<tr>
<th>Source port</th>
<th>Destination port</th>
<th>Sequence number</th>
<th>Acknowledgment</th>
<th>HdrLen</th>
<th>Flags</th>
<th>Advertised window</th>
<th>Urgent pointer</th>
<th>Options (variable)</th>
<th>Data</th>
</tr>
</thead>
</table>

Computed over header and data
What does TCP do?

Many of our previous ideas, but some key differences
- Checksum
- Sequence numbers are byte offsets

TCP: Segments and Sequence Numbers

TCP “Stream of Bytes” Service…

… Provided Using TCP “Segments”

TCP Segment

- IP packet
  - No bigger than Maximum Transmission Unit (MTU)
  - E.g., up to 1500 bytes with Ethernet
- TCP packet
  - IP packet with a TCP header and data inside
  - TCP header ≥ 20 bytes long
- TCP segment
  - No more than Maximum Segment Size (MSS) bytes
  - E.g., up to 1460 consecutive bytes from the stream
  - MSS = MTU − (IP header) − (TCP header)

Sequence Numbers

ISN (initial sequence number)

Sequence number = 1st byte in segment = ISN + k
**Sequence Numbers**

- **ISN (initial sequence number)**

  - Host A
    - Sequence number = 1
    - Acknowledgment
      - Acknowledgment is set to the next expected byte (seqno + length(data))

  - Host B
    - Sequence number = 2
    - Acknowledgment
      - Acknowledgment is set to the next expected byte (seqno + length(data))

**TCP Header**

- **Source port**
- **Destination port**
- **Sequence number**
- **Acknowledgment**
- **Header length**
- **Options (variable)**
- **Data**

**What does TCP do?**

Most of our previous tricks, but a few differences

- **Checksum**
- **Sequence numbers are byte offsets**
- **Receiver sends cumulative acknowledgements (like GBN)**

**ACKing and Sequence Numbers**

- **Sender sends packet**
  - Data starts with sequence number X
  - Packet contains B bytes \([X, X+1, X+2, \ldots, X+B-1]\)

- **Upon receipt of packet, receiver sends an ACK**
  - If all data prior to X already received:
    - ACK acknowledges \(X+B\) (because that is next-expected byte)
    - If highest in-order byte received is \(Y + 1\) < \(X\)
  - ACK acknowledges \(Y+1\)
  - Even if this has been ACKed before

**Normal Pattern**

- **Sender:** seqno=X, length=B
- **Receiver:** ACK=X+B
- **Sender:** seqno=X+B, length=B
- **Receiver:** ACK=X+2B
- **Sender:** seqno=X+2B, length=B
  - Seqno of next packet is same as last ACK field
TCP Header

<table>
<thead>
<tr>
<th>Source port</th>
<th>Destination port</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Sequence number</td>
<td>Acknowledgment</td>
</tr>
<tr>
<td>HdrLen</td>
<td>Flags</td>
</tr>
<tr>
<td>Checksum</td>
<td>Urgent pointer</td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
</tbody>
</table>

Acknowledgment gives seqno just beyond highest seqno received in order ("What Byte is Next")

What does TCP do?

Most of our previous tricks, but a few differences

- Checksum
- Sequence numbers are byte offsets
- Receiver sends cumulative acknowledgements (like GBN)
- Receivers can buffer out-of-sequence packets (like SR)

Loss with cumulative ACKs

- Sender sends packets with 100B and seqnos:
  - 100, 200, 300, 400, 500, 600, 700, 800, 900, ...
- Assume the fifth packet (seqno 500) is lost, but no others
- Stream of ACKs will be:
  - 200, 300, 400, 500, 500, 500, 500...

What does TCP do?

Most of our previous tricks, but a few differences

- Checksum
- Sequence numbers are byte offsets
- Receiver sends cumulative acknowledgements (like GBN)
- Receivers may not drop out of sequence packets (like SR)
- Introduces fast retransmit: optimization that uses duplicate ACKs to trigger early retransmission

Loss with cumulative ACKs

- "Duplicate ACKs" are a sign of an isolated loss
  - The lack of ACK progress means 500 hasn't been delivered
  - Stream of ACKs means some packets are being delivered
- Therefore, could trigger resend upon receiving k duplicate ACKs
  - TCP uses k=3
- But response to loss is trickier....
What does TCP do?
Most of our previous tricks, but a few differences
• Checksum
• Sequence numbers are byte offsets
• Receiver sends cumulative acknowledgements (like GBN)
• Receivers do not drop out of sequence packets (like SR)
• Introduces fast retransmit, optimization that uses duplicate
  ACKs to trigger early retransmission
• Sender maintains a single retransmission timer (like GBN) and
  retransmits on timeout

Retransmission Timeout
• If the sender hasn’t received an ACK by
timeout, retransmit the first packet in the
window
• How do we pick a timeout value?

Timing Illustration

Retransmission Timeout
• If haven’t received ack by timeout, retransmit
the first packet in the window
• How to set timeout?
  – Too long: connection has low throughput
  – Too short: retransmit packet that was just delayed
• Solution: make timeout proportional to RTT
• But how do we measure RTT?

RTT Estimation
• Use exponential averaging of RTT samples

EstimatedRTT = \alpha \times EstimatedRTT + (1 - \alpha) \times SampleRTT
0 < \alpha \leq 1

Exponential Averaging Example

EstimatedRTT (\alpha = 0.5)
EstimatedRTT (\alpha = 0.8)
Problem: Ambiguous Measurements

- How do we differentiate between the real ACK, and ACK of the retransmitted packet?

Karn/Partridge Algorithm

- Measure SampleRTT only for original transmissions
  - Once a segment has been retransmitted, do not use it for any further measurements
- Computes EstimatedRTT using $\alpha = 0.875$
- Timeout value (RTO) = $2 \times$ EstimatedRTT
- Employs exponential backoff
  - Every time RTO timer expires, set RTO $\leftarrow 2 \times$ RTO
  - (Up to maximum of 60 sec)
  - Every time new measurement comes in (= successful original transmission), collapse RTO back to $2 \times$ EstimatedRTT

Karn/Partridge in action

Jacobson/Karels Algorithm

- Problem: need to better capture variability in RTT
  - Directly measure deviation

- Deviation = $|$ SampleRTT – EstimatedRTT $|$
- EstimatedDeviation: exponential average of Deviation
- RTO = EstimatedRTT + $4 \times$ EstimatedDeviation

With Jacobson/Karels

What does TCP do?

Most of our previous ideas, but some key differences

- Checksum
- Sequence numbers are byte offsets
- Receiver sends cumulative acknowledgements (like GBN)
- Receivers do not drop out-of-sequence packets (like SR)
- Introduces fast retransmit: optimization that uses duplicate ACKs to trigger early retransmission
- Sender maintains a single retransmission timer (like GBN) and retransmits on timeout
TCP Header: What’s left?

Source port  | Destination port  
-------------|-------------------
Sequence number | Acknowledgment  
| HdrLen | Flags  | Advertised window  
Checksum | Urgent pointer | Options (variable)  
| Data  

“Must Be Zero” 6 bits reserved  
Number of 4-byte words in TCP header; 5 = no options

TCP Connection Establishment and Initial Sequence Numbers

Initial Sequence Number (ISN)

• Sequence number for the very first byte  
• Why not just use ISN = 0?  
• Practical issue  
  – IP addresses and port #s uniquely identify a connection  
  – Eventually, though, these port #s do get used again  
  – … small chance an old packet is still in flight  
• TCP therefore requires changing ISN  
• Hosts exchange ISNs when they establish a connection

Establishing a TCP Connection

• Three-way handshake to establish connection  
  – Host A sends a SYN (open; “synchronize sequence numbers”) to host B  
  – Host B returns a SYN acknowledgment (SYN ACK)  
  – Host A sends an ACK to acknowledge the SYN ACK

Each host tells its ISN to the other host.
TCP Header

Source port | Destination port
---|---
Sequence number
Acknowledgment
Header length
Flags | Advertised window
Checksum | Urgent pointer
Options (variable)
Data

Step 1: A’s Initial SYN Packet

A’s port | B’s port
---|---
A’s Initial Sequence Number
(Initial SYN-ACK packet)
Checksum | Urgent pointer
Options (variable)

A tells B it wants to open a connection...

Step 2: B’s SYN-ACK Packet

B’s port | A’s port
---|---
B’s Initial Sequence Number
ACK = A’s ISN plus 1
5 | 0 | Flags | Advertised window
Checksum | Urgent pointer
Options (variable)

B tells A it accepts, and is ready to hear the next byte...

… upon receiving this packet, A can start sending data

Step 3: A’s ACK of the SYN-ACK

A’s port | B’s port
---|---
A’s Initial Sequence Number
B’s ISN plus 1
20B | 0 | Flags | Advertised window
Checksum | Urgent pointer
Options (variable)

A tells B it’s likewise okay to start sending

… upon receiving this packet, B can start sending data

Timing Diagram: 3-Way Handshaking

Active
Open
Client (initiator)
connect() SYN, SeqNum = x
SYN + ACK, SeqNum = x, Ack = x + 1
ACK, Ack = y + 1

Passive
Open
Server
listen()
SYN Loss and Web Downloads

- User clicks on a hypertext link
  - Browser creates a socket and does a "connect"
  - The "connect" triggers the OS to transmit a SYN
- If the SYN is lost...
  - 3-6 seconds of delay: can be very long
  - User may become impatient
  - … and click the hyperlink again, or click "reload"
- User triggers an "abort" of the "connect"
  - Browser creates a new socket and another "connect"
  - Essentially, forces a faster send of a new SYN packet!
  - Sometimes very effective, and the page comes quickly

Tearing Down the Connection

Normal Termination, One Side At A Time

- Finish (FIN) to close and receive remaining bytes
  - FIN occupies one byte in the sequence space
- Other host acks the byte to confirm
- Closes A's side of the connection, but not B's
  - Until B likewise sends a FIN
  - Which A then acks

Normal Termination, Both Together

- Same as before, but B sets FIN with their ack of A's FIN

Abrupt Termination

- A sends a RESET (RST) to B
  - E.g., because application process on A crashed
- That's it
  - B does not ack the RST
  - Thus, RST is not delivered reliably
  - And: any data in flight is lost
  - But: if B sends anything more, will elicit another RST

TCP Header

<table>
<thead>
<tr>
<th>Source port</th>
<th>Destination port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence number</td>
<td>Acknowledgment</td>
</tr>
<tr>
<td>AckLen</td>
<td>Flags</td>
</tr>
<tr>
<td>Checksum</td>
<td>Urgent pointer</td>
</tr>
<tr>
<td></td>
<td>Data</td>
</tr>
</tbody>
</table>

| Flags: SYN ACK FIN RST PSH URG |
TCP State Transitions

Data, ACK exchanges are in here

TCP Header

<table>
<thead>
<tr>
<th>Source port</th>
<th>Destination port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sequence number
Acknowledgment
Window
Flags
URP
CheckSum
Options (variable)
Data

Recap: Sliding Window (so far)

- What does TCP do?
  - ARQ windowing, set-up, tear-down
- Flow Control in TCP

- Both sender & receiver maintain a **window**

- **Left edge** of window:
  - Sender: beginning of **unacknowledged** data
  - Receiver: beginning of **undelivered** data

- **Right edge**: Left edge + **constant**
  - constant only limited by buffer size in the transport layer
Solution: Advertised Window (Flow Control)

- Receiver uses an “Advertised Window” (W) to prevent sender from overflowing its window
  - Receiver indicates value of W in ACKs
  - Sender limits number of bytes it can have in flight <= W

Sliding Window w/ Flow Control

- Sender: window advances when new data ack’d
- Receiver: window advances as receiving process consumes data
- Receiver advertises to the sender where the receiver window currently ends (“righthand edge”)
  - Sender agrees not to exceed this amount
Advertised Window Limits Rate

- Sender can send no faster than W/RTT bytes/sec
- Receiver only advertises more space when it has consumed old arriving data
- In original TCP design, that was the sole protocol mechanism controlling sender’s rate
- What’s missing?

TCP

- The concepts underlying TCP are simple
  - acknowledgments (feedback)
  - timers
  - sliding windows
  - buffer management
  - sequence numbers

TCP

- The concepts underlying TCP are simple
- But tricky in the details
- Do the details matter?

TCP

- The concepts underlying TCP are simple
- But tricky in the details

Sizing Windows for Congestion Control

- What are the problems?
- How might we address them?

- What does TCP do?
  - ARQ windowing, set-up, tear-down
- Flow Control in TCP
- Congestion Control in TCP
We have seen:
- Flow control: adjusting the sending rate to keep from overwhelming a slow receiver

Now let's attend…
- Congestion control: adjusting the sending rate to keep from overloading the network

Statistical Multiplexing → Congestion
- If two packets arrive at the same time
  - A router can only transmit one
  - … and either buffers or drops the other
- If many packets arrive in a short period of time
  - The router cannot keep up with the arriving traffic
  - … delays traffic, and the buffer may eventually overflow
- Internet traffic is bursty

Congestion is undesirable
Typical queuing system with bursty arrivals

Who Takes Care of Congestion?
- Network? End hosts? Both?

- TCP’s approach:
  - End hosts adjust sending rate
  - Based on implicit feedback from network

  - Not the only approach
  - A consequence of history rather than planning

Some History: TCP in the 1980s
- Sending rate only limited by flow control
  - Packet drops → senders (repeatedly!) retransmit a full window’s worth of packets

  - Led to “congestion collapse” starting Oct. 1986
  - Throughput on the NSF network dropped from 32Kbits/s to 40bits/sec

  - “Fixed” by Van Jacobson’s development of TCP’s congestion control (CC) algorithms

Jacobson’s Approach
- Extend TCP’s existing window-based protocol but adapt the window size in response to congestion
  - required no upgrades to routers or applications!
  - patch of a few lines of code to TCP implementations

- A pragmatic and effective solution
  - but many other approaches exist

- Extensively improved on since
  - topic now sees less activity in ISP contexts
  - but is making a comeback in datacenter environments
Three Issues to Consider

• Discovering the available (bottleneck) bandwidth
• Adjusting to variations in bandwidth
• Sharing bandwidth between flows

Discovering available bandwidth

• Pick sending rate to match bottleneck bandwidth
  – Without any a priori knowledge
  – Could be gigabit link, could be a modem

Multiple flows and sharing bandwidth

Two Issues:
• Adjust total sending rate to match bandwidth
• Allocation of bandwidth between flows

Adjusting to variations in bandwidth

• Adjust rate to match instantaneous bandwidth
  – Assuming you have rough idea of bandwidth

Abstract View

- Ignore internal structure of router and model it as having a single queue for a particular input-output pair

Reality

Congestion control is a resource allocation problem involving many flows, many links, and complicated global dynamics
View from a single flow

- Knee – point after which
  - Throughput increases slowly
  - Delay increases fast

- Cliff – point after which
  - Throughput starts to drop to zero (congestion collapse)
  - Delay approaches infinity

General Approaches

(0) Send without care
   - Many packet drops

(1) Reservations
   - Pre-arrange bandwidth allocations
   - Requires negotiation before sending packets
   - Low utilization

(2) Pricing
   - Don’t drop packets for the high-bidders
   - Requires payment model

(3) Dynamic Adjustment
   - Hosts probe network; infer level of congestion; adjust
   - Network reports congestion level to hosts; hosts adjust
   - Combinations of the above
   - Simple to implement but suboptimal, messy dynamics

All three techniques have their place
- Generality of dynamic adjustment has proven powerful
- Doesn’t presume business model, traffic characteristics, application requirements; does assume good citizenship
TCP’s Approach in a Nutshell

- TCP connection has window
  - Controls number of packets in flight
- Sending rate: ~Window/RTT
- Vary window size to control sending rate

All These Windows...

- Congestion Window: \( \text{CWND} \)
  - How many bytes can be sent without overflowing routers
  - Computed by the sender using congestion control algorithm
- Flow control window: \( \text{AdvertisedWindow (RWND)} \)
  - How many bytes can be sent without overflowing receiver’s buffers
  - Determined by the receiver and reported to the sender
- Sender-side window = \( \text{minimum}\{\text{CWND, RWND}\} \)
  - Assume for this material that \( \text{RWND} \gg \text{CWND} \)

Note

- This lecture will talk about \( \text{CWND} \) in units of MSS
  - (Recall MSS: Maximum Segment Size, the amount of payload data in a TCP packet)
  - This is only for pedagogical purposes
- In reality this is a LIE: Real implementations maintain \( \text{CWND} \) in bytes

Two Basic Questions

- How does the sender detect congestion?
- How does the sender adjust its sending rate?
  - To address three issues
    - Finding available bottleneck bandwidth
    - Adjusting to bandwidth variations
    - Sharing bandwidth

Detecting Congestion

- Packet delays
  - Tricky: noisy signal (delay often varies considerably)
- Router tells endhosts they’re congested
- Packet loss
  - Fail-safe signal that TCP already has to detect
  - Complication: non-congestive loss (checksum errors)
- Two indicators of packet loss
  - No ACK after certain time interval: timeout
  - Multiple duplicate ACKs

Not All Losses the Same

- Duplicate ACKs: isolated loss
  - Still getting ACKs
- Timeout: much more serious
  - Not enough dupacks
  - Must have suffered several losses
- We will adjust rate differently for each case
Rate Adjustment

• Basic structure:
  – Upon receipt of ACK (of new data): increase rate
  – Upon detection of loss: decrease rate

• How we increase/decrease the rate depends on the phase of congestion control we’re in:
  – Discovering available bottleneck bandwidth vs.
  – Adjusting to bandwidth variations

Bandwidth Discovery with Slow Start

• Goal: estimate available bandwidth
  – start slow (for safety)
  – but ramp up quickly (for efficiency)

• Consider
  – RTT = 100ms, MSS=1000bytes
  – Window size to fill 1Mbps of BW = 12.5 packets
  – Window size to fill 1Gbps = 12,500 packets
  – Either is possible!

“Slow Start” Phase

• Sender starts at a slow rate but increases **exponentially** until first loss

• Start with a small congestion window
  – Initially, CWND = 1
  – So, initial sending rate is MSS/RTT

• Double the CWND for each RTT with no loss

Slow Start in Action

• For each RTT: double CWND
• Simpler implementation: for each ACK, CWND *= 1

Adjusting to Varying Bandwidth

• Slow start gave an estimate of available bandwidth

• Now, want to track variations in this available bandwidth, oscillating around its current value
  – Repeated probing (rate increase) and backoff (rate decrease)

• TCP uses: “Additive Increase Multiplicative Decrease” (AIMD)
  – We’ll see why shortly…

AIMD

• Additive increase
  – Window grows by one MSS for every RTT with no loss
  – For each successful RTT, CWND = CWND + 1
  – Simple implementation:
    • for each ACK, CWND = CWND+ 1/CWND

• Multiplicative decrease
  – On loss of packet, divide congestion window in **half**
  – On loss, CWND = CWND/2
Leads to the TCP “Sawtooth”

Slow-Start vs. AIMD

• When does a sender stop Slow-Start and start Additive Increase?
  • Introduce a “slow start threshold” (ssthresh)
    – Initialized to a large value
    – On timeout, ssthresh = CWND/2
  • When CWND = ssthresh, sender switches from slow-start to AIMD-style increase

Why AIMD?

Recall: Three Issues

• Discovering the available (bottleneck) bandwidth
  – Slow Start

• Adjusting to variations in bandwidth
  – AIMD

• Sharing bandwidth between flows

Goals for bandwidth sharing

• Efficiency: High utilization of link bandwidth
• Fairness: Each flow gets equal share
Why AIMD?

- Some rate adjustment options: Every RTT, we can
  - Multiplicative increase or decrease: \( CWND \to a \times CWND \)
  - Additive increase or decrease: \( CWND \to CWND + b \)

- Four alternatives:
  - AIAD: gentle increase, gentle decrease
  - AIMD: gentle increase, drastic decrease
  - MIAD: drastic increase, gentle decrease
  - MIMD: drastic increase and decrease

Simple Model of Congestion Control

- Two users
  - rates \( x_1 \) and \( x_2 \)
- Congestion when \( x_1 + x_2 > 1 \)
- Unused capacity when \( x_1 + x_2 < 1 \)
- Fair when \( x_1 = x_2 \)

Example

- Efficient: \( x_1 + x_2 = 1 \)
- Congested: \( x_1 + x_2 = 1.2 \)
- Inefficient: \( x_1 + x_2 = 0.7 \)

AIAD

- Increase: \( x + a_I \)
- Decrease: \( x - a_D \)
- Does not converge to fairness

MIMD

- Increase: \( x \cdot b_I \)
- Decrease: \( x \cdot b_D \)
- Does not converge to fairness

Recall: Three Issues

- Discovering the available (bottleneck) bandwidth
  - Slow Start
- Adjusting to variations in bandwidth
  - AIMD
- Sharing bandwidth between flows
AIMD

- Increase: $x + a_1$
- Decrease: $x \times b_D$
- Converges to fairness

Why is AIMD fair? (a pretty animation...)

Two competing sessions:
- Additive increase gives slope of 1, as throughput increases
- Multiplicative decrease decreases throughput proportionally

Fairness line

EFFICIENCY LINE

AIMD Sharing Dynamics

TCP Congestion Control (Gruesome) Details

Implementation

- State at sender
  - CWND (initialized to a small constant)
  - ssthresh (initialized to a large constant)
  - [Also dupACKcount and timer, as before]

- Events
  - ACK (new data)
  - dupACK (duplicate ACK for old data)
  - Timeout

AIAD Sharing Dynamics
Event: ACK (new data)

- If CWND < ssthresh
  - CWND += 1

  \[ \text{CWND packets per RTT} \]
  \[ \text{Hence after one RTT with no drops:} \]
  \[ \text{CWND} = 2\times\text{CWND} \]

- Else
  - CWND = CWND + \( \frac{1}{\text{CWND}} \)

**Slow start phase**

- "Congestion Avoidance" phase (additive increase)

**Congestion Avoidance" phase (additive increase)**

Event: TimeOut

- On Timeout
  - ssthresh \( \rightarrow \) CWND/2
  - CWND \( \leftarrow \) 1

**Flow Control in TCP**

**Congestion Control in TCP**

- AIMD, Fast-Recovery

**What does TCP do?**
- ARQ windowing, set-up, tear-down
- Flow Control in TCP
- Congestion Control in TCP

**Example**

- Slow start in operation until it reaches half of previous CWND, i.e., SS_THRESH

Slow-start restart: Go back to CWND = 1 MSS, but take advantage of knowing the previous value of CWND
One Final Phase: Fast Recovery

• The problem: congestion avoidance too slow in recovering from an isolated loss

Example (in units of MSS, not bytes)

• Consider a TCP connection with:
  – CWND=10 packets
  – Last ACK was for packet # 101
    • i.e., receiver expecting next packet to have seq. no. 101

  • 10 packets [101, 102, 103, ..., 110] are in flight
    – Packet 101 is dropped

The problem – A timeline

• ACK 101 (due to 102) cwnd=10 dupACK#1 [no xmit]
• ACK 101 (due to 103) cwnd=10 dupACK#2 [no xmit]
• ACK 101 (due to 104) cwnd=10 dupACK#3 [no xmit]
  – RETRANSMIT 101 ssthresh=5 cwnd= 5
  • ACK 101 (due to 105) cwnd=5 + 1/5 (no xmit)
  • ACK 101 (due to 106) cwnd=5 + 2/5 (no xmit)
  • ACK 101 (due to 107) cwnd=5 + 3/5 (no xmit)
  • ACK 101 (due to 108) cwnd=5 + 4/5 (no xmit)
  • ACK 101 (due to 109) cwnd=5 + 5/5 (no xmit)
  • ACK 101 (due to 110) cwnd=6 + 1/5 (no xmit)
  – ACK 111 (due to 101) only now can we transmit new packets
    • Plus no packets in flight so ACK “clocking” (no increase CWND) stalls for another RTT

Solution: Fast Recovery

Idea: Grant the sender temporary “credit” for each dupACK so as to keep packets in flight

• If dupACKcount = 3
  – ssthresh = cwnd/2
  – cwnd = ssthresh + 3

• While in fast recovery
  – cwnd = cwnd + 1 for each additional duplicate ACK

• Exit fast recovery after receiving new ACK
  – set cwnd = ssthresh

Example

• Consider a TCP connection with:
  – CWND=10 packets
  – Last ACK was for packet # 101
    • i.e., receiver expecting next packet to have seq. no. 101

  • 10 packets [101, 102, 103,..., 110] are in flight
    – Packet 101 is dropped

Timeline

• ACK 101 (due to 102) cwnd=10 dup#1
• ACK 101 (due to 103) cwnd=10 dup#2
• ACK 101 (due to 104) cwnd=10 dup#3
  – RETRANSMIT 101 ssthresh=5 cwnd= 8 (5+3)
  • ACK 101 (due to 105) cwnd=9 [no xmit]
  • ACK 101 (due to 106) cwnd=10 [no xmit]
  • ACK 101 (due to 107) cwnd=11 [xmit 111]
  • ACK 101 (due to 108) cwnd=12 [xmit 112]
  • ACK 101 (due to 109) cwnd=13 [xmit 113]
  • ACK 101 (due to 110) cwnd=14 [xmit 114]
  • ACK 111 (due to 101) cwnd = 5 [xmit 115] exiting fast recovery
  • Packets 111-114 already in flight
  • ACK 112 (due to 111) cwnd = 5 + 1/5 back in congestion avoidance
Putting it all together: The TCP State Machine (partial)

How are ssthresh, CWND and dupACKcount updated for each event that causes a state transition?

TCP Flavors

- TCP-Tahoe
  - cwnd = 1 on triple dupACK
- TCP-Reno
  - cwnd = 1 on timeout
  - cwnd = cwnd/2 on triple dupack
- TCP-newReno
  - TCP-Reno + improved fast recovery
- TCP-SACK
  - incorporates selective acknowledgements

What does TCP do?
- ARQ windowing, set-up, tear-down
- Flow Control in TCP
- Congestion Control in TCP
  - AIMD, Fast-Recovery, Throughput

TCP Throughput Equation

A Simple Model for TCP Throughput

Packet drop rate, $p = 1/A$, where $A = \frac{3W_{\text{max}}}{B}$

Throughput, $B = \frac{A}{\sqrt{2}} \frac{1}{\sqrt{RTT \sqrt{p}}}$

A Simple Model for TCP Throughput
Some implications: (1) Fairness

Throughput, $B = \sqrt[3]{\frac{3}{2}} \frac{1}{RTT \sqrt{p}}$

- Flows get throughput inversely proportional to RTT
  - Is this fair?

Some Implications:
(2) How does this look at high speed?

- Assume that RTT = 100ms, MSS=1500bytes
- What value of $p$ is required to go 100Gbps?
  - Roughly $2 \times 10^{-12}$
- How long between drops?
  - Roughly 16.6 hours
- How much data has been sent in this time?
  - Roughly 6 petabits
- These are not practical numbers!

Some implications:
(3) Rate-based Congestion Control

Throughput, $B = \sqrt[3]{\frac{3}{2}} \frac{1}{RTT \sqrt{p}}$

- One can dispense with TCP and just match eqtn:
  - Equation-based congestion control
  - Measure drop percentage $p$, and set rate accordingly
  - Useful for streaming applications

Some Implications: (4) Lossy Links

- TCP assumes all losses are due to congestion
- What happens when the link is lossy?
- Throughput $\sim \frac{1}{\sqrt{p}}$ where $p$ is loss prob.
- This applies even for non-congestion losses!

Other Issues: Cheating

- Cheating pays off

- Some favorite approaches to cheating:
  - Increasing CWND faster than 1 per RTT
  - Using large initial CWND
  - Opening many connections

Increasing CWND Faster

$x$ increases by 2 per RTT
$y$ increases by 1 per RTT

Limit rates: $x = 2y$
• What does TCP do?
  — ARQ windowing, set-up, tear-down
• Flow Control in TCP
• Congestion Control in TCP
  — AIMD, Fast-Recovery, Throughput
• Limitations of TCP Congestion Control

A Closer look at problems with TCP Congestion Control
TCP Flavors

- TCP-Tahoe
  - CWND = 1 on triple dupACK
- TCP-Reno
  - CWND = 1 on timeout
  - CWND = CWND/2 on triple dupACK
- TCP-newReno
  - TCP-Reno + improved fast recovery
- TCP-SACK
  - incorporates selective acknowledgements

Interoperability

- How can all these algorithms coexist? Don’t we need a single, uniform standard?
- What happens if I’m using Reno and you are using Tahoe, and we try to communicate?

TCP Throughput Equation

\[
\text{Throughput} = \frac{1}{\sqrt{2} \cdot \text{RTT} \cdot \sqrt{p}}
\]

Packet drop rate, \( p = 1/A \), where \( A = \frac{3}{8} \cdot \frac{W_{\text{max}}}{\text{RTT}} \)

Implications (1): Different RTTs

- Flows get throughput inversely proportional to RTT
- TCP unfair in the face of heterogeneous RTTs!
Implications (2): High Speed TCP

\[
\text{Throughput} = \sqrt{\frac{3}{2}} \frac{1}{\sqrt{\text{RTT} \cdot p}}
\]

- Assume RTT = 100ms, MSS=1500bytes
- What value of \( p \) is required to reach 100Gbps throughput
  - \( \sim 2 \times 10^{-12} \)
- How long between drops?
  - \( \sim 16.6 \) hours
- How much data has been sent in this time?
  - \( \sim 6 \) petabits
- These are not practical numbers!

Adapting TCP to High Speed

- Once past a threshold speed, increase CWND faster
  - A proposed standard [Floyd’03]: once speed is past some threshold, change equation to \( p^{-2} \) rather than \( p^{-3} \)
  - Let the additive constant in AIMD depend on CWND

- Other approaches?
  - Multiple simultaneous connections (hack but works today)
  - Router-assisted approaches (will see shortly)

Implications (3): Rate-based CC

\[
\text{Throughput} = \sqrt{\frac{3}{2}} \frac{1}{\sqrt{\text{RTT} \cdot p}}
\]

- TCP throughput is “choppy”
  - repeated swings between \( W/2 \) to \( W \)
- Some apps would prefer sending at a steady rate
  - e.g., streaming apps
- A solution: “Equation-Based Congestion Control”
  - ditch TCP’s increase/decrease rules and just follow the equation
  - measure drop percentage \( p \), and set rate accordingly
- Following the TCP equation ensures we’re “TCP friendly”
  - i.e., use no more than TCP does in similar setting

Other Limitations of TCP Congestion Control

(4) Loss not due to congestion?

- TCP will confuse any loss event with congestion
- Flow will cut its rate
  - Throughput \( \sim 1/\sqrt{p} \) where \( p \) is loss prob.
  - Applies even for non-congestion losses!
- We’ll look at proposed solutions shortly...

(5) How do short flows fare?

- 50% of flows have < 1500B to send; 80% < 100KB
- Implication (1): short flows never leave slow start!
  - short flows never attain their fair share
- Implication (2): too few packets to trigger dupACKs
  - Isolated loss may lead to timeouts
  - At typical timeout values of \( \sim 500 \)ms, might severely impact flow completion time
(6) TCP fills up queues $\rightarrow$ long delays

- A flow deliberately overshoots capacity, until it experiences a drop
- Means that delays are large for everyone
  - Consider a flow transferring a 10GB file sharing a bottleneck link with 10 flows transferring 100B

(7) Cheating

- Three easy ways to cheat
  - Increasing CWND faster than +1 MSS per RTT

Increasing CWND Faster

- $x$ increases by 2 per RTT
- $y$ increases by 1 per RTT
- Limit rates: $x = 2y$

(7) Cheating

- Three easy ways to cheat
  - Increasing CWND faster than +1 MSS per RTT
  - Opening many connections
  - Using large initial CWND

Open Many Connections

- Assume
  - A starts 10 connections to B
  - D starts 1 connection to E
  - Each connection gets about the same throughput

- Then A gets 10 times more throughput than D

- Why hasn’t the Internet suffered a congestion collapse yet?
(8) CC intertwined with reliability

- Mechanisms for CC and reliability are tightly coupled
  - CWND adjusted based on ACKs and timeouts
  - Cumulative ACKs and fast retransmit/recovery rules
- Complicates evolution
  - Consider changing from cumulative to selective ACKs
  - A failure of modularity, not layering
- Sometimes we want CC but not reliability
  - e.g., real-time applications
- Sometimes we want reliability but not CC (?)

Recap: TCP problems

- Misled by non-congestion losses
- Fills up queues leading to high delays
- Short flows complete before discovering available capacity
- AIMD impractical for high speed links
- Sawtooth discovery too choppy for some apps
- Unfair under heterogeneous RTTs
- Tight coupling with reliability mechanisms
- Endhosts can cheat

Could fix many of these with some help from routers!

Router-Assisted Congestion Control

- Three tasks for CC:
  - Isolation/fairness
  - Adjustment
  - Detecting congestion

Fairness: General Approach

- Routers classify packets into “flows”
  - [For now] flows are packets between same source/destination
- Each flow has its own FIFO queue in router
- Router services flows in a fair fashion
  - When line becomes free, take packet from next flow in a fair order
- What does “fair” mean exactly?

How can routers ensure each flow gets its “fair share”?
Max-Min Fairness

- Given set of bandwidth demands $r_i$ and total bandwidth $C$, max-min bandwidth allocations are:
  
  $$a_i = \min(f, r_i)$$

  where $f$ is the unique value such that $\text{Sum}(a_i) = C$

Example

- $C = 10$; $r_1 = 8$, $r_2 = 6$, $r_3 = 2$; $N = 3$
- $C/3 = 3.33 \rightarrow$
  - Can service all of $r_3$
  - Remove $r_3$ from the accounting: $C = C - r_3 = 8$; $N = 2$
- $C/2 = 4 \rightarrow$
  - Can’t service all of $r_1$ or $r_2$
  - So hold them to the remaining fair share: $f = 4$

How do we deal with packets of different sizes?

- Mental model: Bit-by-bit round robin (“fluid flow”)
- Can you do this in practice?
- No, packets cannot be preempted
- But we can approximate it
  - This is what “fair queuing” routers do

Fair Queuing (FQ)

- For each packet, compute the time at which the last bit of a packet would have left the router if flows are served bit-by-bit
- Then serve packets in the increasing order of their deadlines
Fair Queuing (FQ)

- Think of it as an implementation of round-robin generalized to the case where not all packets are equal sized
- Weighted fair queuing (WFQ): assign different flows different shares
- Today, some form of WFQ implemented in almost all routers
  - Not the case in the 1980s-90s, when CC was being developed
  - Mostly used to isolate traffic at larger granularities (e.g., per-prefix)

FQ vs. FIFO

- FQ advantages:
  - Isolation: cheating flows don’t benefit
  - Bandwidth share does not depend on RTT
  - Flows can pick any rate adjustment scheme they want
- Disadvantages:
  - More complex than FIFO: per flow queue/state, additional per-packet book-keeping

FQ in the big picture

- FQ does not eliminate congestion → it just manages the congestion

```
Blue and Green get 0.5Gbps, any excess will be dropped
If the green flow doesn’t drop its sending rate to 100Mbps, we’re wasting 400Mbps that could be usefully given to the blue flow
```

FQ in the big picture

- FQ does not eliminate congestion → it just manages the congestion
  - robust to cheating, variations in RTT, details of delay, reordering, retransmission, etc.
- But congestion (and packet drops) still occurs
- And we still want end-hosts to discover/adapt to their fair share!
- What would the end-to-end argument say w.r.t. congestion control?

Fairness is a controversial goal

- What if you have 8 flows, and I have 4?
  - Why should you get twice the bandwidth
- What if your flow goes over 4 congested hops, and mine only goes over 1?
  - Why shouldn’t you be penalized for using more scarce bandwidth?
- And what is a flow anyway?
  - TCP connection
  - Source-Destination pair?
  - Source?

Router-Assisted Congestion Control

- CC has three different tasks:
  - Isolation/fairness
  - Rate adjustment
  - Detecting congestion
Why not just let routers tell endhosts what rate they should use?

- Packets carry “rate field”
- Routers insert “fair share” $f$ in packet header
  - Calculated as with FQ
- End-hosts set sending rate (or window size) to $f$
  - Hopefully (still need some policing of endhosts!)
- This is the basic idea behind the “Rate Control Protocol” (RCP) from Dukkipati et al. ’07

Flow Completion Time: TCP vs. RCP (Ignore XCP)

Why the improvement?

Router-Assisted Congestion Control

- CC has three different tasks:
  - Isolation/fairness
  - Rate adjustment
  - Detecting congestion

Explicit Congestion Notification (ECN)

- Single bit in packet header; set by congested routers
  - If data packet has bit set, then ACK has ECN bit set
- Many options for when routers set the bit
  - Tradeoff between (link) utilization and (packet) delay
- Congestion semantics can be exactly like that of drop
  - i.e., endhost reacts as though it saw a drop
- Advantages:
  - Don’t confuse corruption with congestion; recovery w/ rate adjustment
  - Can serve as an early indicator of congestion to avoid delays
  - Easy (easier) to incrementally deploy
  - Defined as extension to TCP/IP in RFC 3168 (uses diffserv bits in the IP header)

One final proposal: Charge people for congestion!

- Use ECN as congestion markers
- Whenever I get an ECN bit set, I have to pay $5$
- Now, there’s no debate over what a flow is, or what fair is…
- Idea started by Frank Kelly here in Cambridge
  - “optimal” solution, backed by much math
  - Great idea: simple, elegant, effective
  - Unclear that it will impact practice — although London congestion works
Some TCP issues outstanding...

Synchronized Flows

- Aggregate window has same dynamics
- Therefore buffer occupancy has same dynamics
- Rule-of-thumb still holds.

Many TCP Flows

- Independent, desynchronized
- Central limit theorem says the aggregate becomes Gaussian
- Variance (buffer size) decreases as $N$ increases

TCP in detail

- What does TCP do?
  – ARQ windowing, set-up, tear-down
- Flow Control in TCP
- Congestion Control in TCP
  – AIMD, Fast-Recovery, Throughput
- Limitations of TCP Congestion Control
- Router-assisted Congestion Control

Recap

- TCP:
  – somewhat hacky
  – but practical/deployable
  – good enough to have raised the bar for the deployment of new, more optimal, approaches
  – though the needs of datacenters might change the status quos
Topic 6 – Applications

- Overview
- Infrastructure Services (DNS)
- Traditional Applications (web)
- Multimedia Applications (SIP)
- P2P Networks

Client-server architecture

- server:
  - always-on host
  - permanent IP address
  - server farms for scaling
- clients:
  - communicate with server
  - may be intermittently connected
  - may have dynamic IP addresses
  - do not communicate directly with each other

Pure P2P architecture

- no always-on server
- arbitrary end systems directly communicate
- peers are intermittently connected and change IP addresses

Hybrid of client-server and P2P

- Skype
  - voice-over IP P2P application
  - centralized server: finding address of remote party
  - client-client connection: direct (not through server)
- Instant messaging
  - chatting between two users is P2P
  - centralized service: client presence detection/location
    - user registers its IP address with central server when it comes online
    - user contacts central server to find IP addresses of buddies

Addressing processes

- to receive messages, process must have identifier
- host device has unique 32-bit IP address
- Q: does IP address of host on which process runs suffice for identifying the process?
  - A: No, many processes can be running on same host
- identifier includes both IP address and port numbers associated with process on host
- Example port numbers:
  - HTTP server: 80
  - Mail server: 25
- to send HTTP message to yuba.stanford.edu web server:
  - IP address: 171.64.74.58
  - Port number: 80
- more shortly...

Recall: Multiplexing is a service provided by (each) layer too!
App-layer protocol defines

- Types of messages exchanged, e.g., request, response
- Message syntax: what fields in messages & how fields are delineated
- Message semantics: meaning of information in fields
- Rules for when and how processes send & respond to messages

Public-domain protocols:
- defined in RFCs
- allows for interoperability
  - e.g., HTTP, SMTP

Proprietary protocols:
- e.g., Skype

Public-domain protocols:
- defined in RFCs
- allows for interoperability
  - e.g., HTTP, SMTP

Proprietary protocols:
- e.g., Skype

What transport service does an app need?

Data loss
- some apps (e.g., audio) can tolerate some loss
- other apps (e.g., file transfer, telnet) require 100% reliable data transfer

Throughput
- some apps (e.g., multimedia) require minimum amount of throughput to be "effective"
- other apps ("elastic apps") make use of whatever throughput they get

Security
- Encryption, data integrity, ...

Mysterious secret of Transport
- There is more than sort of transport layer

Shocked?
- I seriously doubt it...

Recall the two most common TCP and UDP

Logical Steps in Using Internet

- Human has name of entity she wants to access — Content, host, etc.
- Invokes an application to perform relevant task — Using that name
- App invokes DNS to translate name to address
- App invokes transport protocol to contact host — Using address as destination

Addresses vs Names

- Scope of relevance:
  - App/user is primarily concerned with names
  - Network is primarily concerned with addresses
- Timescales:
  - Name lookup once (or get from cache)
  - Address lookup on each packet
- When moving a host to a different subnet:
  - The address changes
  - The name does not change
- When moving content to a differently named host:
  - Name and address both change!

Relationship Between Names & Addresses

- Addresses can change underneath
  - Move www.bbc.co.uk to 212.58.246.92
  - Humans/Apps should be unaffected

- Name could map to multiple IP addresses
  - www.bbc.co.uk to multiple replicas of the Web site
  - Enables
    - Load-balancing
    - Reducing latency by picking nearby servers

- Multiple names for the same address
  - E.g., aliases like www.bbc.co.uk and bbc.co.uk
  - Mnemonic stable name, and dynamic canonical name
    - Canonical name = actual name of host
Mapping from Names to Addresses

• Originally: per-host file /etc/hosts
  – SRI (Menlo Park) kept master copy
  – Downloaded regularly
  – Flat namespace

• Single server not resilient, doesn’t scale
  – Adopted a distributed hierarchical system

• Two intertwined hierarchies:
  – Infrastructure: hierarchy of DNS servers
  – Naming structure: www.bbc.co.uk

Domain Name System (DNS)

• Top of hierarchy: Root
  – Location hardwired into other servers

• Next Level: Top-level domain (TLD) servers
  – .com, .edu, etc.
  – .uk, .au, .to, etc.
  – Managed professionally

• Bottom Level: Authoritative DNS servers
  – Actually do the mapping
  – Can be maintained locally or by a service provider

Distributed Hierarchical Database

DNS Root Servers

• 13 root servers (see http://www.root-servers.org/)
  – Labeled A through M
• Does this scale?

DNS Root Servers

• 13 root servers (see http://www.root-servers.org/)
  – Labeled A through M
• Replication via any-casting (localized routing for addresses)
Using DNS

- Two components
  - Local DNS servers
  - Resolver software on hosts
- Local DNS server ("default name server")
  - Usually near the endhosts that use it
  - Local hosts configured with local server (e.g., `/etc/resolv.conf`) or learn server via DHCP
- Client application
  - Extract server name (e.g., from the URL)
  - Do `gethostbyname()` to trigger resolver code

How Does Resolution Happen? (Iterative example)

Host at cl.cam.ac.uk wants IP address for www.stanford.edu

1. Host enquiry is delegated to local DNS server
2. Consider transactions 2–7 only
3. Local host contact server replies with name of next server to contact
4. "I don’t know this name, but ask this server"

Requesting host cl.cam.ac.uk

Local DNS server
dns.cam.ac.uk

TLD DNS server
dns.stanford.edu

Authoritative DNS server
dns.stanford.edu

How DNS caching works
- DNS servers cache responses to queries
- Responses include a "time to live" (TTL) field
- Server deletes cached entry after TTL expires

Recursive and Iterative Queries - Hybrid case

- Recursive query
  - Ask server to get answer for you
  - E.g., requests 1,2 and responses 9,10
- Iterative query
  - Ask server who to ask next
  - E.g., all other request-response pairs

Negative Caching

- Remember things that don’t work
  - Misspellings like bbc.co.uk and www.bbc.com.uk
  - These can take a long time to fail the first time
  - Good to remember that they don’t work
  - ... so the failure takes less time the next time around

- But: negative caching is optional
  - And not widely implemented
Reliability

- DNS servers are replicated (primary/secondary)
  - Name service available if at least one replica is up
  - Queries can be load-balanced between replicas
- Usually, UDP used for queries
  - Need reliability: must implement this on top of UDP
  - Spec supports TCP too, but not always implemented
- Try alternate servers on timeout
  - Exponential backoff when retrying same server
- Same identifier for all queries
  - Don’t care which server responds

DNS Measurements (MIT data from 2000)

- What is being looked up?
  - ~60% requests for A records
  - ~25% for PTR records
  - ~5% for MX records
  - ~6% for ANY records
- How long does it take?
  - Median ~100msec (but 90th percentile ~500msec)
  - 80% have no referrals; 99.9% have fewer than four
- Query packets per lookup: ~2.4
  - But this is misleading....

DNS Measurements (MIT data from 2000)

- Does DNS give answers?
  - ~23% of lookups fail to elicit an answer!
  - ~13% of lookups result in NXDOMAIN (or similar)
    - Mostly reverse lookups
    - Only ~64% of queries are successful!
      - How come the web seems to work so well?
- ~63% of DNS packets in unanswered queries!
  - Failing queries are frequently retransmitted
  - 99.9% successful queries have ≤2 retransmissions

DNS Measurements (MIT data from 2000)

- Top 10% of names accounted for ~70% of lookups
  - Caching should really help!
- 9% of lookups are unique
  - Cache hit rate can never exceed 91%
- Cache hit rates ~75%
  - But caching for more than 10 hosts doesn’t add much

A Common Pattern.....

- Distributions of various metrics (file lengths, access patterns, etc.) often have two properties:
  - Large fraction of total metric in the top 10%
  - Sizable fraction (~10%) of total fraction in low values
- Not an exponential distribution
  - Large fraction is in top 10%
  - But low values have very little of overall total
- Lesson: have to pay attention to both ends of dist.
  - Here: caching helps, but not a panacea

Moral of the Story

- If you design a highly resilient system, many things can be going wrong without you noticing it!
and this is a good thing
Cache Poisoning, an old badness example

- Suppose you are a Bad Guy and you control the name server forfoobar.com. You receive a request to resolve www.foobar.com and reply:

```plaintext
; QUESTION SECTION: 

; ANSWER SECTION: 
www.foobar.com. 300 IN A 212.44.9.144

; AUTHORITY SECTION: 

; ADDITIONAL SECTION: 
google.com. IN A 212.44.9.155
```

Evidence of the attack disappears 5 seconds later!

A foobar.com machine, not google.com

Why is the web so successful?

- What do the web, youtube, facebook, tumblr, twitter, flickr, …… have in common?
  - The ability to self-publish
- Self-publishing that is easy, independent, free
- No interest in collaborative and idealistic endeavor
  - People aren’t looking for Nirvana (or even Xanadu)
  - People also aren’t looking for technical perfection
- Want to make their mark, and find something neat
  - Two sides of the same coin, creates synergy
  - “Performance” more important than dialogue……

DNS and Security

- No way to verify answers
  - Opens up DNS to many potential attacks
  - DNSSEC fixes this
- Most obvious vulnerability: recursive resolution
  - Using recursive resolution, host must trust DNS server
  - When at Starbucks, server is under their control
  - And can return whatever values it wants
- More subtle attack: Cache poisoning
  - Those “additional” records can be anything!

Web Components

- Infrastructure:
  - Clients
  - Servers
  - Proxies
- Content:
  - Individual objects (files, etc.)
  - Web sites (coherent collection of objects)
- Implementation
  - HTML: formatting content
  - URL: naming content
  - HTTP: protocol for exchanging content
    Any content not just HTML!

HTML: HyperText Markup Language

- A Web page has:
  - Base HTML file
  - Referenced objects (e.g., images)
- HTML has several functions:
  - Format text
  - Reference images
  - Embed hyperlinks (HREF)

URL Syntax

```
protocol : //hostname/:port//directorypath/resource
```

- protocol: http, ftp, https, smtp, rtsp, etc.
- hostname: DNS name, IP address
- port: Defaults to protocol’s standard port e.g. http: 80, https: 443
- directory path: Hierarchical, reflecting file system
- resource: Identifies the desired resource

Can also extend to program executions:
```
http://us.e413.yahoo.com/yj/ShowLetter?box=4
Or408u&screenid=2461_1744106_29609_1223_1261_0_289
17.3052_123997?10&message=showed=2D48c&a=order=
Aheadout?datagptView=sahheadz.
```
HyperText Transfer Protocol (HTTP)

- Request-response protocol
- Reliance on a global namespace
- Resource metadata
- Stateless
- ASCII format

Steps in HTTP Request

- HTTP Client initiates TCP connection to server
  - SYN
  - SYNACK
  - ACK
- Client sends HTTP request to server
  - Can be piggybacked on TCP's ACK
- HTTP Server responds to request
- Client receives the request, terminates connection
  TCP connection termination exchange
  How many RTTs for a single request?

Client-Server Communication

- two types of HTTP messages: request, response
- HTTP request message: (GET POST HEAD ...)
- HTTP response message

```
GET /www.cl.cam.ac.uk 80
GET ~/awm22/win HTTP/1.0
<blank line, i.e., CRLF>
```

HTTP Resource Meta-Data

- Meta-data
  - Info about a resource, stored as a separate entity
- Examples:
  - Size of resource, last modification time, type of content
- Usage example: Conditional GET Request
  - If unchanged, "HTTP/1.1 304 Not Modified"
  - No body in the server’s response, only a header

HTTP is Stateless

- Each request-response treated independently
  - Servers not required to retain state
- Good: Improves scalability on the server-side
  - Failure handling is easier
  - Can handle higher rate of requests
  - Order of requests doesn’t matter
- Bad: Some applications need persistent state
  - Need to uniquely identify user or store temporary info
    - e.g., Shopping cart, user profiles, usage tracking, ...

Different Forms of Server Response

- Return a file
  - URL matches a file (e.g., /www/index.html)
  - Server returns file as the response
  - Server generates appropriate response header
- Generate response dynamically
  - URL triggers a program on the server
  - Server runs program and sends output to client
- Return meta-data with no body
State in a Stateless Protocol:
Cookies
- Client-side state maintenance
  - Client stores small state on behalf of server
  - Client sends state in future requests to the server
- Can provide authentication
  
  ![Cookies Diagram]

HTTP Performance
- Most Web pages have multiple objects
  - e.g., HTML file and a bunch of embedded images
- How do you retrieve those objects (naively)?
  - One item at a time
- Put stuff in the optimal place?
  - Where is that precisely?
    - Enter the Web cache and the CDN

Fetch HTTP Items: Stop & Wait

![Stop & Wait Diagram]

Concurrent Requests & Responses
- Use multiple connections in parallel
- Does not necessarily maintain order of responses
  - Client =
  - Server =
  - Network = Why?

Pipelined Requests & Responses
- Batch requests and responses
  - Reduce connection overhead
  - Multiple requests sent in a single batch
  - Maintains order of responses
  - Item 1 always arrives before item 2
- How is this different from concurrent requests/responses?
  - Single TCP connection

Persistent Connections
- Enables multiple transfers per connection
  - Maintain TCP connection across multiple requests
  - Including transfers subsequent to current page
  - Client or server can tear down connection
- Performance advantages:
  - Avoid overhead of connection set-up and tear-down
  - Allow TCP to learn more accurate RTT estimate
  - Allow TCP congestion window to increase
    - i.e., leverage previously discovered bandwidth
- Default in HTTP/1.1
HTTP evolution

• 1.0 – one object per TCP: simple but slow
• Parallel connections - multiple TCP, one object each: wastes b/w, may be svr limited, out of order
• 1.1 pipelining – aggregate retrieval time: ordered, multiple objects sharing single TCP
• 1.1 persistent – aggregate TCP overhead: lower overhead in time, increase overhead at ends (e.g., when should/do you close the connection?)

Scorecard: Getting n Small Objects

Time dominated by latency

• One-at-a-time: ~2n RTT
• Persistent: ~ (n+1)RTT
• M concurrent: ~2[n/m] RTT
• Pipelined: ~2 RTT
• Pipelined/Persistent: ~2 RTT first time, RTT later

Scorecard: Getting n Large Objects

Time dominated by bandwidth

• One-at-a-time: ~ nF/B
• M concurrent: ~ [n/m] F/B
  – assuming shared with large population of users
• Pipelined and/or persistent: ~ nF/B
  – The only thing that helps is getting more bandwidth..

Improving HTTP Performance: Caching

• Many clients transfer same information
  – Generates redundant server and network load
  – Clients experience unnecessary latency

Improving HTTP Performance: Caching: How

• Modifier to GET requests:
  – If-modified-since – returns “not modified” if resource not modified since specified time
• Response header:
  – Expires – how long it’s safe to cache the resource
  – No-cache – ignore all caches; always get resource directly from server

Improving HTTP Performance: Caching: Why

• Motive for placing content closer to client:
  – User gets better response time
  – Content providers get happier users
  – Network gets reduced load
• Why does caching work?
  – Exploits locality of reference
• How well does caching work?
  – Very well, up to a limit
  – Large overlap in content
  – But many unique requests
Example: Conditional GET Request

- Return resource only if it has changed at the server
- Save server resources!

GET /~awm22/win HTTP/1.1
Host: www.cl.cam.ac.uk
User-Agent: Mozilla/4.03
If-Modified-Since: Sun, 27 Aug 2006 22:25:50 GMT

- Client specifies "if-modified-since" time in request
- Server compares this against "last modified" time of desired resource
- Server returns "304 Not Modified" if resource has not changed
- ... or a "200 OK" with the latest version otherwise

Cache documents close to server

- Typically done by content providers
- Only works for static(*) content
  (*) static can also be snapshots of dynamic content

Caching with Reverse Proxies

Cache documents close to clients

- Typically done by ISPs or corporate LANs
- Integrate forward and reverse caching functionality
  - One overlay network (usually) administered by one entity
    - e.g., Akamai
  - Provide document caching
    - Pull: Direct result of clients’ requests
    - Push: Expectation of high access rate
  - Also do some processing
    - Handle dynamic web pages
    - Transcoding
    - Maybe do some security function – watermark IP

Caching with Forward Proxies

- Akamai creates new domain names for each client content provider.
  - e.g., a128.g.akamai.net
- The CDN’s DNS servers are authoritative for the new domains
- The client content provider modifies its content so that embedded URLs reference the new domains.
  - “Akamaize” content
    - e.g.: http://www.bbc.co.uk/popular-image.jpg becomes
      http://a128.g.akamai.net/popular-image.jpg
- Requests now sent to CDN’s infrastructure...

Caching w/ Content Distribution Networks

CDN Example – Akamai
Hosting: Multiple Sites Per Machine

- Multiple Web sites on a single machine
  - Hosting company runs the Web server on behalf of multiple sites (e.g., www.foo.com and www.bar.com)
- Problem: GET /index.html
- Solutions:
  - Multiple server processes on the same machine
    - Have a separate IP address (or port) for each server
  - Include site name in HTTP request
    - Single Web server process with a single IP address
    - Client includes "Host" header (e.g., Host: www.foo.com)
  - Required header with HTTP/1.1

Hosting: Multiple Machines Per Site

- Replicate popular Web site across many machines
  - Helps to handle the load
  - Places content closer to clients
- Helps when content isn’t cacheable
- Problem: Want to direct client to particular replica
  - Balance load across server replicas
  - Pair clients with nearby servers

Multi-Hosting at Single Location

- Single IP address, multiple machines
  - Run multiple machines behind a single IP address
  - Ensure all packets from a single TCP connection go to the same replica

CDN examples round-up

- CDN using DNS
  - DNS has information on loading/distribution/location
- CDN using anycast
  - Same address from DNS name but local routes
- CDN based on rewriting HTML URLs
  - (akami example just covered – akami uses DNS too)

Multi-Hosting at Several Locations

- Multiple addresses, multiple machines
  - Same name but different addresses for all of the replicas
  - Configure DNS server to return closest address

SIP – Session Initiation Protocol

Session?
Anyone smell an OSI / ISO standards document burning?
SIP - VoIP

Establishing communication through SIP proxies.

SIP?

- SIP – bringing the fun/complexity of telephony to the Internet
  - User location
  - User availability
  - User capabilities
  - Session setup
  - Session management
    - (e.g. “call forwarding”)

H.323 – ITU

- Why have one standard when there are at least two....
- The full H.323 is hundreds of pages
  - The protocol is known for its complexity – an ITU hallmark
- SIP is not much better
  - IETF grew up and became the ITU....

Multimedia Applications

Message flow for a basic SIP session

The (still?) missing piece:
Resource Allocation for Multimedia Applications

I can ‘differentiate’ VoIP from data but...
I can only control data going into the Internet

Multimedia Applications

- Resource Allocation for Multimedia Applications

Admission control using session control protocol.
Resource Allocation for Multimedia Applications

So where does it happen?
Inside single institutions or domains of control...
(Universities, Hospitals, big corp...)

What about my ADSL/CABLE/etc. It combines voice and data?
Phone company controls the multiplexing on the line and throughout their own network too....

Co-ordination of SIP signaling and resource reservation.

Pure P2P architecture

• no always-on server
• arbitrary end systems directly communicate
• peers are intermittently connected and change IP addresses

Three topics:
- File distribution
- Searching for information
- Case Study: Skype

File Distribution: Server-Client vs P2P

Question: How much time to distribute file from one server to N peers?

File distribution time: server-client

- server sequentially sends N copies:
  - \(NF/u_s\) time
- client i takes \(F/d_i\) time to download

Time to distribute \(F\) to \(N\) clients using client/server approach:

\[d_{s,N} = \max\left\{NF/u_s, F/min(d_i)\right\}\]

Increases linearly in \(N\) (for large \(N\))

File distribution time: P2P

- server must send one copy: \(F/u_s\) time
- client i takes \(F/d_i\) time to download
- \(NF\) bits must be downloaded (aggregate)
- fastest possible upload rate: \(u_i = \sum u_i\)

\[d_{P2P} = \max\left\{F/u_s, F/min(d_i), NF/\left(u_i + \sum u_i\right)\right\}\]
Server-client vs. P2P: example

Client upload rate = \( u \), \( f/u = 1 \) hour, \( u = 10u \), \( d_{\text{min}} \geq u \)

File distribution: BitTorrent*

*rather old BitTorrent

BitTorrent (1)

- file divided into 256KB chunks.
- peer joining torrent:
  - has no chunks, but will accumulate them over time
  - registers with tracker to get list of peers, connects to subset of peers ("neighbors")
- while downloading, peer uploads chunks to other peers.
- peers may come and go
- once peer has entire file, it may (selfishly) leave or (altruistically) remain

BitTorrent (2)

- at any given time, different peers have different subsets of file chunks
- periodically, a peer (Alice) asks each neighbor for list of chunks that they have.
- Alice sends requests for her missing chunks
  - rarest first

Pulling Chunks

Sending Chunks: tit-for-tat

- Alice sends chunks to four neighbors currently sending her chunks at the highest rate
- re-evaluate top 4 every 10 secs
- every 30 secs: randomly select another peer, starts sending chunks
- newly chosen peer may join top 4
- "optimistically unchoke"

Distributed Hash Table (DHT)

- DHT = distributed P2P database
- Database has (key, value) pairs;
  - key: ss number; value: human name
  - key: content type; value: IP address
- Peers query DB with key
  - DB returns values that match the key
- Peers can also insert (key, value) peers

BitTorrent: Tit-for-tat

(1) Alice "optimistically unchokes" Bob
(2) Alice becomes one of Bob ’s top-four providers; Bob reciprocates
(3) Bob becomes one of Alice ’s top-four providers

With higher upload rate, can find better trading partners & get file faster!
**Distributed Hash Table (DHT)**

- DHT = distributed P2P database
- Database has (key, value) pairs;
  - key: ss number; value: human name
  - key: content type; value: IP address
- Peers query DB with key
  - DB returns values that match the key
- Peers can also insert (key, value) peers

**DHT Identifiers**

- Assign integer identifier to each peer in range [0,2^n-1].
  - Each identifier can be represented by n bits.
- Require each key to be an integer in same range.
- To get integer keys, hash original key.
  - eg, key = h("Game of Thrones season 4")
  - This is why they call it a distributed "hash" table

**How to assign keys to peers?**

- Central issue:
  - Assigning (key, value) pairs to peers.
- Rule: assign key to the peer that has the closest ID.
- Convention in lecture: closest is the immediate successor of the key.
- Ex: n=4; peers: 1,3,4,5,8,10,12,14;
  - key = 13, then successor peer = 14
  - key = 15, then successor peer = 1

**Circular DHT (1)**

- Each peer only aware of immediate successor and predecessor.
- “Overlay network”

**Circle DHT (2)**

- Define closest as closest successor

**Circular DHT with Shortcuts**

- Each peer keeps track of IP addresses of predecessor, successor, short cuts.
- Reduced from 6 to 2 messages.
- Possible to design shortcuts so O(log N) neighbors, O(log N) messages in query
Peer Churn

• Peer 5 abruptly leaves
• Peer 4 detects; makes 8 its immediate successor; asks 8 who its immediate successor is; makes 8’s immediate successor its second successor.
• What if peer 13 wants to join?

To handle peer churn, require each peer to know the IP address of its two successors.
• Each peer periodically pings its two successors to see if they are still alive.

P2P Case study: Skype (pre-Microsoft)

• inherently P2P: pairs of users communicate.
• proprietary application-layer protocol (inferred via reverse engineering)
• hierarchical overlay with SNs
• Index maps usernames to IP addresses; distributed over SNs

Peers as relays

• Problem when both Alice and Bob are behind “NATs”.
  – NAT prevents an outside peer from initiating a call to insider peer
• Solution:
  – Using Alice’s and Bob’s SNs, Relay is chosen
  – Each peer initiates session with relay
  – Peers can now communicate through NATs via relay

Summary.

• Apps need protocols too
• We covered examples from
  – Traditional Applications (web)
  – Scaling and Speeding the web (CDN/Cache tricks)
• Infrastructure Services (DNS)
  – Cache and Hierarchy
• Multimedia Applications (SIP)
  – Extremely hard to do better than worst-effort
• P2P Network examples
Topic 7: Datacenters

What we will cover

• Characteristics of a datacenter environment  
  – goals, constraints, workloads, etc.
• How and why DC networks are different (vs. WAN)  
  – e.g., latency, geo, autonomy, ...
• How traditional solutions fare in this environment  
  – e.g., IP, Ethernet, TCP, ARP, DHCP
• Not details of how datacenter networks operate

Disclaimer

• Material is emerging (not established) wisdom
• Material is incomplete  
  – many details on how and why datacenter networks operate aren’t public

Why Datacenters?

Your <public-life, private-life, banks, government> live in my datacenter.

Security, Privacy, Control, Cost, Energy, (breaking) received wisdom; all this and more come together into sharp focus in datacenters.

Do I need to labor the point?

What goes into a datacenter (network)?

• Servers organized in racks

What goes into a datacenter (network)?

• Servers organized in racks
• Each rack has a ‘Top of Rack’ (ToR) switch
What goes into a datacenter (network)?

- Servers organized in racks
- Each rack has a ‘Top of Rack’ (ToR) switch
- An ‘aggregation fabric’ interconnects ToR switches

Example 1

Brocade reference design

Example 2

Cisco reference design

Observations on DC architecture

- Regular, well-defined arrangement
- Hierarchical structure with rack/aggr/core layers
- Mostly homogenous within a layer
- Supports communication between servers and between servers and the external world

Contrast: ad-hoc structure, heterogeneity of WANs

What’s new?
SCALE!

How big exactly?

• 1M servers [Microsoft]
  → less than google, more than amazon

• > $1B to build one site [Facebook]

• > $20M/month/site operational costs [Microsoft '09]

But only O(10-100) sites

What’s new?

• Scale
• Service model
  → user-facing, revenue generating services
  → multi-tenancy
  → jargon: SaaS, PaaS, DaaS, IaaS, ...

Implications

• Scale
  → need scalable solutions (duh)
  → improving efficiency, lowering cost is critical
  → "scale out" solutions w/ commodity technologies

• Service model
  → performance means $$
  → virtualization for isolation and portability

Multi-Tier Applications

• Applications decomposed into tasks
  → Many separate components
  → Running in parallel on different machines

Componentization leads to different types of network traffic

• "North-South traffic"
  → Traffic between external clients and the datacenter
  → Handled by front-end (web) servers, mid-tier application servers, and back-end databases
  → Traffic patterns fairly stable, though diurnal variations
Componentization leads to different types of network traffic

- **“North-South traffic”**
  - Traffic between external clients and the datacenter
  - Handled by front-end (web) servers, mid-tier application servers, and back-end databases
  - Traffic patterns fairly stable, though diurnal variations

- **“East-West traffic”**
  - Traffic between machines in the datacenter
  - Comm within “big data” computations (e.g., Map Reduce)
  - Traffic may shift on small timescales (e.g., minutes)
What’s different about DC networks?

Characteristics
• Huge scale:
  – ~20,000 switches/routers
  – contrast: AT&T ~500 routers

What’s different about DC networks?

Characteristics
• Huge scale:
  • Limited geographic scope:
  – High bandwidth: 10/40/100G
  – Contrast: Cable/DSL/WiFi
  – Very low RTT: 10s of microseconds
  – Contrast: 100s of milliseconds in the WAN

What’s different about DC networks?

Characteristics
• Huge scale
• Limited geographic scope
• Single administrative domain
  – Can deviate from standards, invent your own, etc.
  – “Green field” deployment is still feasible

What’s different about DC networks?

Characteristics
• Huge scale
• Limited geographic scope
• Single administrative domain
• Control over one/both endpoints
  – can change (say) addressing, congestion control, etc.
  – can add mechanisms for security/policy/etc. at the endpoints (typically in the hypervisor)

What’s different about DC networks?

Characteristics
• Huge scale
• Limited geographic scope
• Single administrative domain
• Control over one/both endpoints
• Control over the placement of traffic source/sink
  – e.g., map-reduce scheduler chooses where tasks run
  – alters traffic pattern (what traffic crosses which links)

What’s different about DC networks?

Characteristics
• Huge scale
• Limited geographic scope
• Single administrative domain
• Control over one/both endpoints
• Control over the placement of traffic source/sink
• Regular/planned topologies (e.g., trees/fat-trees)
  – Contrast: ad-hoc WAN topologies (dictated by real-world geography and facilities)
What’s different about DC networks?

**Characteristics**
- Huge scale
- Limited geographic scope
- Single administrative domain
- Control over one/both endpoints
- Control over the placement of traffic source/sink
- Regular/planned topologies (e.g., trees/fat-trees)
- Limited heterogeneity
  - link speeds, technologies, latencies, ...

**Goals**
- Extreme bisection bandwidth requirements
  - recall: all that east-west traffic
  - target: any server can communicate at its full link speed
  - problem: server’s access link is 10Gbps!

Full Bisection Bandwidth

A “Scale Out” Design

- Build multi-stage ‘Fat Trees’ out of k-port switches
  - k/2 ports up, k/2 down
  - Supports k^3/4 hosts:
    - 48 ports, 27,648 hosts

Full Bisection Bandwidth Not Sufficient

- To realize full bisectional throughput, routing must spread traffic across paths
- Enter load-balanced routing
  - How? (1) Let the network split traffic/flows at random (e.g., ECMP protocol -- RFC 2991/2992)
  - How? (2) Centralized flow scheduling?
  - Many more research proposals

Goals
- Extreme bisection bandwidth requirements
- Extreme latency requirements
  - real money on the line
  - current target: 1μs RTTs
  - how? cut-through switches making a comeback
    - reduces switching time
What’s different about DC networks?

Goals
- Extreme bisection bandwidth requirements
- Extreme latency requirements
  - real money on the line
  - current target: 1μs RTTs
  - how? cut-through switches making a comeback
  - how? avoid congestion
    • reduces queuing delay

An example problem at scale - INCAST

The Incast Workload

Incast Workload Overfills Buffers

Queue Buildup

- Big flows buildup queues.
  ➢ Increased latency for short flows.

- Measurements in Bing cluster
  ➢ For 90% packets: RTT < 1ms
  ➢ For 10% packets: 1ms < RTT < 15ms
Link-Layer Flow Control
Common between switches but this is flow-control to the end host too...

- Another idea to reduce incast is to employ Link-Layer Flow Control......

Recall: the Data-Link can use specially coded symbols in the coding to say “Stop” and “Start”

Link Layer Flow Control
But its worse that you imagine....

What’s different about DC networks?

**Goals**
- Extreme bisection bandwidth requirements
- Extreme latency requirements
- Predictable, deterministic performance
  - “your packet will reach in Xms, or not at all”
  - “your VM will always see at least YGbps throughput”
  - Resurrecting ‘best effort’ vs. ‘Quality of Service’ debates
  - How is still an open question

What’s different about DC networks?

**Goals**
- Extreme bisection bandwidth requirements
- Extreme latency requirements
- Predictable, deterministic performance
- Differentiating between tenants is key
  - e.g., “No traffic between VMs of tenant A and tenant B”
  - “Tenant X cannot consume more than XGbps”
  - “Tenant Y’s traffic is low priority”

What’s different about DC networks?

**Goals**
- Extreme bisection bandwidth requirements
- Extreme latency requirements
- Predictable, deterministic performance
- Differentiating between tenants is key
- Scalability (of course)
  - Q: How’s that Ethernet spanning tree looking?
What’s different about DC networks?

**Goals**
- Extreme bisection bandwidth requirements
- Extreme latency requirements
- *Predictable, deterministic performance*
- Differentiating between tenants is key
- Scalability (of course)
- Cost/efficiency
  - focus on commodity solutions, ease of management
  - some debate over the importance in the network case

**Summary**
- new characteristics and goals
- some liberating, some constraining
- scalability is the baseline requirement
- more emphasis on performance
- less emphasis on heterogeneity
- less emphasis on interoperability

---

Computer Networking UROP
- Assessed Practicals for Computer Networking.
  - so supervisors can set/use work
  - so we can have a Computer Networking tick
    *running over summer 2017*

*Talk to me.*

Part 2 projects for 17-18
- Fancy doing something at scale or speed?

*Talk to me.*
Computer Networking

Michaelmas/Lent Term
M/W/F 11:00-12:00
LT1 in Gates Building

Slide Set 2

Andrew W. Moore
andrew.moore@cl.cam.ac.uk
2016-2017
Topic 2 – Architecture and Philosophy

- Abstraction
- Layering
- Layers and Communications
- Entities and Peers
- What is a protocol?
- Protocol Standardization
- The architects process
  - How to break system into modules
  - Where modules are implemented
  - Where is state stored
- Internet Philosophy and Tensions

Abstraction Concept

A mechanism for breaking down a problem

- *what not how*
- eg Specification versus implementation
- eg Modules in programs
- Allows replacement of implementations without affecting system behavior

*Vertical versus Horizontal*

“Vertical” what happens in a box “How does it attach to the network?”
“Horizontal” the communications paths running through the system

Hint: paths are build on top of (“layered over”) other paths

Computer System Modularity

Partition system into modules & abstractions:

- Well-defined interfaces give flexibility
  - *Hides* implementation - can be freely changed
  - Extend functionality of system by adding new modules
- E.g., libraries encapsulating set of functionality
- E.g., programming language + compiler
  abstracts away how the particular CPU works …

Computer System Modularity (cnt’ d)

- Well-defined interfaces hide information
  - Isolate assumptions
  - Present high-level abstractions
- But can impair performance!
- Ease of implementation vs worse performance

Network System Modularity

Like software modularity, but:

- Implementation is distributed across many machines (routers and hosts)
- Must decide:
  - How to break system into modules
    - *Layering*
  - Where modules are implemented
    - *End-to-End Principle*
  - Where state is stored
    - *Fate-sharing*

Layering Concept

- A restricted form of abstraction: system functions are divided into layers, one built upon another
- Often called a *stack;* but not a data structure!
Layers and Communications

- Interaction only between adjacent layers
- Layer $n$ uses services provided by layer $n-1$
- Layer $n$ provides service to layer $n+1$
- Bottom layer is physical media
- Top layer is application

Entities and Peers

*Entity – a thing (an independent existence)*

Entities *interact* with the layers above and below

Entities *communicate* with peer entities

- same level but different place (eg different person, different box, different host)

Communications between peers is supported by entities at the lower layers

Entities and Peers

Entities usually do something useful

- Encryption – Error correction – Reliable Delivery
- Nothing at all is also reasonable

Not all communications is end-to-end

Examples for things in the middle

- IP Router – Mobile Phone Cell Tower
- Person translating French to English

Layering and Embedding

In Computer Networks we often see higher-layer information embedded within lower-layer information

- Such embedding can be considered a form of layering
- Higher layer information is generated by stripping off headers and trailers of the current layer
- Eg an IP entity only looks at the IP headers

*BUT* embedding is not the only form of layering

Layering is to help understand a communications system

*NOT* determine implementation strategy

Distributing Layers Across Network

- Layers are simple if only on a single machine
  - Just stack of modules interacting with those above/below
- But we need to implement layers across machines
  - Hosts
  - Routers (switches)
- What gets implemented where?
**What Gets Implemented on Host?**

- Bits arrive on wire, must make it up to application
- Therefore, all layers must exist at the host's source/destination

**What Gets Implemented on a Router?**

- Bits arrive on wire
  - Physical layer necessary
- Packets must be delivered to next-hop
  - Datalink layer necessary
- Routers participate in global delivery
  - Network layer necessary
- Routers don’t support reliable delivery
  - Transport layer (and above) not supported

**What Gets Implemented on Switches?**

- Switches do what routers do, except they don’t participate in global delivery, just local delivery
- They only need to support Physical and Datalink
  - Don’t need to support Network layer
- Won’t focus on the router/switch distinction
  - When I say switch, I almost always mean router
  - Almost all boxes support network layer these days
  - Routers have switches but switches do not have routers

**The Internet Hourglass**

There is just one network-layer protocol, **IP**.

The “narrow waist” facilitates interoperability.

**Internet protocol stack versus OSI Reference Model**

- **OSI Reference Model**
  - Application
  - Presentation
  - Session
  - Transport
  - Network
  - Data Link
  - Physical
- **Internet Protocol stack**
  - Application
  - Transport
  - Network
  - Data Link
  - Physical

**ISO/OSI reference model**

- **presentation**: allow applications to interpret meaning of data, e.g., encryption, compression, machinespecific conventions
- **session**: synchronization, checkpointing, recovery of data exchange
- Internet stack “missing” these layers!
  - These services, if needed, must be implemented in application
  - Needed?
What is a protocol?

**human protocols:**
- “what’s the time?”
- “I have a question”
- introductions

**network protocols:**
- machines rather than humans
- all communication activity in Internet governed by protocols

protocols define format, order of msgs sent and received among network entities, and actions taken on msg transmission, receipt

What is a protocol?

a human protocol and a computer network protocol:

<table>
<thead>
<tr>
<th>Protocol Standardization</th>
</tr>
</thead>
<tbody>
<tr>
<td>All hosts must follow same protocol</td>
</tr>
<tr>
<td>- Very small modifications can make a big difference</td>
</tr>
<tr>
<td>- Or prevent it from working altogether</td>
</tr>
<tr>
<td>- Cisco bug compatible!</td>
</tr>
<tr>
<td>This is why we have standards</td>
</tr>
<tr>
<td>- Can have multiple implementations of protocol</td>
</tr>
<tr>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>- Based on working groups that focus on specific issues</td>
</tr>
<tr>
<td>- Produces “Request For Comments” (RFCs)</td>
</tr>
<tr>
<td>- IETF Web site is <a href="http://www.ietf.org">http://www.ietf.org</a></td>
</tr>
<tr>
<td>- RFCs archived at <a href="http://www.rfc-editor.org">http://www.rfc-editor.org</a></td>
</tr>
</tbody>
</table>

So many Standards Problem

- Many different packet-switching networks
- Each with its own Protocol
- Only nodes on the same network could communicate

INTERnet Solution

Alternative to Standardization?

- Have one implementation used by everyone
- Open-source projects
  - Which has had more impact, Linux or POSIX?
- Or just sole-sourced implementation
  - Skype, many P2P implementations, etc.
A Multitude of Apps Problem

- Re-implement every application for every technology?
- No! But how does the Internet design avoid this?

Solution: Intermediate Layers

- Introduce intermediate layers that provide a set of abstractions for various network functionality and technologies
  - A new app/media implemented only once
  - Variation on “add another level of indirection”

Remember that slide!

- The relationship between architectural principles and architectural decisions is crucial to understand

Internet Design Goals (Clark ‘88)

- Connect existing networks
- Robust in face of failures
- Support multiple types of delivery services
- Accommodate a variety of networks
- Allow distributed management
- Easy host attachment
- Cost effective
- Allow resource accountability

Real Goals

- Build something that works!
- Connect existing networks
- Robust in face of failures
- Support multiple types of delivery services
- Accommodate a variety of networks
- Allow distributed management
- Easy host attachment
- Cost effective
- Allow resource accountability

Internet Motto

We reject kings, presidents, and voting. We believe in rough consensus and running code.” – David Clark

In the context of the Internet
Three Observations

- Each layer:
  - Depends on layer below
  - Supports layer above
  - Independent of others
- Multiple versions in layer
  - Interfaces differ somewhat
  - Components pick which lower-level protocol to use
- But only one IP layer
  - Unifying protocol

Layering Crucial to Internet’s Success

- Reuse
- Hides underlying detail
- Innovation at each level can proceed in parallel
- Pursued by very different communities

What are some of the drawbacks of protocols and layering?

- Layer N may duplicate lower layer functionality
  – e.g., error recovery to retransmit lost data
- Information hiding may hurt performance
  – e.g., packet loss due to corruption vs. congestion
- Headers start to get really big
  – e.g., typical TCP+IP+Ethernet is 54 bytes
- Layer violations when the gains too great to resist
  – e.g., TCP-over-wireless
- Layer violations when network doesn’t trust ends
  – e.g., firewalls

Placing Network Functionality

- Hugely influential paper: “End-to-End Arguments in System Design” by Saltzer, Reed, and Clark (’84)
  – articulated as the “End-to-End Principle” (E2E)
- Endless debate over what it means
- Everyone cites it as supporting their position (regardless of the position!)

Basic Observation

- Some application requirements can only be correctly implemented end-to-end
  – reliability, security, etc.
- Implementing these in the network is hard
  – every step along the way must be fail proof
- Hosts
  – Can satisfy the requirement without network’s help
  – Will/must do so, since they can’t rely on the network
Example: Reliable File Transfer

- Solution 1: make each step reliable, and string them together to make reliable end-to-end process
- Solution 2: end-to-end check and retry

Discussion

- Solution 1 is incomplete
  - What happens if any network element misbehaves?
  - Receiver has to do the check anyway!

- Solution 2 is complete
  - Full functionality can be entirely implemented at application layer with no need for reliability from lower layers

- Is there any need to implement reliability at lower layers?

Summary of End-to-End Principle

- Implementing functionality (e.g., reliability) in the network
  - Doesn’t reduce host implementation complexity
  - Does increase network complexity
  - Probably increases delay and overhead on all applications even if they don’t need the functionality (e.g., VoIP)

- However, implementing in the network can improve performance in some cases
  - e.g., consider a very lossy link

“Only-if-Sufficient” Interpretation

- Don’t implement a function at the lower levels of the system unless it can be completely implemented at this level

  Unless you can relieve the burden from hosts, don’t bother

“Only-if-Necessary” Interpretation

- Don’t implement anything in the network that can be implemented correctly by the hosts

- Make network layer absolutely minimal
  - This E2E interpretation trumps performance issues
  - Increases flexibility, since lower layers stay simple

“Only-if-Useful” Interpretation

- If hosts can implement functionality correctly, implement it in a lower layer only as a performance enhancement

- But do so only if it does not impose burden on applications that do not require that functionality
We have some tools:

- Abstraction
- Layering
- Layers and Communications
- Entities and Peers
- Protocol as motivation
- Examples of the architects process
- Internet Philosophy and Tensions
**Topic 3: The Data Link Layer**

**Our goals:**
- understand principles behind data link layer services:
  - error detection, correction
  - sharing a broadcast channel: multiple access
  - link layer addressing
  - reliable data transfer, flow control:
- instantiation and implementation of various link layer technologies
  - Wired Ethernet (aka 802.3)
  - Wireless Ethernet (aka 802.11 WiFi)
- Algorithms
  - Binary Exponential Backoff
  - Spanning Tree

**Link Layer: Introduction**

**Some terminology:**
- hosts and routers are nodes
- communication channels that connect adjacent nodes along communication path are links
  - wired links
  - wireless links
  - LANs
- layer-2 packet is a frame, encapsulates datagram

**data-link layer** has responsibility of transferring datagram from one node to adjacent node over a link

---

**Link Layer (Channel) Services**

- **framing, link access:**
  - encapsulate datagram into frame, adding header, trailer
  - channel access if shared medium
  - "MAC" addresses used in frame headers to identify source, dest
    - different from IP address!
- **reliable delivery between adjacent nodes**
  - we see some of this again in the Transport Topic
  - seldom used on low bit-error link (fiber, some twisted pair)
  - wireless links: high error rates
- **Q:** why both link-level and end-end reliability?

**Link Layer (Channel) Services - 2**

- **flow control:**
  - pacing between adjacent sending and receiving nodes
- **error detection:**
  - errors caused by signal attenuation, noise.
  - receiver detects presence of errors:
    - signals sender for retransmission or drops frame
- **error correction:**
  - receiver identifies and corrects bit error(s) without resorting to retransmission
- **half-duplex and full-duplex**
  - with half duplex, nodes at both ends of link can transmit, but not at same time

---

**Where is the link layer implemented?**

- in each and every host
- link layer implemented in "adapter" (aka network interface card NIC)
  - Ethernet card, PCMCIA card, 802.11 card
  - implements link, physical layer
- attaches into host’s system buses
- combination of hardware, software, firmware

**Adaptors Communicating**

- **sending side:**
  - encapsulates datagram in frame
  - encodes data for the physical layer
  - adds error checking bits, provide reliability, flow control, etc.

- **receiving side:**
  - decodes data from the physical layer
  - looks for errors, provides reliability, flow control, etc.
  - extracts datagram, passes to upper layer at receiving side
Coding – a channel function
Change the representation of data.

Given Data

Encoding

Changed Data

Decoding

1. Encryption: MyPasswd <-> AA$$ff
2. Error Detection: AA$$ff <-> AA$$fff
3. Compression: AA$$fff <-> A2$4
4. Analog: A2$4 <-> 10

Non-Return-to-Zero (NRZ)

Non-Return-to-Zero-Mark (NRZM) 1 = transition 0 = no transition

Non-Return-to-Zero Inverted (NRZI) (note transitions on the 1)

Clock

Line Coding Examples
Non-Return-to-Zero (NRZ) [Baud = bit-rate]

Clock

Manchester example (Baud = 2 x bit-rate)

Clock

Quad-level code (2 x Baud = bit-rate)

Line Coding – Block Code example

Data to send

Non-Return-to-Zero (NRZ)

Non-Return-to-Zero-Mark (NRZM) 1 = transition 0 = no transition

Non-Return-to-Zero Inverted (NRZI) (note transitions on the 1)

Clock

Manchester example (Baud = 2 x bit-rate)

Clock

Quad-level code (2 x Baud = bit-rate)

Line (Wire) representation

Block coding transfers data with a fixed overhead: 20% less information per Baud in the case of 4b/5b

So to send data at 100Mbps; the line rate (the Baud rate) must be 125Mbps.

1Gbps uses an 8b/10b codec; encoding entire bytes at a time but with 25% overhead

Data to send

Line Coding Examples

Non-Return-to-Zero (NRZ)

Non-Return-to-Zero-Mark (NRZM) 1 = transition 0 = no transition

Non-Return-to-Zero Inverted (NRZI) (note transitions on the 1)

Clock

Manchester example (Baud = 2 x bit-rate)

Clock

Quad-level code (2 x Baud = bit-rate)

Line (Wire) representation

Block coding transfers data with a fixed overhead: 20% less information per Baud in the case of 4b/5b

So to send data at 100Mbps; the line rate (the Baud rate) must be 125Mbps.

1Gbps uses an 8b/10b codec; encoding entire bytes at a time but with 25% overhead
Line Coding Scrambling – with secrecy

Step 1
Scrambling Sequence
Communications Channel
Message
Message XOR Sequence

Step 2
Scrambling Sequence
Message
Message XOR Sequence

Step 3
Don’t ever reuse Scrambling sequence, ever. <<< this is quite important.

Line Coding Scrambling—no secrecy

Scrambling Sequence
Communications Channel
Message
Message XOR Sequence

Scrambling Sequence
Communications Channel
Message
Message XOR Sequence

Example (Self-synchronizing) scrambler

δ δ δ δ

Inserted bits marking “start of frame/block/sequence”

Identify (and remove) “start of frame/block/sequence”
This gives you the Byte-delinations for free.

FDMA

frequency

time

TDMA

frequency

time

Multiple Access Mechanisms

Each dimension is orthogonal (so may be trivially combined)?
There are other dimensions too, can you think of them?

66b/66b combines a scrambler and a frame. The start of frame is a pair of bits 01 or 10: 01 means “this frame is data,” 10 means “this frame contains data and control” – control could be configuration information, length of encoded data or simply “this line is idle” (no data at all).
Code Division Multiple Access (CDMA) (not to be confused with CSMA!)

- used in several wireless broadcast channels (cellular, satellite, etc) standards
- unique “code” assigned to each user; i.e., code set partitioning
- all users share same frequency, but each user has own “chipping” sequence (i.e., code) to encode data
- **encoded signal** = (original data) XOR (chipping sequence)
- **decoding:** inner-product of encoded signal and chipping sequence
- allows multiple users to “coexist” and transmit simultaneously with minimal interference (if codes are “orthogonal”)

**CDMA Encode/Decode**

- Each sender adds a unique code
- Each receiver removes its unique code

**CDMA: two-sender interference**

**Coding Examples summary**

- Common Wired coding
  - Block codecs: table-lookups
  - fixed overhead, inline control signals
  - Scramblers: shift registers
    - overhead free

Like earlier coding schemes and error correction/detection; you can combine these
  - e.g., 10Gb/s Ethernet may use a hybrid

**CDMA (Code Division Multiple Access)**

- coping intelligently with competing sources
- Mobile phones

**Error Detection and Correction**

- **Basic Idea:**
  1. Add additional information to a message.
  2. Detect an error and re-send a message.
  Or, fix an error in the received message.
How to use coding to deal with errors in data communication?

Basic Idea:
1. Add additional information to a message.
2. Detect an error and re-send a message.
   Or, fix an error in the received message.

Error Detection and Correction

Error Detection

EDC = Error Detection and Correction bits (redundancy = overhead)
D = Data protected by error checking, may include header fields

- Error detection not 100% reliable!
- Protocol may miss some errors, but rarely
- Larger EDC field yields better detection and correction

Error Detection Code

Sender:
\[ Y = \text{generateCheckBit}(X); \]
\[ \text{send}(XY); \]

Receiver:
\[ \text{receive}(X1Y1); \]
\[ Y2 = \text{generateCheckBit}(X1); \]
\[ \text{if}(Y1 \neq Y2) \text{ERROR}; \]
\[ \text{else NOERROR}. \]

Error Detection Code: Parity

Add one bit, such that the number of 1's is even.

Parity Checking

Single Bit Parity:
Detect single bit errors

Two Dimensional Bit Parity:
Detect and correct single bit errors

Internet checksum

Goal: detect "errors" (e.g., flipped bits) in transmitted packet
(note: used at transport layer only)

Sender:
- treat segment contents as sequence of 1-bit integers
- checksum: addition (1's complement sum) of segment contents
- sender puts checksum value into UDP checksum field

Receiver:
- compute checksum of received segment
- check if computed checksum equals checksum field value:
  - NO - error detected
  - YES - no error detected. But maybe errors nonetheless?
Error Detection Code: CRC

- CRC means “Cyclic Redundancy Check”.
- More powerful than parity.
  - It can detect various kinds of errors, including 2-bit errors.
- More complex: multiplication, binary division.
- Parameterized by n-bit divisor $P$.
  - Example: 3-bit divisor 101.
  - Choosing good $P$ is crucial.

CRC with 3-bit Divisor 101

The divisor ($P$) – Secret sauce of CRC

- If the divisor were 100, instead of 101, data 1111 and 1001 would give the same check bit 00.
- Mathematical analysis about the divisor:
  - Last bit should be 1.
  - Should contain at least two 1’s.
  - Should be divisible by 11.
- ATM, HDLC, Ethernet each use a CRC with well-chosen fixed divisors

Divisor analysis keeps mathematicians in jobs
(a branch of pure math: combinatorial mathematics)

Checksumming: Cyclic Redundancy Check recap

- view data bits, $D$, as a binary number
- choose $r+1$ bit pattern (generator), $P$
- goal: choose $r$ CRC bits, $R$, such that
  - $<D, R>$ exactly divisible by $G$ (modulo 2)
  - receiver knows $G$, divides $<D, R>$ by $G$. If non-zero remainder: error detected!
  - can detect all burst errors less than $r+1$ bits
- widely used in practice (Ethernet, 802.11 WiFi, ATM)

CRC Another Example – this time with long division

Want:
$D \cdot 2^r \text{ XOR } R = nP$

equivalently:
$D \cdot 2^r = nP \text{ XOR } R$
equivalently:
if we divide $D \cdot 2^r$ by $P$, want remainder $R$

$R = \text{remainder}(\frac{D \cdot 2^r}{P})$

Error Detection Code becomes….

Sender:
$Y = \text{generateCheckBit}(X)$;
$\text{send}(XY)$;

Receiver:
receive($X1Y1$);
$Y2=\text{generateCheckBit}(X1)$;
if ($Y1 \neq Y2$) ERROR;
else NOERROR
Forward Error Correction (FEC)

Sender:
\[ Y = \text{generateCheckBit}(X); \]
\[ \text{send}(XY); \]

Receiver:
\[ \text{receive}(X1Y1); \]
\[ Y2=\text{generateCheckBit}(X1); \]
\[ \text{if} \ (Y1 \neq Y2) \ \text{FIXERROR}(X1Y1); \]
\[ \text{else} \ \text{NOERROR} \]

Error Detection vs Correction

Error Correction:
- Cons: More check bits. False recovery.
- Pros: No need to re-send.

Error Detection:
- Cons: Need to re-send.
- Pros: Less check bits.

Usage:
- Correction: A lot of noise. Expensive to re-send.
- Detection: Less noise. Easy to re-send.
- Can be used together.

Basic Idea of Forward Error Correction

Replace erroneous data by its “closest” error-free data.

Multiple Access Links and Protocols

Two types of “links”:
- point-to-point
  - point-to-point link between Ethernet switch and host
- broadcast (shared wire or medium)
  - old-fashioned wired Ethernet (here be dinosaurs – extinct)
  - upstream HFC (Hybrid Fiber-Coax – the Coax may be broadcast)
  - Home plug / Powerline networking
  - 802.11 wireless LAN

Multiple Access protocols

- single shared broadcast channel
- two or more simultaneous transmissions by nodes: interference
  - collision if node receives two or more signals at the same time
- distributed algorithm that determines how nodes share channel, i.e., determine when node can transmit
- communication about channel sharing must use channel itself!
  - no out-of-band channel for coordination
Ideal Multiple Access Protocol

Broadcast channel of rate $R$ bps
1. when one node wants to transmit, it can send at rate $R$
2. when $M$ nodes want to transmit, each can send at average rate $R/M$
3. fully decentralized:
   - no special node to coordinate transmissions
   - no synchronization of clocks, slots
4. simple

MAC Protocols: a taxonomy

Three broad classes:
- **Channel Partitioning**
  - divide channel into smaller “pieces” (time slots, frequency, code)
  - allocate piece to node for exclusive use
- **Random Access**
  - channel not divided, allow collisions
  - “recover” from collisions
- **“Taking turns”**
  - nodes take turns, but nodes with more to send can take longer turns

Channel Partitioning MAC protocols: TDMA
(time travel warning – we mentioned this earlier)

**TDMA:** time division multiple access
- access to channel in “rounds”
- each station gets fixed length slot (length = pkt trans time) in each round
- unused slots go idle
- example: station LAN, 1,3,4 have pkt, slots 2,5,6 idle

Channel Partitioning MAC protocols: FDMA
(time travel warning – we mentioned this earlier)

**FDMA:** frequency division multiple access
- channel spectrum divided into frequency bands
- each station assigned fixed frequency band
- unused transmission time in frequency bands go idle
- example: station LAN, 1,3,4 have pkt, frequency bands 2,5,6 idle

“Taking Turns” MAC protocols

channel partitioning MAC protocols:
- share channel efficiently and fairly at high load
- inefficient at low load: delay in channel access, 1/N bandwidth allocated even if only 1 active node!
Random access MAC protocols
- efficient at low load: single node can fully utilize channel
- high load: collision overhead
“taking turns” protocols
look for best of both worlds!
Random Access MAC Protocols

- When node has packet to send
  - Transmit at full channel data rate
  - No a priori coordination among nodes
- Two or more transmitting nodes ⇒ collision
  - Data lost
- Random access MAC protocol specifies:
  - How to detect collisions
  - How to recover from collisions
- Examples
  - ALOHA and Slotted ALOHA
  - CSMA, CSMA/CD, CSMA/CA (wireless)

Key Ideas of Random Access

- Carrier sense
  - Listen before speaking, and don’t interrupt
  - Checking if someone else is already sending data
  - … and waiting till the other node is done
- Collision detection
  - If someone else starts talking at the same time, stop
  - Realizing when two nodes are transmitting at once
  - … by detecting that the data on the wire is garbled
- Randomness
  - Don’t start talking again right away
  - Waiting for a random time before trying again

CSMA (Carrier Sense Multiple Access)

- CSMA: listen before transmit
  - If channel sensed idle: transmit entire frame
  - If channel sensed busy, defer transmission
- Human analogy: don’t interrupt others!
- Does this eliminate all collisions?
  - No, because of nonzero propagation delay

CSMA Collisions

Propagation delay: two nodes may not hear each other’s before sending.

Would slots hurt or help?

CSMA reduces but does not eliminate collisions

Biggest remaining problem?

Collisions still take full slot!

How do you fix that?
CSMA/CD (Collision Detection)

- **CSMA/CD:** carrier sensing, deferral as in CSMA
  - Collisions detected within short time
  - Colliding transmissions aborted, reducing wastage
- Collision detection easy in wired LANs:
  - Compare transmitted, received signals
- Collision detection difficult in wireless LANs:
  - Reception shut off while transmitting (well, perhaps not)
  - Not perfect broadcast (limited range) so collisions local
  - Leads to use of collision avoidance instead (later)

Limits on CSMA/CD Network Length

- Latency depends on physical length of link
  - Time to propagate a packet from one end to the other
- Suppose A sends a packet at time $t$
  - And B sees an idle line at a time just before $t + d$
  - ... so B happily starts transmitting a packet
- B detects a collision, and sends jamming signal
  - But A can’t see collision until $t + 2d$

Performance of CSMA/CD

- Time wasted in collisions
  - Proportional to distance $d$
- Time spend transmitting a packet
  - Packet length $p$ divided by bandwidth $b$
- Rough estimate for efficiency ($K$ some constant)
  \[
  E \approx \frac{p}{\frac{p}{b} + Kd}
  \]
  - Note:
    - For large packets, small distances, $E \sim 1$
    - As bandwidth increases, $E$ decreases
    - That is why high-speed LANs are all switched

Benefits of Ethernet

- Easy to administer and maintain
- Inexpensive
- Increasingly higher speed
- Evolvable!

Evolution of Ethernet

- Changed **everything** except the frame **format**
  - From single coaxial cable to hub-based star
  - From shared media to **switches**
  - From electrical signaling to optical
- **Lesson #1**
  - The right interface can accommodate many changes
  - Implementation is hidden behind interface
- **Lesson #2**
  - Really hard to displace the dominant technology
  - Slight performance improvements are not enough
Ethernet: CSMA/CD Protocol

- **Carrier sense**: wait for link to be idle
- **Collision detection**: listen while transmitting
  - No collision: transmission is complete
  - Collision: abort transmission & send jam signal
- **Random access**: binary exponential back-off
  - After collision, wait a random time before trying again
  - After m\textsuperscript{th} collision, choose K randomly from \{0, …, 2\textsuperscript{m-1}\}
  - … and wait for K*512 bit times before trying again
    - Using min packet size as “slot”
    - If transmission occurring when ready to send, wait until end of transmission (CSMA)

The Wireless Spectrum

Metrics for evaluation / comparison of wireless technologies

- Bitrate or Bandwidth
- Range - PAN, LAN, MAN, WAN
- Two-way / One-way
- Multi-Access / Point-to-Point
- Digital / Analog
- Applications and industries
- Frequency – Affects most physical properties:
  - Distance (free-space loss)
  - Penetration, Reflection, Absorption
  - Energy proportionality
  - Policy: Licensed / Deregulated
  - Line of Sight (Fresnel zone)
  - Size of antenna

- Determined by wavelength – \( \lambda = \frac{V}{f} \)

Wireless Communication Standards

- **Cellular (800/900/1700/1800/1900MHz)**:
  - 2G: GSM / CDMA / GPRS / EDGE
  - 3G: CDMA2000 / UMTS / HSDPA / EVDO
  - 4G: LTE, WiMax
- **IEEE 802.11 (aka WiFi)**:
  - b: 2.4GHz band, 11Mbps (~4.5 Mbps operating rate)
  - g: 2.4GHz, 54-108Mbps (~19 Mbps operating rate)
  - a: 5.0GHz band, 54-108Mbps (~25 Mbps operating rate)
  - n: 2.4/5GHz, 150-600Mbps (4x4 mimo).
- **IEEE 802.15** – lower power wireless:
  - 802.15.1: 2.4GHz, 2.1 Mbps (Bluetooth)
  - 802.15.4: 2.4GHz, 250 Kbps (Sensor Networks)

What Makes Wireless Different?

- Broadcast and multi-access medium...
  - err, so….
- BUT, Signals sent by sender don’t always end up at receiver intact
  - Complicated physics involved, which we won’t discuss
  - But what can go wrong?

Path Loss / Path Attenuation

- **Free Space Path Loss**: \( \text{FSPL} = \left( \frac{4 \pi d}{\lambda} \right)^2 \)
  \( d = \text{distance} \)
  \( \lambda = \text{wave length} \)
  \( f = \text{frequency} \)
  \( c = \text{speed of light} \)
- Reflection, Diffraction, Absorption
- Terrain contours (Urban, Rural, Vegetation).
- Humidity
Multipath Effects

- Signals bounce off surface and interfere with one another
- Self-interference

Interference from Other Sources

- External Interference
  - Microwave is turned on and blocks your signal
  - Would that affect the sender or the receiver?
- Internal Interference
  - Hosts within range of each other collide with one another’s transmission
  - We have to tolerate path loss, multipath, etc., but we can try to avoid internal interference

Wireless Bit Errors

- The lower the SNR (Signal/Noise) the higher the Bit Error Rate (BER)
- We could make the signal stronger...
- Why is this not always a good idea?
  - Increased signal strength requires more power
  - Increases the interference range of the sender, so you interfere with more nodes around you
    - And then they increase their power......
- Local link-layer Error Correction schemes can correct some problems

Let's focus on 802.11
aka - WiFi ...
What makes it special?

Deregulation > Innovation > Adoption > Lower cost = Ubiquitous technology

JUST LIKE ETHERNET – not lovely but sufficient

802.11 Architecture

- Designed for limited area
- AP’s (Access Points) set to specific channel
- Broadcast beacon messages with SSID (Service Set Identifier) and MAC Address periodically
- Hosts scan all the channels to discover the AP’s
  - Host associates with AP

Wireless Multiple Access Technique?

- Carrier Sense?
  - Sender can listen before sending
  - What does that tell the sender?
- Collision Detection?
  - Where do collisions occur?
  - How can you detect them?
Hidden Terminals

- A and C can both send to B but can’t hear each other
  - A is a hidden terminal for C and vice versa
- Carrier Sense will be ineffective

Exposed Terminals

- Exposed node: B sends a packet to A; C hears this and decides not to send a packet to D (despite the fact that this will not cause interference)
- Carrier sense would prevent a successful transmission.

Key Points

- No concept of a global collision
  - Different receivers hear different signals
  - Different senders reach different receivers
- Collisions are at receiver, not sender
  - Only care if receiver can hear the sender clearly
  - It does not matter if sender can hear someone else
  - As long as that signal does not interfere with receiver
- Goal of protocol:
  - Detect if receiver can hear sender
  - Tell senders who might interfere with receiver to shut up

Basic Collision Avoidance

- Since can’t detect collisions, we try to avoid them
- Carrier sense:
  - When medium busy, choose random interval
  - Wait that many idle timeslots to pass before sending
- When a collision is inferred, retransmit with binary exponential backoff (like Ethernet)
  - Use ACK from receiver to infer “no collision”
  - Use exponential backoff to adapt contention window

CSMA/CA - MA with Collision Avoidance

- Before every data transmission
  - Sender sends a Request to Send (RTS) frame containing the length of the transmission
  - Receiver respond with a Clear to Send (CTS) frame
  - Sender sends data
  - Receiver sends an ACK; now another sender can send data
- When sender doesn’t get a CTS back, it assumes collision

CSMA/CA, con’t

- If other nodes hear RTS, but not CTS: send
  - Presumably, destination for first sender is out of node’s range ...
CSMA/CA, con’t

If other nodes hear RTS, but not CTS: **send**
- Presumably, destination for first sender is out of node’s range...
- ...Can cause problems when a CTS is **lost**

When you hear a CTS, you keep quiet until scheduled transmission is over (hear ACK)

---

Preventing Collisions Altogether

- Frequency Spectrum partitioned into several channels
  - Nodes within interference range can use separate channels
  - Now A and C can send without any interference!
- Most cards have only 1 transceiver
  - Not Full Duplex: Cannot send and receive at the same time
  - Aggregate Network throughput doubles

---

CSMA/CD vs CSMA/CA (without RTS/CTS)

**CD** Collision Detect
- wired – listen and talk
1. Listen for others
3. Send message (and listen)
4. Collision?
   a. JAM
   b. increase your BEB
   c. sleep
   d. goto 1.

**CA** Collision Avoidance
- wireless – talk OR listen
1. Listen for others
2. Busy?
   a. increase your BEB
   b. sleep
   c. goto 1.
3. Send message
4. Wait for ACK (MAC ACK)
5. Got No ACK from MAC?
   a. increase your BEB
   b. sleep
   c. goto 1.

---

Changing the rules: an 802.11 feature

**Rate Adaptation**
(for a variety of out-of-context reasons often unused)

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies
- 1. SNR decreases, BER increases as node moves away from base station
2. When BER becomes too high, switch to lower transmission rate but with lower BER

---

RTS / CTS Protocols (CSMA/CA)

B sends to C

Overcome hidden terminal problems with contention-free protocol
1. B sends to C *Request To Send (RTS)*
2. A hears RTS and defers (to allow C to answer)
3. C replies to B with *Clear To Send (CTS)*
4. D hears CTS and defers to allow the data
5. B sends to C
Summary of MAC protocols

- **channel partitioning**, by time, frequency or code
  - Time Division, Frequency Division
- **random access** (dynamic),
  - ALOHA, S-ALOHA, CSMA, CSMA/CD
  - carrier sensing: easy in some technologies (wire), hard in others (wireless)
  - CSMA/CD used in Ethernet
  - CSMA/CA used in 802.11
- **taking turns**
  - polling from central site, token passing
  - Bluetooth, FDDI, IBM Token Ring

MAC Addresses

- **MAC** (or **LAN** or **physical** or **Ethernet**) address:
  - function: *get frame from one interface to another physically-connected interface* (same network)
  - 48 bit MAC address (for most LANs)
    - *burned* in NIC ROM, nowadays usually software settable and set at boot time
- **LAN Address** (more)
  - MAC address allocation administered by IEEE
  - manufacturer buys portion of MAC address space (to assure uniqueness)
  - analogy:
    - (a) MAC address: like Social Security Number
    - (b) IP address: like postal address
  - MAC flat address ➔ portability
    - can move LAN card from one LAN to another
  - IP hierarchical address NOT portable
    - address depends on IP subnet to which node is attached

Hubs

...physical-layer (“dumb”) repeaters:
- bits coming in one link go out all other links at same rate
- all nodes connected to hub can collide with one another
- no frame buffering
- no CSMA/CD at hub: host NICs detect collisions

Switch

(like a Hub but smarter)

- link-layer device: smarter than hubs, take active role
  - store, forward Ethernet frames
  - examine incoming frame’s MAC address, selectively forward frame to one-or-more outgoing links when frame is to be forwarded on segment, uses CSMA/CD to access segment
- transparent
  - hosts are unaware of presence of switches
- plug-and-play, self-learning
  - switches do not need to be configured
Switch: allows multiple simultaneous transmissions

- hosts have dedicated, direct connection to switch
- switches buffer packets
- Ethernet protocol used on each incoming link, but no collisions; full duplex
  - each link is its own collision domain
- switching: A-to-A' and B-to-B' simultaneously, without collisions
  - not possible with dumb hub

Switching: A to A' and B to B'

Switch Table

- Q: how does switch know that A' reachable via interface 4, B' reachable via interface 5?
- A: each switch has a switch table, each entry:
  - (MAC address of host, interface to reach host, time stamp)
  - looks like a routing table!
- Q: how are entries created, maintained in switch table?
  - something like a routing protocol?

Switch: self-learning (recap)

- switch learns which hosts can be reached through which interfaces
  - when frame received, switch "learns" location of sender:
    incoming LAN segment
  - records sender/location pair in switch table

Switch: frame filtering/forwarding

When frame received:

1. record link associated with sending host
2. index switch table using MAC dest address
3. if entry found for destination
   then
     - if dest on segment from which frame arrived:
       drop the frame
     else forward the frame on interface indicated
   else flood

Switch: frame filtering/forwarding

Interconnecting switches

- switches can be connected together

Q: sending from A to G - how does S1 know to forward frame destined to F via S5 and S7?
A: self learning! (works exactly the same as in single-switch case – flood/forward/drop)
Flooding Can Lead to Loops
- Flooding can lead to **forwarding loops**
  - E.g., if the network contains a cycle of switches
    - "Broadcast storm"

```
+-----------------+-----------------+
|                  | Flooding        |
|                  | can lead to     |
|                  | forwarding loops |
|                  |                  |
```

**Solution: Spanning Trees**
- Ensure the forwarding **topology** has no loops
  - Avoid using some of the links when flooding
  - … to prevent loop from forming
- **Spanning tree**
  - Sub-graph that covers all vertices but **contains no cycles**
  - Links not in the spanning tree do not forward frames

```
+-----------------+-----------------+
|                  |                  |
|                  | Graph Has Cycles! |
|                  |                  |
```

**What Do We Know?**
- Shortest paths to (or from) a node form a tree
- So, algorithm has two aspects:
  - Pick a root
  - Compute shortest paths to it
- Only keep the links on shortest-path

```
+-----------------+-----------------+
|                  |                  |
|                  | Graph Has No Cycles! |
|                  |                  |
```

**Constructing a Spanning Tree**
- Switches need to **elect a root**
  - The switch w/ smallest identifier (MAC addr)
- Each switch determines if each interface is on the shortest path from the root
  - Excludes it from the tree if not
- Messages (Y, d, X)
  - From node X
  - Proposing Y as the root
  - And the distance is d

```
+-----------------+-----------------+
|                  |                  |
|                  | root             |
|                  | One hop          |
|                  | Three hops 3     |
```

**Steps in Spanning Tree Algorithm**
- Initially, each switch proposes itself as the root
  - Switch sends a message out every interface
  - … proposing itself as the root with distance 0
  - Example: switch X announces (X, 0, X)
- Switches update their view of the root
  - Upon receiving message (Y, d, Z) from Z, check Y’s id
  - If new id smaller, start viewing that switch as root
- Switches compute their distance from the root
  - Add 1 to the distance received from a neighbor
  - Identify interfaces not on shortest path to the root
  - … and exclude them from the spanning tree
- If root or shortest distance to it changed, "flood" updated message (Y, d+1, X)

```
+-----------------+-----------------+
|                  |                  |
|                  |                  |
```

**Example From Switch #4’s Viewpoint**
- Switch #4 thinks it is the root
  - Sends (4, 0, 4) message to 2 and 7
- Then, switch #4 hears from #2
  - Receives (2, 0, 2) message from 2
  - … and thinks that #2 is the root
  - And realizes it is just one hop away
- Then, switch #4 hears from #7
  - Receives (2, 1, 7) from 7
  - And realizes this is a longer path
  - So, prefers its own one-hop path
  - And removes 4-7 link from the tree

```
+-----------------+-----------------+
|                  |                  |
|                  |                  |
```

```
+-----------------+-----------------+
|                  |                  |
|                  |                  |
```

```
+-----------------+-----------------+
|                  |                  |
|                  |                  |
```
Example From Switch #4’s Viewpoint

- Switch #2 hears about switch #1
  - Switch 2 hears (1, 1, 3) from 3
  - Switch 2 starts treating 1 as root
  - And sends (1, 2, 2) to neighbors
- Switch #4 hears from switch #2
  - Switch 4 starts treating 1 as root
  - And sends (1, 3, 4) to neighbors
- Switch #4 hears from switch #7
  - Switch 4 receives (1, 3, 7) from 7
  - And realizes this is a longer path
  - So, prefers its own three-hop path
  - And removes 4-7 link from the tree

Robust Spanning Tree Algorithm

- Algorithm must react to failures
  - Failure of the root node
    - Need to elect a new root, with the next lowest identifier
    - Failure of other switches and links
      - Need to recompute the spanning tree
  - Root switch continues sending messages
    - Periodically reannouncing itself as the root (1, 0, 1)
    - Other switches continue forwarding messages
  - Detecting failures through timeout (soft state)
    - If no word from root, times out and claims to be the root
    - Delay in reestablishing spanning tree is major problem
  - Work on rapid spanning tree algorithms...

---

Topic 3: Summary

- principles behind data link layer services:
  - error detection, correction
  - sharing a broadcast channel: multiple access
  - link layer addressing
- instantiation and implementation of various link layer technologies
  - Ethernet
  - switched LANs
  - WiFi
- algorithms
  - Binary Exponential Backoff
  - Spanning Tree
**Topic 4: Network Layer**

**Our goals:**
- understand principles behind network layer services:
  - network layer service models
  - forwarding versus routing (versus switching)
  - how a router works
  - routing (path selection)
  - IPv6
- For the most part, the Internet is our example – again.

**Name:** a *something*

**Address:** Where a *something* is

**Routing:** How do I get to the *something*

**Addressing (at a conceptual level)**
- Assume all hosts have unique IDs
- No particular structure to those IDs
- Later in topic I will talk about real IP addressing
- Do I route on location or identifier?
- If a host moves, should its address change?
  - If not, how can you build scalable Internet?
  - If so, then what good is an address for identification?

**Packets (at a conceptual level)**
- Assume packet headers contain:
  - Source ID, Destination ID, and perhaps other information

**Switches/Routers**
- Multiple ports (attached to other switches or hosts)
- Ports are typically duplex (incoming and outgoing)

**A Variety of Networks**
- ISPs: carriers
  - Backbone
  - Edge
  - Border (to other ISPs)
- Enterprises: companies, universities
  - Core
  - Edge
  - Border (to outside)
- Datacenters: massive collections of machines
  - Top-of-Rack
  - Aggregation and Core
  - Border (to outside)
Switches forward packets

Forwarding Decisions
- When packet arrives...
  - Must decide which outgoing port to use
  - In single transmission time
  - Forwarding decisions must be simple
- Routing state dictates where to forward packets
  - Assume decisions are deterministic
- Global routing state means collection of routing state in each of the routers
  - Will focus on where this routing state comes from
  - But first, a few preliminaries....

Forwarding vs Routing
- Forwarding: “data plane”
  - Directing a data packet to an outgoing link
  - Individual router using routing state
- Routing: “control plane”
  - Computing paths the packets will follow
  - Routers talking amongst themselves
  - Jointly creating the routing state
- Two very different timescales....

Router definitions
- \( N \) = number of external router “ports”
- \( R \) = speed (“line rate”) of a port
- Router capacity = \( N \times R \)

Networks and routers

Examples of routers (core)
Cisco CRS
- \( R = 10/40/100 \) Gbps
- \( NR = 922 \) Tbps
- Netflix: 0.7GB per hour (1.5Mb/s)
- ~600 million concurrent Netflix users

72 racks, >1MW
Examples of routers (edge)

Cisco ASR
- $R=1/10/40$ Gbps
- $NR = 120$ Gbps

Examples of routers (small business)

Cisco 3945E
- $R = 10/100/1000$ Mbps
- $NR < 10$ Gbps

What’s inside a router?

Processes packets on their way in

Processes packets before they leave

Transfers packets from input to output ports

Input and Output for the same port are on one physical linecard

Constitutes the data plane

Constitutes the control plane

Linecards (input)
1
2
•
•
N

Linecards (output)
1
2
•
•
N

Linecard
s
(input)

Interconnect
(Switching)
Fabric

Route/Control
Processor

Linecard
s
(output)

(1) Implement IGP and BGP protocols; compute routing tables

(2) Push forwarding tables to the line cards

Context+and+Terminology

“End hosts”
“Clients”, “Users”
“End points”

“Border Routers”

“Autonomous System (AS)” or “Domain”
Region of a network under a single administrative entity

“Interior Routers”

“Route” or “Path”
Routing Protocols

- Routing protocols implement the core function of a network
  - Establish paths between nodes
  - Part of the network’s “control plane”

- Network modeled as a graph
  - Routers are graph vertices
  - Links are edges
  - Edges have an associated “cost”
    - e.g., distance, loss

- Goal: compute a “good” path from source to destination
  - “good” usually means the shortest (least cost) path

Internet Routing

- Internet Routing works at two levels

- Each AS runs an intra-domain routing protocol that establishes routes within its domain
  - (AS – region of network under a single administrative entity)
  - Link State, e.g., Open Shortest Path First (OSPF)
  - Distance Vector, e.g., Routing Information Protocol (RIP)

- ASes participate in an inter-domain routing protocol that establishes routes between domains
  - Path Vector, e.g., Border Gateway Protocol (BGP)

Addressing (for now)

- Assume each host has a unique ID (address)

- No particular structure to those IDs

- Later in course will talk about real IP addressing

Outline

- Link State
- Distance Vector
- Routing: goals and metrics (if time)
Link State Routing

- Each node maintains its local "link state" (LS)
  - i.e., a list of its directly attached links and their costs

Dijkstra’s Shortest Path Algorithm

- INPUT:
  - Network topology (graph), with link costs

- OUTPUT:
  - Least cost paths from one node to all other nodes

- Iterative: after $k$ iterations, a node knows the least cost path to its $k$ closest neighbors

Example

Notation

- $c(i,j)$: link cost from node $i$ to $j$; cost is infinite if not direct neighbors; $\geq 0$

- $D(v)$: total cost of the current least cost path from source to destination $v$

- $p(v)$: $v$'s predecessor along path from source to $v$

- $S$: set of nodes whose least cost path definitively known
**Dijkstra’s Algorithm**

1. **Initialization:**
   - Set $S = \{A\}$.
   - For all nodes $v$,
     - If $v$ adjacent to $A$,
       - Then $D(v) = c(A,v)$.
     - Else $D(v) = \infty$.

2. **Loop**
   - Find $w$ not in $S$ such that $D(w)$ is a minimum.
   - Add $w$ to $S$.
   - Update $D(v)$ for all $v$ adjacent to $w$ and not in $S$.
   - If $D(w) + c(w,v) < D(v)$ then
     - Update $D(v)$ with $D(v) = D(w) + c(w,v)$.
   - Else $D(v) = D(w)$.
   - For all nodes $v$,
     - Update $D(v)$ for all $v$ adjacent to $w$ and not in $S$.
   - Repeat until all nodes in $S$.

**Example:**

- **Initialization:**
  - Set $S = \{A\}$.
  - For all nodes $v$,
    - If $v$ adjacent to $A$,
      - Then $D(v) = c(A,v)$.
    - Else $D(v) = \infty$.

- **Loop**
  - Find $w$ not in $S$ such that $D(w)$ is a minimum.
  - Add $w$ to $S$.
  - Update $D(v)$ for all $v$ adjacent to $w$ and not in $S$.
  - If $D(w) + c(w,v) < D(v)$ then
    - Update $D(v)$ with $D(v) = D(w) + c(w,v)$.
  - Else $D(v) = D(w)$.
  - For all nodes $v$,
    - Update $D(v)$ for all $v$ adjacent to $w$ and not in $S$.
  - Repeat until all nodes in $S$.
Example: Dijkstra’s Algorithm

Step | set S | D(B),p(B) | D(C),p(C) | D(D),p(D) | D(E),p(E) | D(F),p(F)
--- | --- | --- | --- | --- | --- | ---
0 | A | 2,A | 5,A | 1,A | 5,A | 5,A
1 | AD | A | 4,D | 2,D | 2,D | 2,D
2 | ADE | 3,E | 4,E | 4,E | 4,E | 4,E
3 | ADEB | ADEB | ADEB | ADEB | ADEB | ADEB
4 | ADEBCDF | ADEBCDF | ADEBCDF | ADEBCDF | ADEBCDF | ADEBCDF

To determine path A → C (say), work backward from C via p(v)

The Forwarding Table
- Running Dijkstra at node A gives the shortest path from A to all destinations
- We then construct the forwarding table

<table>
<thead>
<tr>
<th>Destination</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>(A,B)</td>
</tr>
<tr>
<td>C</td>
<td>(A,D)</td>
</tr>
<tr>
<td>D</td>
<td>(A,D)</td>
</tr>
<tr>
<td>E</td>
<td>(A,D)</td>
</tr>
<tr>
<td>F</td>
<td>(A,D)</td>
</tr>
</tbody>
</table>

Issue #1: Scalability
- How many messages needed to flood link state messages?
  - O(N x E), where N is #nodes; E is #edges in graph
- Processing complexity for Dijkstra’s algorithm?
  - O(N^2), because we check all nodes w not in S at each iteration and we have O(N) iterations
  - more efficient implementations: O(N log(N))
- How many entries in the LS topology database? O(E)
- How many entries in the forwarding table? O(N)
**Issue#2: Transient Disruptions**

- Inconsistent link-state database
  - Some routers know about failure before others
  - The shortest paths are no longer consistent
  - Can cause transient forwarding loops

**Learn-By-Doing**

Let’s try to collectively develop distance-vector routing from first principles

**Experiment**

- Your job: find the (route to) the youngest person in the room
- **Ground Rules**
  - You may not leave your seat, nor shout loudly across the class
  - You may talk with your immediate neighbors (N-S-E-W only)
    (hint: "exchange updates" with them)
  - At the end of 5 minutes, I will pick a victim and ask:
    - who is the youngest person in the room? (date&name)
    - which one of your neighbors first told you this info.?
Example of Distributed Computation

Distance Vector Routing

• Each router knows the links to its neighbors
  – Does not flood this information to the whole network
• Each router has provisional “shortest path” to every other router
  – E.g.: Router A: “I can get to router B with cost 11”
• Routers exchange this distance vector information with their neighboring routers
  – Vector because one entry per destination
• Routers look over the set of options offered by their neighbors and select the best one
• Iterative process converges to set of shortest paths

A few other inconvenient truths

• What if we use a non-additive metric?
  – E.g., maximal capacity

• What if routers don’t use the same metric?
  – I want low delay, you want low loss rate?

• What happens if nodes lie?

Can You Use Any Metric?

• I said that we can pick any metric. Really?
• What about maximizing capacity?

What Happens Here?

Problem: “cost” does not change around loop

Additive measures avoid this problem!

No agreement on metrics?

• If the nodes choose their paths according to different criteria, then bad things might happen
• Example
  – Node A is minimizing latency
  – Node B is minimizing loss rate
  – Node C is minimizing price
• Any of those goals are fine, if globally adopted
  – Only a problem when nodes use different criteria
• Consider a routing algorithm where paths are described by delay, cost, loss
What Happens Here?

- Cares about price, then loss
- Low price link
- Low loss link
- Low delay link
- Cares about delay, then price
- Cares about loss, then delay

Must agree on loop-avoiding metric

- When all nodes minimize same metric
- And that metric increases around loops
- Then process is guaranteed to converge

What happens when routers lie?

- What if a router claims a 1-hop path to everywhere?
- All traffic from nearby routers gets sent there
- How can you tell if they are lying?
- Can this happen in real life?
  - It has, several times....

Link State vs. Distance Vector

- Core idea
  - LS: tell all nodes about your immediate neighbors
  - DV: tell your immediate neighbors about (your least cost distance to) all nodes

Link State vs. Distance Vector

- LS: each node learns the complete network map; each node computes shortest paths independently and in parallel
- DV: no node has the complete picture; nodes cooperate to compute shortest paths in a distributed manner

- LS has higher messaging overhead
- LS has higher processing complexity
- LS is less vulnerable to looping

Message complexity

- LS: $O(N^2 E)$ messages;
  - $N$ is number of nodes; $E$ is edges
- DV: $O(\text{#Iterations} \times E)$
  - where #Iterations is ideally $O(\text{network diameter})$ but varies due to routing loops or the count-to-infinity problem

Processing complexity

- LS: $O(N^2)$
- DV: $O(\text{#Iterations} \times N)$

Robustness: what happens if router malfunctions?

- LS:
  - node can advertise incorrect link cost
  - each node computes only its own table
- DV:
  - node can advertise incorrect path cost
  - each node’s table used by others; error propagates through network
Routing: Just the Beginning

- Link state and distance-vector are the deployed routing paradigms for intra-domain routing
- Inter-domain routing (BGP)
  - more Part II (Principles of Communications)
  - A version of DV

What are desirable goals for a routing solution?

- “Good” paths (least cost)
- Fast convergence after change/failures — no/rare loops
- Scalable
  - #messages
  - table size
  - processing complexity
- Secure
- Policy
- Rich metrics (more later)

Delivery models

- What if a node wants to send to more than one destination?
  - broadcast: send to all
  - multicast: send to all members of a group
  - anycast: send to any member of a group

- What if a node wants to send along more than one path?

Metrics

- Propagation delay
- Congestion
- Load balance
- Bandwidth (available, capacity, maximal, bbw)
- Price
- Reliability
- Loss rate
- Combinations of the above

In practice, operators set abstract “weights” (much like our costs); how exactly is a bit of a black art

From Routing back to Forwarding

- Routing: “control plane”
  - Computing paths the packets will follow
  - Routers talking amongst themselves
  - Jointly creating the routing state
- Forwarding: “data plane”
  - Directing a data packet to an outgoing link
  - Individual router using routing state
- Two very different timescales....

Basic Architectural Components of an IP Router
Per-packet processing in an IP Router
1. Accept packet arriving on an incoming link.
2. Lookup packet destination address in the forwarding table, to identify outgoing port(s).
3. Manipulate packet header: e.g., decrement TTL, update header checksum.
4. Send packet to the outgoing port(s).
5. Buffer packet in the queue.
6. Transmit packet onto outgoing link.

Generic Router Architecture

Forwarding tables
- Naive approach: One entry per address
  - Example: 4 billion entries
- Improved approach: Group entries to reduce table size
  - Example: 4 billion entries

IP addresses as a line

Longest Prefix Match (LPM)
Longest Prefix Match (LPM)

<table>
<thead>
<tr>
<th>Entry</th>
<th>Destination</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cambridge</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Oxford</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Europe</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>USA</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>Everywhere (default)</td>
<td>5</td>
</tr>
</tbody>
</table>

Matching entries:
- Europe
- Everywhere

To: France  
Data

Implementing Longest Prefix Match

<table>
<thead>
<tr>
<th>Entry</th>
<th>Destination</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cambridge</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Oxford</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Europe</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>USA</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>Everywhere (default)</td>
<td>5</td>
</tr>
</tbody>
</table>

Most specific

Least specific

Router Architecture Overview

Two key router functions:
- run routing algorithms/protocol (RIP, OSPF, BGP)
- forwarding datagrams from incoming to outgoing link

Switching Via Memory

First generation routers:
- traditional computers with switching under direct control of CPU
- packet copied to system’s memory
- speed limited by memory bandwidth (2 bus crossings per datagram)
Switching Via a Bus

- Datagram from input port memory to output port memory via a shared bus
- Bus contention: switching speed limited by bus bandwidth
- Lots of ports?? speed up the bus no contention bus speed = 2 x port speed x port count
- 32 Gbps bus, Cisco 5600: sufficient speed for access routers

Switching Via An Interconnection Network

- Overcome bus bandwidth limitations
- Banyan networks, other interconnection nets initially developed to connect processors in multiprocessor stages
- Advanced design: fragmenting datagram into fixed length cells, switch cells through the fabric.
- Cisco CRS-1: switches 1.2 Tbps through the interconnection network

Output Ports

- Buffering required when datagrams arrive from fabric faster than the transmission rate
- Scheduling discipline chooses among queued datagrams for transmission

Output port queueing

- Buffering when arrival rate via switch exceeds output line speed
- Queueing (delay) and loss due to output port buffer overflow!

Input Port Queuing

- Fabric slower than input ports combined -> queueing may occur at input queues
- Head-of-the-Line (HOL) blocking: queued datagram at front of queue prevents others in queue from moving forward
- Queueing delay and loss due to input buffer overflow!

Buffers in Routers

- So how large should the buffers be?

Buffer size matters

- End-to-end delay
  - Transmission, propagation, and queueing delay
  - The only variable part is queueing delay
- Router architecture
  - Board space, power consumption, and cost
  - On-chip buffers: higher density, higher cost
  - Optical buffers: all-optical routers

You are now touching the edge of the research zone……
Rule-of-thumb – Intuition

Rule for adjusting $W$
- If an ACK is received: $W ← W + 1/W$
- If a packet is lost: $W ← W/2$

Small Buffers – Intuition

Synchronized Flows
- Aggregate window has same dynamics
- Therefore buffer occupancy has same dynamics
- Rule-of-thumb still holds.

Many TCP Flows
- Independent, desynchronized
- Central limit theorem says the aggregate becomes Gaussian
- Variance (buffer size) decreases as $N$ increases
(Packet) Network Tasks One-by-One

- Read packet correctly
- Get packet to the destination
- Get responses to the packet back to source
- Carry data
- Tell host what to do with packet once arrived
- Specify any special network handling of the packet
- Deal with problems that arise along the path

Getting Packet to Destination and Back

- Two IP addresses
  - Source IP address (32 bits)
  - Destination IP address (32 bits)
- Destination address
  - Unique identifier/locator for the receiving host
  - Allows each node to make forwarding decisions
- Source address
  - Unique identifier/locator for the sending host
  - Recipient can decide whether to accept packet
  - Enables recipient to send a reply back to source

Telling Host How to Handle Packet

- Protocol (8 bits)
  - Identifies the higher-level protocol
  - Important for demultiplexing at receiving host
- Most common examples
  - E.g., “6” for the Transmission Control Protocol (TCP)
  - E.g., “17” for the User Datagram Protocol (UDP)

Special Handling

- Type-of-Service (8 bits)
  - Allow packets to be treated differently based on needs
  - E.g., low delay for audio, high bandwidth for bulk transfer
  - Has been redefined several times
- Options

Reading Packet Correctly

- Version number (4 bits)
  - Indicates the version of the IP protocol
  - Typically “4” (for IPv4), and sometimes “6” (for IPv6)
- Header length (4 bits)
  - Number of 32-bit words in the header
  - Typically “5” (for a 20-byte IPv4 header)
  - Can be more when IP options are used
- Total length (16 bits)
  - Number of bytes in the packet
  - Maximum size is 65,535 bytes (216 – 1)
  - … though underlying links may impose smaller limits

Potential Problems

- Header Corrupted: Checksum
- Loop: TTL
- Packet too large: Fragmentation
Header Corruption

• Checksum (16 bits)
  – Particular form of checksum over packet header

• If not correct, router discards packets
  – So it doesn’t act on bogus information

• Checksum recalculated at every router
  – Why?
  – Why include TTL?
  – Why only header?

Preventing Loops

(aka Internet Zombie plan)

• Forwarding loops cause packets to cycle forever
  – As these accumulate, eventually consume all capacity

• Time-to-Live (TTL) Field (8 bits)
  – Decremented at each hop, packet discarded if reaches 0
  – ...and “time exceeded” message is sent to the source
  • Using “ICMP” control message; basis for traceroute

Fragmentation

(some assembly required)

• Fragmentation: when forwarding a packet, an Internet router can split it into multiple pieces (“fragments”) if too big for next hop link

• Must reassemble to recover original packet
  – Need fragmentation information (32 bits)
  – Packet identifier, flags, and fragment offset

IP Fragmentation & Reassembly

• network links have MTU (max transfer size), largest possible link-level frame.
  – different link types, different MTUs
  – large IP datagram divided (“fragmented”) within not
  – one datagram becomes several datagrams
  – “reassembled” only at final destination
  – IP header bits used to identify, order related fragments
  – IPv6 does things differently...

IP Fragmentation and Reassembly

Example

1. 4000 byte datagram
2. MTU = 1500 bytes

One large datagram becomes several smaller datagrams

Length = 1500  ID = x  fragflag = x  offset = x

Length = 1500  ID = x  fragflag = x  offset = x

Length = 1040  ID = x  fragflag = x  offset = x

1480 bytes in data field

offset = 1480/8

IP Fragmentation Details

• Identifier (16 bits): used to tell which fragments belong together

• Flags (3 bits):
  – Reserved (RF): unused bit
  – Don’t Fragment (DF): instruct routers to not fragment the packet even if it won’t fit
    • Instead, they drop the packet and send back a “Too Large” ICMP control message
  – Forms the basis for “Path MTU Discovery”
  – More (MF): this fragment is not the last one

• Offset (13 bits): what part of datagram this fragment covers in 8-byte units

Pop quiz question: What happens when a fragment is lost?

Pop quiz question: Why do frags use offset and not a frag number?
### IP Addressing: Introduction

- **IP address:** 32-bit identifier for host, router interface
- **Interface:** connection between host/router and physical link
  - router’s typically have multiple interfaces
  - host typically has one interface
- IP addresses associated with each interface

- Subnets

- **IP addresses:** how to get one?

  **Q:** How does a host get IP address?
  - Windows: control-panel->network->configuration->tcp/ip->properties
  - UNIX: /etc/rc.config (circa 1980’s your mileage will vary)
  - DHCP: Dynamic Host Configuration Protocol: dynamically get address
    from as server
    - "plug-and-play"

### DHCP Client-server Scenario

**Goal:** allow host to dynamically obtain its IP address from network server when it joins network

- Can renew its lease on address in use
- Allows reuse of addresses (only hold address while connected an “on”)
- Support for mobile users who want to join network (more shortly)

**IP addresses:** how to get one?

**Q:** How does network get subnet part of IP addr?

**A:** gets allocated portion of its provider ISP’s address space

<table>
<thead>
<tr>
<th>ISP’s block</th>
<th>11001000 00010111 00010000 00000000 200.23.16.0/20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization 0</td>
<td>11001000 00010111 00010000 00000000 200.23.16.0/23</td>
</tr>
<tr>
<td>Organization 1</td>
<td>11001000 00010111 00100101 00000000 200.23.18.0/23</td>
</tr>
<tr>
<td>Organization 2</td>
<td>11001000 00010111 00101000 00000000 200.23.20.0/23</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Organization 7</td>
<td>11001000 00010111 00110110 00000000 200.23.30.0/23</td>
</tr>
</tbody>
</table>
Hierarchical addressing: route aggregation

Hierarchical addressing allows efficient advertisement of routing information:

- Send me anything with addresses beginning 200.23.16.0/20
- Send me anything with addresses beginning 200.23.18.0/23
- Send me anything with addresses beginning 200.23.30.0/23

Fly By Night ISP

Organization 0
200.23.16.0/23

Organization 1
200.23.18.0/23

Organization 2
200.23.20.0/23

Organization 3
200.23.22.0/23

Organization 4
200.23.24.0/23

Organization 5
200.23.26.0/23

Organization 6
200.23.28.0/23

Organization 7
200.23.30.0/23

ISP R-U

Internet

Hierarchical addressing: more specific routes

ISP-R-U has a more specific route to Organization 1

ISP R-U

Organization 0
200.23.15.0/23

Organization 1
200.23.18.0/23

Organization 2
200.23.20.0/23

Organization 3
200.23.22.0/23

Organization 4
200.23.24.0/23

Organization 5
200.23.26.0/23

Organization 6
200.23.28.0/23

Organization 7
200.23.30.0/23

ISP-R-U

Internet

IP addressing: the last word...

Q: How does an ISP get a block of addresses?

A: ICANN: Internet Corporation for Assigned Names and Numbers
- allocates addresses
- manages DNS
- assigns domain names, resolves disputes

NAT: Network Address Translation

Implementation:
- Motivation: local network uses just one IP address as far as outside world is concerned:
  - range of addresses not needed from ISP: just one IP address for all devices
  - can change addresses of devices in local network without notifying outside world
  - can change ISP without changing addresses of devices in local network
  - devices inside local net not explicitly addressable, visible by outside world (a security plus).

- outgoing datagrams: replace (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #)
- incoming datagrams: replace (NAT IP address, new port #) in dest fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table
NAT: Network Address Translation

2. NAT router changes datagram source addr from 10.0.0.1 to 138.76.29.7, 5001, updates table

3. NAT router

1. host 10.0.0.1 sends datagram to 128.119.40.186, 80

4. NAT router changes datagram dest addr from 138.76.29.7, 5001 to 10.0.0.1, 3345

NAT traversal problem

• client wants to connect to server with address 10.0.0.1
  – server address 10.0.0.1 local to LAN [client can’t use it as destination addr]
  – only one externally visible NATed address: 138.76.29.7

• solution 3: statically configure NAT to forward incoming connection requests at given port to server
  – e.g., (138.76.29.7, port 2500) always forwarded to 10.0.0.1 port 25000

NAT traversal problem

• solution 2: Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol. Allows NATed host to:
  - learn public IP address (138.76.29.7)
  - add/remove port mappings (with lease times)

  i.e., automate static NAT port map configuration

NAT traversal problem

• 16-bit port-number field:
  – 60,000 simultaneous connections with a single LAN-side address!

• NAT is controversial:
  – routers should only process up to layer 3
  – violates end-to-end argument (?)
  
  • NAT possibility must be taken into account by app designers, eg. P2P applications
  
  – address shortage should instead be solved by IPv6

NAT traversal problem

• solution 3: relaying (used in Skype)
  – NATed client establishes connection to relay
  – External client connects to relay
  – relay bridges packets between to connections

Remember this? Traceroute at work... trace: rio.cl.cam.ac.uk to munnari.oz.au
(tracethat on pof is similar)
Traceroute and ICMP

- Source sends series of UDP segments to dest
  - First has TTL=1
  - Second has TTL=2, etc.
  - Unlikely port number
- When nth datagram arrives at nth router:
  - Router discards datagram
  - And sends to source an ICMP message (type 11, code 0)
- Destination returns ICMP “host unreachable” packet (type 3, code 3)
- When source gets this ICMP, stops.

When ICMP message arrives, source calculates RTT

Stopping criterion

UDP segment eventually arrives at destination host

ICMP: Internet Control Message Protocol

- used by hosts & routers to communicate network-level information
  - error reporting: unreachable host, network, port, protocol
  - echo request/reply (used by ping)
  - network-layer “above” IP:
    - ICMP msgs carried in IP datagrams
  - ICMP message: type, code plus first 8 bytes of IP datagram causing error

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>echo reply (ping)</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>dest, network unreachable</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>dest protocol unreachable</td>
</tr>
<tr>
<td>0</td>
<td>3</td>
<td>dest port unreachable</td>
</tr>
<tr>
<td>0</td>
<td>4</td>
<td>dest network unknown</td>
</tr>
<tr>
<td>0</td>
<td>6</td>
<td>dest host unknown</td>
</tr>
<tr>
<td>0</td>
<td>7</td>
<td>source quench (congestion control - not used)</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>echo request (ping)</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>route advertisement</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>router discovery</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>TTL expired</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>bad IP header</td>
</tr>
</tbody>
</table>

Gluing it together:
How does my Network (address) interact with my Data-Link (address)?

Switches vs. Routers Summary

- both store-and-forward devices
  - routers: network layer devices (examine network layer headers)
  - switches are link layer devices
- routers maintain routing tables, implement routing algorithms
- switches maintain switch tables, implement filtering, learning algorithms

MAC Addresses (and IPv4 ARP) or How do I glue my network to my data-link?

- 32-bit IP address:
  - network-layer address
  - used to get datagram to destination IP subnet
- MAC (or LAN or physical or Ethernet) address:
  - function: get frame from one interface to another physically-connected interface (same network)
  - 48 bit MAC address (for most LANs)
    - burned in NIC ROM, also (commonly) software settable

LAN Addresses and ARP

Each adapter on LAN has unique LAN address

Ethernet broadcast address = FF-FF-FF-FF-FF-FF

LAN [wired or wireless] 1A-2F-68-70-A0
adapter

Broadcast address = 71-4F-72-B8-53
58-23-D7-FA-20-80
OC-03-11-4F-33-98
**Address Resolution Protocol**

- Every node maintains an **ARP** table
  - `<IP address, MAC address>` pair

- Consult the table when sending a packet
  - Map destination IP address to destination MAC address
  - Encapsulate and transmit the data packet

- But: what if IP address **not** in the table?
  - Sender **broadcasts**: “Who has IP address 1.2.3.156?”
  - Receiver responds: “MAC address 58-23-D7-FA-20-B0”
  - Sender **caches** result in its ARP table

---

**Example: A Sending a Packet to B**

How does host A send an IP packet to host B?

1. A sends packet to R.
2. R sends packet to B.

**Host A Decides to Send Through R**

- Host A constructs an IP packet to send to B
  - Source 111.111.111.111, destination 222.222.222.222
- Host A has a gateway router R
  - Used to reach destinations outside of 111.111.111.0/24
  - Address 111.111.111.110 for R learned via DHCP/config

**Host A Sends Packet Through R**

- Host A learns the MAC address of R’s interface
  - ARP request: broadcast request for 111.111.111.110
  - ARP response: R responds with 6E-E9-00-17-8B-4B
- Host A encapsulates the packet and sends to R

**R Decides how to Forward Packet**

- Router R’s adaptor receives the packet
  - R extracts the IP packet from the Ethernet frame
  - R sees the IP packet is destined to 222.222.222.222
- Router R consults its forwarding table
  - Packet matches 222.222.222.0/24 via other adaptor
**Key Ideas in Both ARP and DHCP**
- **Broadcasting:** Can use broadcast to make contact
  - Scalable because of limited size
- **Caching:** remember the past for a while
  - Store the information you learn to reduce overhead
  - Remember your own address & other host’s addresses
- **Soft state:** eventually forget the past
  - Associate a time-to-live field with the information
  - ... and either refresh or discard the information
  - Key for robustness in the face of unpredictable change

**Why Not Use DNS-Like Tables?**
- **When host arrives:**
  - Assign it an IP address that will last as long it is present
  - Add an entry into a table in DNS-server that maps MAC to IP addresses
- **Answer:**
  - Names: explicit creation, and are plentiful
  - Hosts: come and go without informing network
    - Must do mapping on demand
  - Addresses: not plentiful, need to reuse and remap
    - Soft-state enables dynamic reuse

---

**R Sends Packet to B**
- Router R’s learns the MAC address of host B
  - ARP request: broadcast request for 222.222.222.222
  - ARP response: B responds with 49-B0-D2-C7-52A
- Router R encapsulates the packet and sends to B

**Security Analysis of ARP**
- **Impersonation**
  - Any node that hears request can answer ...
  - ... and can say whatever they want
- **Actual legit receiver never sees a problem**
  - Because even though later packets carry its IP address, its NIC doesn’t capture them since not its MAC address

---

**No More IPv4 Addresses**
- IPv4 address space in terms of /8’s

**No More IPv4 Addresses**
- 24 /8’s on January 12, 2010
No More IPv4 Addresses

- 20 /8's on April 10, 2010
- 13 /8's on May 8, 2010

No More IPv4 Addresses

- 7 /8's on November 30th, 2010
- 0 /8's on January 31st, 2011!

IPv6

- Motivated (prematurely) by address exhaustion
  - Address field four times as long

- Steve Deering focused on simplifying IP
  - Got rid of all fields that were not absolutely necessary
  - "Spring Cleaning" for IP

- Result is an elegant, if unambitious, protocol

Larger Address Space

- IPv4 = 4,294,967,295 addresses
- IPv6 = 340,282,366,920,938,463,744,607,432,768,211,456 addresses
- 4x in number of bits translates to huge increase in address space!
Other Significant Protocol Changes

- Increased minimum MTU from 576 to 1280
- No enroute fragmentation... fragmentation only at source
- Header changes
  - Replace broadcast with multicast

IPv4

<table>
<thead>
<tr>
<th>Segment</th>
<th>Identification</th>
<th>Flags</th>
<th>Fragment Offset</th>
<th>Total Length</th>
</tr>
</thead>
</table>

IPv6

<table>
<thead>
<tr>
<th>Segment</th>
<th>Next Header</th>
<th>Hop Limit</th>
<th>Source Address</th>
<th>Destination Address</th>
</tr>
</thead>
</table>

Legend:
- IPv6 Address Notation
  - RFC 5952
  - 128-bit IPv6 addresses are represented in:
    - Eight 16-bit segments
    - Hexadecimal (non-case sensitive) between 0000 and FFFF
  - Separated by colons
  - Example:
    - 3ffe:1944:100:000a:0000:00bc:2500:0d0b
  - Two rules for dealing with 0’s

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addresses are 32 bits (4 bytes) in length.</td>
<td>Addresses are 128 bits (16 bytes) in length</td>
</tr>
<tr>
<td>Address (A) resource records in DNS to map host names to IPv4 addresses.</td>
<td>Address (AAAA) resource records in DNS to map host names to IPv6 addresses.</td>
</tr>
<tr>
<td>Pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.</td>
<td>Pointer (PTR) resource records in the IMHO.ARPA DNS domain to map IPv6 addresses to host names.</td>
</tr>
<tr>
<td>IPSec is optional and should be supported externally.</td>
<td>IPSec support is not optional</td>
</tr>
<tr>
<td>Header does not identify packet flow for QoS handling by routers.</td>
<td>Header contains Flow Label field, which identifies packet flow for QoS handling by router.</td>
</tr>
<tr>
<td>Both routers and the sending host fragment packets.</td>
<td>Routers do not support packet fragmentation.</td>
</tr>
<tr>
<td>Header includes a checksum.</td>
<td>Header does not include a checksum.</td>
</tr>
<tr>
<td>Header includes options.</td>
<td>Optional data is supported as extension headers.</td>
</tr>
<tr>
<td>ARP uses broadcast ARP request to resolve IP to MAC/Hardware address.</td>
<td>Multicast Neighbor Solicitation messages resolve IP addresses to MAC addresses.</td>
</tr>
<tr>
<td>Internet Group Management Protocol (IGMP) manages membership in local subnet groups.</td>
<td>Multicast Listener Discovery (MLD) messages manage membership in local subnet groups.</td>
</tr>
<tr>
<td>Broadcast addresses are used to send traffic to all nodes on a subnet.</td>
<td>IPv6 uses a link-local scope all-nodes multicast address.</td>
</tr>
<tr>
<td>Must support a 576-byte packet size (possibly fragmented).</td>
<td>Must support a 1280-byte packet size (without fragmentation).</td>
</tr>
</tbody>
</table>

IPv6 Address Notation

- 3ffe:1944:100:000a:0000:00bc:2500:0d0b
- 3ffe:1944:100:a:0:bc:2500:0d0b

0’s Rule 1 – Leading 0’s

- The leading zeroes in any 16-bit segment do not have to be written.

- Example
  - 3ffe:1944:100:000a:0000:00bc:2500:0d0b
  - 3ffe:1944:100:a:0:bc:2500:0d0b
0’s Rule 1 – Leading 0’s

- Can only apply to leading zeros... otherwise ambiguous results
- Example
  - 3ffe : 1944 : 100 : 0 : bc : 2500 : d0b
- Could be either
  - 3ffe : 1944 : 0100 : 000a : 0000 : 00bc : 2500 : 0d0b
  - 3ffe : 1944 : 1000 : a000 : 0000 : bc00 : 2500 : d0b0
  - Which is correct?

0’s Rule 2 – Double Colon

- Any single, contiguous string of 16-bit segments consisting of all zeroes can be represented with a double colon.

\[ ff02 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0005 \]
\[ ff02 : 0 : 0 : 0 : 0 : 0 : 0 : 5 \]
\[ ff02 :: 5 \]

Network Prefixes

- In IPv4, network portion of address can be identified by either
  - Netmask: 255.255.255.0
  - Bitcount: /24
- Only use bitcount with IPv6
  \[ 3ffe:1944:100:a::/64 \]
Special IPv6 Addresses

- Default route: ::/0
- Unspecified Address: ::/128
  - Used in SLAAC (coming later)
- Loopback/Local Host: ::1/128
  - No longer a /8 of addresses but a single address

Types of IPv6 Addresses

- RFC 4291 - "IPv6 Addressing Architecture"
  - Global Unicast
    - Globally routable IPv6 addresses
  - Link Local Unicast
    - Addresses for use on a given subnet
  - Unique Local Unicast
    - Globally unique address for local communication
  - Multicast
  - Anycast
    - A unicast address assigned to interfaces belonging to different nodes

Types of IPv6 Addresses

- RFC 4291 - "IPv6 Addressing Architecture"
  - Global Unicast
  - Globally routable IPv6 addresses
  - Link Local Unicast
    - Addresses for use on a given subnet
  - Unique Local Unicast
    - Globally unique address for local communication
  - Multicast
  - Anycast
    - A unicast address assigned to interfaces belonging to different nodes

Global Unicast Addresses

- Globally routable addresses
  - RFC 3587
    - 48 bit global routing prefix
      - Hierarchically-structured value assigned to a site
    - 16 bit Subnet ID
      - Identifier of a subnet within a site
    - 64(!) bit Interface ID
      - Identifier an interface on a subnet
      - Motivated by expected use of MAC addresses (IEEE EUI-64 identifiers) in SLAAC...
      - Except GIAs that start with ‘001…’ binary
        - Used for, e.g., “IPv4-Mapped IPv6 Addresses” (RFC 4085)

Subnetting Global Unicast Addresses

- Each site can identify $2^{32}$ (65,535) subnets
  - 2340:1111:AAAA::/64
  - 2340:1111:AAAA:2/64
  - 2340:1111:AAAA:3/64
  - 2340:1111:AAAA:4/64
  - ...

- Subnet has address space of $2^{32}$... an IAS of IASs!

- Can extend the subnet ID into the interface ID portion of the address...
  - Sacrifice ability to use EUI-64 style of SLAAC...
  - Maybe not a bad thing... more later

Global Unicast Addresses

- Current ARIN policy is to assign no longer than /32 to an ISP
  - American Registry for Internet Numbers
    - https://www.arin.net/policy/nrpn.html
  - UCSC allocation is 2607:F5F0::/32

- IANA currently assigning addresses that start with ‘001…’ binary
  - 2000:1::/3
    - Supports
      - Maximum 2^{23} (38,870,912... /3 of an Internet address space) of IASs
      - 2^{29} sites (equivalent to 8,192 IASs of sites)

- ISP can delegate a minimum of 2^{16}, or 65,535 site prefixes
  - Difference between Global Prefix (48 bits) and ISP Prefix (32 bits)
These are huge numbers!!  

- Assume average /16’s allocated to ISPs and /22’s allocated to sites in IPv4
- And this keeps assumption of /64 subnets!

<table>
<thead>
<tr>
<th>Description</th>
<th>Total # ISPs</th>
<th>Total # Sites</th>
<th>Sites/ISP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total # ISPs</td>
<td>/3 / /32</td>
<td>2 7/64</td>
<td>512M</td>
</tr>
<tr>
<td>Total # Sites</td>
<td>/3 / /48</td>
<td>2 24</td>
<td>1.2M</td>
</tr>
<tr>
<td>Sites/ISP</td>
<td>/48 / /64</td>
<td>2 24</td>
<td>1.024</td>
</tr>
</tbody>
</table>

- IPv6 Address Space
  - Allocated
    - 2000::/3 Global Unicast
    - FE80::/10 Link Local Unicast
    - FEC0::/8 Multicast
  - Unallocated ("Reserved by IETF")
    - /7.x – 4000, 6000, 8000, A000, C000
    - /8.x – 0000, 0100, 0200
    - /9.x – 0300
    - /10.x – 0400
    - /11.x – 0500
  - Accounts for a bit more than 2125 of the address space.

- Problem with /64 Subnets
  - Scanning a subnet becomes a DoS attack!
    - Creates IPv6 version of 24 ARP entries in routers
    - Exhaust address-translation table space
  - So now we have:
    - ping6 ff02::1 All nodes in broadcast domain
    - ping6 ff02::2 All routers in broadcast domain
  - Solutions
    - RFC 6164 recommends use of /127 to protect router-router links
    - RFC 3756 suggest "clever cache management" to address more generally

- Types of IPv6 Addresses
  - RFC 4291 – "IPv6 Addressing Architecture"
  - Global Unicast
    - Globally routable IPv6 addresses
  - Link Local Unicast
    - Addresses for use on a given subnet
  - Unique Local Unicast
    - Globally unique address for local communication
  - Multicast
  - Anycast
    - A unicast address assigned to interfaces belonging to different nodes

- Link-Local Addresses
  - '11111110 10...’ binary (FE80::/10)
    - According to RFC 4291 bits 11-64 should be 0... so really FE80::/64?
  - For use on a single link
    - Automatic address configuration
    - Neighbor discovery (IPv6 ARP)
    - When no routers are present
    - Routers must not forward
  - Addresses “chicken-or-egg” problem... need an address to get an address.
  - Address assignment done unilaterally by node (later)
  - IPv4 has link-local address (169.254/16, RFC 3927)
    - Only used if no globally routable addresses available
Types of IPv6 Addresses

- **RFC 4291** — *IPv6 Addressing Architecture*
- **Global Unicast**
  - Globally routable IPv6 addresses
- **Link Local Unicast**
  - Addresses for use on a given subnet
- **Unique Local Unicast**
  - Globally unique address for local communication
- **Multicast**
- **Anycast**
  - A unicast address assigned to interfaces belonging to different nodes

Unique Local Addresses

- 4 parts
  - "L" bit always 1
  - Global ID (40 bits) randomly generated to enforce the idea that these addresses are not to be globally routed or aggregated
  - Subnet ID (16 bits)... same as Globally Unique Subnet ID
  - Interface ID (64 bits)... same as Globally Unique Interface ID

Multicast Addresses

- \'11111111…\' binary (FF00::/8)
- Equivalent to IPv4 multicast (224.0.0.0/8)
- 3 parts
  - Flag [4 bits]
  - Scope [4 bits]

Reserved Multicast Addresses

- **All nodes**
  - FF01::1 — interface-local; used for loopback multicast transmissions
  - FF02::1 — link-local; replaces IPv4 broadcast address (all 1’s host)
- **All routers**
  - FF02::1 (interface-local), FF02:: (link-local)
- **Solicited-Node multicast**
  - Used in Neighbor Discovery Protocol (later)
  - FF02::1:FF00::/104 [FF02::1:XXXX:XXXX]
  - Construct by replacing ‘XX:XXXX’ above with low-order 24 bits of a node’s unicast or anycast address
  - Example
    - For unicast address 4017:1111:0010:2000:10C6
    - Solicited-Node multicast is FF02::1:10C6:0010
Types of IPv6 Addresses

- RFC 4291 – “IPv6 Addressing Architecture”
- Global Unicast
  - Globally routable IPv6 addresses
- Link Local Unicast
  - Addresses for use on a given subnet
- Unique Local Unicast
  - Globally unique address for local communication
- Multicast
  - Anycast
    - A unicast address assigned to interfaces belonging to different nodes

Anycast Addresses

- Allocated from unicast address space
  - Syntactically indistinguishable from unicast addresses
- An address assigned to more than one node
- Anycast traffic routed to the “nearest” host with the anycast address
- Typically used for a service (e.g. local DNS servers)
- Nodes must be configured to know an address is anycast
  - Don’t do Duplicate Address Detection
  - Advertise a route?

A Node’s Required Addresses

- Link-local address for each interface
- Configured unicast or anycast addresses
- Loopback address
- All-Nodes multicast interface and link addresses
- Solicited-Node multicast for each configured unicast and anycast address
- Multicast addresses for all groups the node is a member of
- Routers must add
  - Subnet-Router anycast address for each interface
  - Subnet prefix with all IPv6 host part
  - All-Routers multicast address

Roundup: IPv6 Addresses

- “Interface ID” (host part) is 64 bits
- New addresses required by all nodes (host or router)
  - Link-local address
  - All-nodes interface-local and link-local multicast
  - Solicited-node multicast for each unicast/anycast address
- New addresses required by routers
  - All-routers interface-local, link-local and site-local multicast
  - Subnet-Router anycast for each interface?

Assigning Address to Interfaces

- Static (manual) assignment
  - Needed for network equipment
- DHCPv6
  - Needed to track who uses an IP address
- StateLess Address AutoConfiguration (SLAAC)
  - New to IPv6
- Describe SLAAC in the following...
SLAAC

- RFC 4862 – IPv6 Stateful Address Autoconfiguration
- Used to assign unicast addresses to interfaces
  - Link-Local Unicast
  - Global Unicast
  - Unique-Local Unicast?
- Goal is to minimize manual configuration
  - No manual configuration of hosts
  - Limited router configuration
  - No additional servers
- Use when "not particularly concerned with the exact addresses hosts use"
  - Otherwise use DHCPv6 (RFC 3315)

SLAAC Building Blocks

- Interface IDs
- Neighbor Discovery Protocol
- SLAAC Process

SLAAC Building Blocks

- Interface IDs
- Neighbor Discovery Protocol
- SLAAC Process

IEEE EUI-64 Option for Interface ID

- Use interface MAC address
- Insert FFFE to convert EUI-48 to EUI-64
- Flip Universal/Local bit to “1”
  - Section 2.5.1 RFC 4291

Privacy Option for Interface ID

- Using MAC uniquely identifies a host... security/privacy concerns!
- Microsoft(I) defined an alternative solution for Interface IDs (RFC 4941)
- Hosts generates a random 64 bit Interface ID
SLAAC Building Blocks

• Interface IDs
• Neighbor Discovery Protocol
• SLAAC Process

NDP

• RFC 4861 – Neighbor Discovery for IPv6
• Used to
  – Determine MAC address for nodes on same subnet (ARP)
  – Find routers on same subnet
  – Determine subnet prefix and MTU
  – Determine address of local DNS server (RFC 6106)
• Uses 5 ICMPv6 messages
  – Router Solicitation (RS) – request routers to send RA
  – Router Advertisement (RA) – router’s address and subnet parameters
  – Neighbor Solicitation (NS) – request neighbor’s MAC address (ARP Request)
  – Neighbor Advertisement (NA) – MAC address for an IPv6 address (ARP Reply)
  – Redirect – inform host of a better next hop for a destination

NDP RS & RA

• Router Solicitation (RS)
  – Originated by hosts to request that a router send an RA
  – Source = unspecified :: or link-local address,
  – Destination = All-routers multicast (FF02::2)
• Router Advertisement (RA)
  – Originated by routers to advertise their address and link-specific parameters
  – Sent periodically and in response to Router Solicitation messages
  – Source = link-local address.
  – Destination = All-routers multicast (FF02:1)

NDP NS & NA

• Neighbor Solicitation (NS)
  – Request target MAC address while providing target of source (IPv4 ARP Request)
  – Used to resolve address or verify reachability of neighbor
  – Source = unspecified or :: (Duplicate Address Detection…next slide)
  – Destination = solicited-node multicast
• Neighbor Advertisement (NA)
  – Advertise MAC address for given IPv6 address (IPv4 ARP Reply)
  – Respond to NS or communicate MAC address change
  – Source = unspecified, destination = NS’s source or all nodes multicast (if source ::)

Duplicate Address Detection

• Duplicate Address Detection (DAD) used to verify address is unique in subnet prior to assigning it to an interface
• MUST take place on all unicast addresses, regardless of whether they are obtained through stateful, stateless or manual configuration
• MUST NOT be performed on anycast addresses
• Uses Neighbor Solicitation and Neighbor Advertisement messages
• NS sent to solicited-node multicast; if no NA received address is unique
• Solicited-node multicast: FF02::1 FF10/104 w/ last 24 bits of target
SLAAC Building Blocks

• Interface IDs
• Neighbor Discovery Protocol
• SLAAC Process

SLAAC Steps

• Select link-local address
• Verify "tentative" address not in use by another host with DAD
• Send RS to solicit RAs from routers
• Receive RA with
  – router address,
  – subnet MTU,
  – subnet prefix,
  – local DNS server (RFC 6106)
• Generate global unicast address
• Verify address is not in use by another host with DAD

Prefix Leases

• Prefix information contained in RA includes lifetime information
  – Preferred lifetime: when an address's preferred lifetime expires SHOULD only be used for existing communications
  – Valid lifetime: when an address's valid lifetime expires it MUST NOT be used as a source address or accepted as a destination address.

• Unsolicited RAs can reduce prefix lifetime values
  – Can be used to force re-addressing

Roundup: ICMPv6

• Implements router discovery and ARP functions
• ICMPv6 messages
  – Router Solicitation/Router Advertisement
  – Neighbor Solicitation/Neighbor Advertisement
  – (Next hop) Redirect
• Duplicate Address Detection (DAD)
  – verify unique link-local and global-unicast addresses
  – Uses:
    • NS/NA (i.e. gratuitous ARP)
    • Solicited node multicast address

Review - SLAAC

• Assigns link-local and global-unicast addresses
• Goals
  – Eliminate manual configuration
  – Require minimal router configuration
  – Require no additional servers
• Host part options
  – EUI-64
  – Random ("privacy") addresses
• Steps
  – Generate link-local address and verify with DAD
  – Find router - RS/RA
  – Generate global unicast address and verify with DAD
Improving on IPv4 and IPv6?

- Why include unverifiable source address?
  - Would like accountability and anonymity (now neither)
  - Return address can be communicated at higher layer
- Why packet header used at edge same as core?
  - Edge: host tells network what service it wants
  - Core: packet tells switch how to handle it
    - One is local to host, one is global to network
- Some kind of payment/responsibility field?
  - Who is responsible for paying for packet delivery?
    - Source, destination, other?
- Other ideas?

Summary Network Layer

- understand principles behind network layer services:
  - network layer service models
  - forwarding versus routing (versus switching)
  - how a router works
  - routing (path selection)
  - IPv6
- Algorithms
  - Two routing approaches (LS vs DV)
  - One of these in detail (LS)
  - ARP
Topic 5 – Transport

Our goals:
• understand principles behind transport layer services:
  – multiplexing/demultiplexing
  – reliable data transfer
  – flow control
  – congestion control
• learn about transport layer protocols in the Internet:
  – UDP: connectionless transport
  – TCP: connection-oriented transport
  – TCP congestion control

Transport Layer

• Commonly a layer at end-hosts, between the application and network layer

Why a transport layer?

• IP packets are addressed to a host but end-to-end communication is between application processes at hosts
  – Need a way to decide which packets go to which applications (more multiplexing)
Why a transport layer?

- IP packets are addressed to a host but end-to-end communication is between application processes at hosts.
  - Need a way to decide which packets go to which applications (mux/demux).
- IP provides a weak service model (best-effort)
  - Packets can be corrupted, delayed, dropped, reordered, duplicated
  - No guidance on how much traffic to send and when
  - Dealing with this is tedious for application developers.

Role of the Transport Layer

- Communication between application processes
  - Multiplexing between application processes
  - Implemented using ports.

Role of the Transport Layer

- Communication between processes
- Provide common end-to-end services for app layer [optional]
  - Reliable, in-order data delivery
  - Paced data delivery: flow and congestion-control
    - too fast may overwhelm the network
    - too slow is not efficient
- TCP and UDP are the common transport protocols
  - also SCTP, MTCP, SST, RDP, DCCP, ...

Role of the Transport Layer

- Communication between processes
- Provide common end-to-end services for app layer [optional]
- TCP and UDP are the common transport protocols
- UDP is a minimalist, no-frills transport protocol
  - only provides mux/demux capabilities
- TCP is the *totus porcus* protocol
  - offers apps a reliable, in-order, byte-stream abstraction
  - with congestion control
  - but no performance (delay, bandwidth, ...) guarantees.
Role of the Transport Layer

- Communication between processes
  - mux/demux from and to application processes
  - implemented using ports

Context: Applications and Sockets

- Socket: software abstraction by which an application process exchanges network messages with the (transport layer in the) operating system
  - socketID = socket(…, socket.TYPE)
  - socketID.sendto(message, …)
  - socketID.recvfrom(…)

- Two important types of sockets
  - UDP socket: TYPE is SOCK_DGRAM
  - TCP socket: TYPE is SOCK_STREAM

Ports

- Problem: deciding which app (socket) gets which packets
  - Solution: port as a transport layer identifier
    - 16-bit identifier
    - OS stores mapping between sockets and ports
    - a packet carries a source and destination port number in its transport layer header

- For UDP ports (SOCK_DGRAM)
  - OS stores (local port, local IP address) ↔ socket

- For TCP ports (SOCK_STREAM)
  - OS stores (local port, local IP, remote port, remote IP) ↔ socket
Recap: Multiplexing and Demultiplexing

- Host receives IP packets
  - Each IP packet has source and destination IP address
  - Each Transport Layer header has source and destination port number
- Host uses IP addresses and port numbers to direct the message to appropriate socket

More on Ports

- Separate 16-bit port address space for UDP and TCP
- “Well known” ports (0-1023): everyone agrees which services run on these ports
  - e.g., ssh:22, http:80
  - Helps client know server’s port
- Ephemeral ports (most 1024-65535): dynamically selected: as the source port for a client process

UDP: User Datagram Protocol

- Lightweight communication between processes
  - Avoid overhead and delays of ordered, reliable delivery
- UDP described in RFC 768 – (1980!)
  - Destination IP address and port to support demultiplexing
  - Optional error checking on the packet contents
    - (checksum field of 0 means “don’t verify checksum”)

Principles of Reliable data transfer

- Important in app., transport, link layers
- Top-10 list of important networking topics!
  - In a perfect world, reliable transport is easy
  - But the Internet default is best-effort
    - All the bad things best-effort can do
      - A packet is corrupted (bit errors)
      - A packet is lost
      - A packet is delayed (why?)
      - Packets are reordered (why?)
      - A packet is duplicated (why?)
Principles of Reliable data transfer

• important in app., transport, link layers
• top-10 list of important networking topics!

 characteristics of unreliable channel will determine complexity of reliable data transfer protocol (rdt)

Reliable data transfer: getting started

We’ll:
• incrementally develop sender, receiver sides of reliable data transfer protocol (rdt)
• consider only unidirectional data transfer
  – but control info will flow on both directions!
• use finite state machines (FSM) to specify sender, receiver

KR state machines – a note.

Beware
Kurose and Ross has a confusing/confused attitude to state-machines.
I’ve attempted to normalise the representation.

UPSHOT: these slides have differing information to the KR book (from which the RDT example is taken.)

in KR “actions taken” appear wide-ranging, my interpretation is more specific/relevant.

Rdt1.0: reliable transfer over a reliable channel

• underlying channel perfectly reliable
  – no bit errors
  – no loss of packets
• separate FSMs for sender, receiver:
  – sender sends data into underlying channel
  – receiver read data from underlying channel
Rdt2.0: channel with bit errors

- underlying channel may flip bits in packet
  - checksum to detect bit errors
- the question: how to recover from errors:
  - acknowledgements (ACKs): receiver explicitly tells sender that packet received is OK
  - negative acknowledgements (NAKs): receiver explicitly tells sender that packet had errors
  - sender retransmits packet on receipt of NAK
- new mechanisms in rdt2.0 (beyond rdt1.0):
  - error detection
  - receiver feedback: control msgs (ACK, NAK) receiver ➔ sender

Dealing with Packet Corruption

Sender | Time | Receiver
--- | --- | ---
1 | ack |
2 | | nnak
2 | | 2

Rdt2.0: FSM specification

Sender state diagram:
- IDLE
- Waiting for reply
- udt_send(data)
- udt_send(packet)

Receiver state diagram:
- IDLE
- Waiting for reply
- udt_recv(reply) ➔ udt_send(packet)

Note: the sender holds a copy of the packet being sent until the delivery is acknowledged.

Rdt2.0: operation with no errors

Sender state diagram:
- IDLE
- Waiting for reply
- udt_send(data)
- udt_send(packet)

Receiver state diagram:
- IDLE
- Waiting for reply
- udt_recv(reply) ➔ udt_send(packet)

Rdt2.0 has a fatal flaw!

What happens if ACK/NAK corrupted?
- sender doesn’t know what happened at receiver!
- can’t just retransmit: possible duplicate

Handling duplicates:
- sender retransmits current packet if ACK/NAK garbled
- sender adds sequence number to each packet
- receiver discards (doesn’t deliver) duplicate packet

Stop and wait:
- Sender sends one packet, then waits for receiver response
Dealing with Packet Corruption

Data and ACK packets carry sequence numbers

### rdt2.1: sender, handles garbled ACK/NAKs

- **Sender:**
  - seq # added to pkt
  - two seq. #’s (0,1) will suffice. Why?
  - must check if received ACK/NAK corrupted
  - twice as many states
    - state must “remember” whether “current” pkt has a 0 or 1 sequence number

- **Receiver:**
  - must check if received packet is duplicate
    - state indicates whether 0 or 1 is expected pkt seq #
  - note: receiver can not know if its last ACK/NAK received OK at sender

### rdt2.1: discussion

Sender:
- seq # added to pkt
- two seq. #’s (0,1) will suffice. Why?
- must check if received ACK/NAK corrupted
- twice as many states
  - state must “remember” whether “current” pkt has a 0 or 1 sequence number

Receiver:
- must check if received packet is duplicate
  - state indicates whether 0 or 1 is expected pkt seq #
- note: receiver can not know if its last ACK/NAK received OK at sender

### rdt2.2: a NAK-free protocol

- same functionality as rdt2.1, using ACKs only
- instead of NAK, receiver sends ACK for last pkt received OK
  - receiver must explicitly include seq # of pkt being ACKed
- duplicate ACK at sender results in same action as NAK: retransmit current pkt

### rdt2.2: sender, receiver fragments

**Sender FSM**
- reset to 0 from show
- next to 0 from show
- next to ACK

**Receiver FSM**
- reset to 0 from show
- next to ACK

receiver_fragment
- send(ACK1)
- send(NAK)
- not corrupt(packet) & has_seq1(packet)
- udt_send(packet)
- udt_send(ACK)
- udt_send(NAK)

- udt_rcv(packet) & not corrupt(packet)
- & has_seq1(packet)
- send(ACK1)
- send(NAK)
- not corrupt(packet) & has_seq1(packet)
- udt_send(packet)
- udt_send(ACK)
- udt_send(NAK)

- udt_rcv(packet) & not corrupt(packet)
- & has_seq0(packet)
- send(NAK)
- send(ACK)
- not corrupt(packet) & has_seq0(packet)
- udt_send(packet)
- udt_send(ACK)
- udt_send(NAK)
Dealing with Packet Loss

Timeout

Timer-driven loss detection
Set timer when packet is sent; retransmit on timeout

Dealing with Packet Loss

Timeout

Timer-driven retransmit can lead to duplicates

Dealing with Packet Loss

Timeout

New assumption: underlying channel can also lose packets (data or ACKs)
- checksum, seq. #, ACKs, retransmissions will be of help, but not enough
- rdt3.0: channels with errors and loss

Approach: sender waits “reasonable” amount of time for ACK
- retransmits if no ACK received in this time
- if pkt (or ACK) just delayed (not lost):
  - retransmission will be duplicate, but use of seq. #’s already handles this
  - receiver must specify seq # of pkt being ACKed
- requires countdown timer

Performance of rdt3.0

- rdt3.0 works, but performance stinks
- ex: 1 Gbps link, 15 ms prop. delay, 8000 bit packet:
  \[ d_{\text{max}} = \frac{L}{R} \]
  \[ = \frac{8000\text{bits}}{10^6\text{bps}} = 8\text{ microseconds} \]
  \[ U_{\text{sender}} = \frac{L}{RTT + L/R} = \frac{0.008}{30.008} = 0.00027 \]
  \[ \text{1KB pkt every 30 msec => 33KB/sec throughput over 1 Gbps link} \]
  \[ \text{network protocol limits use of physical resources!} \]
A Sliding Packet Window

- **window** = set of adjacent sequence numbers
  - The size of the set is the window size; assume window size is \( n \)

- General idea: send up to \( n \) packets at a time
  - Sender can send packets in its window
  - Receiver can accept packets in its window
  - Window of acceptable packets "slides" on successful reception/acknowledgement

Acknowledgements w/ Sliding Window

- Two common options
  - cumulative ACKs: ACK carries next in-order sequence number that the receiver expects

Cumulative Acknowledgements (1)

- At receiver
  - \( B_n \) = \( B+2 \) 
  - Receiver sends ACK(\( B_{new}+1 \))
Cumulative Acknowledgements (2)

- At receiver

![Diagram showing cumulative acknowledgements]

- After receiving B+4, B+5

![Diagram showing cumulative acknowledgements]

- Receiver sends ACK(B+1)

How do we recover?

Go-Back-N (GBN)

- Sender transmits up to n unacknowledged packets

- Receiver only accepts packets in order
  - discards out-of-order packets (i.e., packets other than B+1)

- Receiver uses cumulative acknowledgements
  - i.e., sequence# in ACK = next expected in-order sequence#

- Sender sets timer for 1st outstanding ack (A+1)
- If timeout, retransmit A+1, ..., A+n

Sliding Window with GBN

- Let A be the last ack’d packet of sender without gap; then window of sender = \( (A+1, A+2, ..., A+n) \)

- Let B be the last received packet without gap by receiver, then window of receiver = \( (B+1, ..., B+n) \)

GBN Example w/o Errors

![Diagram showing GBN example without errors]

GBN Example with Errors

![Diagram showing GBN example with errors]

GBN: sender extended FSM

```
udt_send(data)
if (nextseqnum + base = 0)
    udt_send(packet[0:nextseqnum])
else
    refuse_data(data)
```

```
udt_rcv(reply)
if (notcorrupt(reply))
    base = getacknum(reply) + 1
else
    refuse_data(data)
```
GBN: receiver extended FSM

- Ack-only: always send an ACK for correctly-received packet with the highest in-order seq #
  - may generate duplicate ACKs
  - need only remember expected seq num
- out-of-order packet:
  - discard (don’t buffer) > no receiver buffering!
  - Re-ACK packet with highest in-order seq #

Selective Repeat (SR)

- Sender: transmit up to \( n \) unacknowledged packets
- Assume packet \( k \) is lost, \( k+1 \) is not
- Receiver: indicates packet \( k+1 \) correctly received
- Sender: retransmit only packet \( k \) on timeout
- Efficient in retransmissions but complex book-keeping
  - need a timer per packet

SR Example with Errors

- Window size = 3 packets
- Time
- Packet 4
- ACK 4
- ACK 5
- ACK 6

Observations

- With sliding windows, it is possible to fully utilize a link, provided the window size \( n \) is large enough. Throughput is \( \sim (n/RTT) \)
  - Stop & Wait is like \( n = 1 \).
- Sender has to buffer all unacknowledged packets, because they may require retransmission
- Receiver may be able to accept out-of-order packets, but only up to its buffer limits
- Implementation complexity depends on protocol details (GBN vs. SR)

Acknowledgements w/ Sliding Window

- Two common options
  - cumulative ACKs: ACK carries next in-order sequence number the receiver expects
  - selective ACKs: ACK individually acknowledges correctly received packets
- Selective ACKs offer more precise information but require more complicated book-keeping
- Many variants that differ in implementation details

Recap: components of a solution

- Checksums (for error detection)
- Timers (for loss detection)
- Acknowledgments
  - cumulative
  - selective
- Sequence numbers (duplicates, windows)
- Sliding Windows (for efficiency)
- Reliability protocols use the above to decide when and what to retransmit or acknowledge
What does TCP do?

Most of our previous tricks + a few differences
- Sequence numbers are byte offsets
- Sender and receiver maintain a sliding window
- Receiver sends cumulative acknowledgements (like GBN)
- Sender maintains a single retrans timer
- Receivers do not drop out-of-sequence packets (like SR)
- Introduces fast retransmit optimization that uses duplicate ACKs to trigger early retrans
- Introduces timeout estimation algorithms

Automatic Repeat Request (ARQ)

+ Self-clocking (Automatic)
+ Adaptive
+ Flexible
- Slow to start / adapt

TCP arguably the most successful protocol in the Internet...
its an ARQ protocol

TCP Header

<table>
<thead>
<tr>
<th>Source port</th>
<th>Destination port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence number</td>
<td>Acknowledgment</td>
</tr>
<tr>
<td>Advertised window</td>
<td>Flags</td>
</tr>
<tr>
<td>Checksum</td>
<td>Urgent pointer</td>
</tr>
<tr>
<td>Options (variable)</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td>Used to mux and demux</td>
</tr>
</tbody>
</table>

Last time: Components of a solution for reliable transport

- Checksums (for error detection)
- Timers (for loss detection)
- Acknowledgments
  - cumulative
  - selective
- Sequence numbers (duplicates, windows)
- Sliding Windows (for efficiency)
  - Go-Back-N (GBN)
  - Selective Replay (SR)

TCP Header

<table>
<thead>
<tr>
<th>Source port</th>
<th>Destination port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence number</td>
<td>Acknowledgment</td>
</tr>
<tr>
<td>Advertised window</td>
<td>Flags</td>
</tr>
<tr>
<td>Checksum</td>
<td>Urgent pointer</td>
</tr>
<tr>
<td>Options (variable)</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td>Computed over header and data</td>
</tr>
</tbody>
</table>
What does TCP do?

Many of our previous ideas, but some key differences
- Checksum
- Sequence numbers are byte offsets

TCP: Segments and Sequence Numbers

TCP “Stream of Bytes” Service… ...

… Provided Using TCP “Segments”

TCP Segment

- IP packet
  - No bigger than Maximum Transmission Unit (MTU)
  - E.g., up to 1500 bytes with Ethernet
- TCP packet
  - IP packet with a TCP header and data inside
  - TCP header ≥ 20 bytes long
- TCP segment
  - No more than Maximum Segment Size (MSS) bytes
  - E.g., up to 1460 consecutive bytes from the stream
  - MSS = MTU – (IP header) – (TCP header)

Sequence Numbers

- ISN (initial sequence number)
- Sequence number = 1st byte in segment = ISN + k
Sequence Numbers

TCP Header

What does TCP do?

Most of our previous tricks, but a few differences

- Checksum
- Sequence numbers are byte offsets
- Receiver sends cumulative acknowledgements (like GBN)

ACKing and Sequence Numbers

Normal Pattern

- Sender: seqno=X, length=B
- Receiver: ACK=X+B
- Sender: seqno=X+B, length=B
- Receiver: ACK=X+2B
- Sender: seqno=X+2B, length=B
- Seqno of next packet is same as last ACK field
TCP Header

<table>
<thead>
<tr>
<th>Source port</th>
<th>Destination port</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sequence number</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acknowledgment</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Advertised window</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Urgent pointer</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Options (variable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
</tr>
</tbody>
</table>

Acknowledgment gives seqno just beyond highest seqno received in order (“What Byte is Next?”)

What does TCP do?

Most of our previous tricks, but a few differences

- Checksum
- Sequence numbers are byte offsets
- Receiver sends cumulative acknowledgements (like GBN)
- Receivers can buffer out-of-sequence packets (like SR)

Loss with cumulative ACKs

- Sender sends packets with 100B and seqnos:
  - 100, 200, 300, 400, 500, 600, 700, 800, 900, ...

- Assume the fifth packet (seqno 500) is lost, but no others

- Stream of ACKs will be:
  - 200, 300, 400, 500, 500, 500, 500, ...

Loss with cumulative ACKs

- “Duplicate ACKs” are a sign of an isolated loss
  - The lack of ACK progress means 500 hasn’t been delivered
  - Stream of ACKs means some packets are being delivered

- Therefore, could trigger resend upon receiving k duplicate ACKs
  - TCP uses k=3

- But response to loss is trickier....

Loss with cumulative ACKs

- Two choices:
  - Send missing packet and increase W by the number of dup ACKs
  - Send missing packet, and wait for ACK to increase W

- Which should TCP do?
What does TCP do?

Most of our previous tricks, but a few differences

- Checksum
- Sequence numbers are byte offsets
- Receiver sends cumulative acknowledgements (like GBN)
- Receivers do not drop out-of-sequence packets (like SR)
- Introduces fast retransmit optimization that uses duplicate ACKs to trigger early retransmission
- Sender maintains a single retransmission timer (like GBN) and retransmits on timeout

Retransmission Timeout

- If the sender hasn’t received an ACK by timeout, retransmit the first packet in the window
  - How do we pick a timeout value?

Timing Illustration

Timeout too long \(\rightarrow\) inefficient  
Timeout too short \(\rightarrow\) duplicate packets

Retransmission Timeout

- If haven’t received ack by timeout, retransmit the first packet in the window
- How to set timeout?
  - Too long: connection has low throughput
  - Too short: retransmit packet that was just delayed
- Solution: make timeout proportional to RTT
- But how do we measure RTT?

RTT Estimation

- Use exponential averaging of RTT samples

\[
\text{SampleRTT} = \text{AckRcvdTime} - \text{SendPacketTime} \\
\text{EstimatedRTT} = \alpha \times \text{EstimatedRTT} + (1 - \alpha) \times \text{SampleRTT} \\
0 < \alpha \leq 1
\]

Exponential Averaging Example

\[
\text{EstimatedRTT} = \alpha \times \text{EstimatedRTT} + (1 - \alpha) \times \text{SampleRTT}
\]

Assume RTT is constant \(\rightarrow\) SampleRTT = RTT
Problem: Ambiguous Measurements

- How do we differentiate between the real ACK, and ACK of the retransmitted packet?

Karn/Partridge Algorithm

- Measure SampleRTT only for original transmissions
  - Once a segment has been retransmitted, do not use it for any further measurements
- Computes EstimatedRTT using $\alpha = 0.875$
- Timeout value (RTO) = $2 \times$ EstimatedRTT
- Employs exponential backoff
  - Every time RTO timer expires, set RTO $\leftarrow 2 \times$ RTO
  - (Up to maximum $\geq 60$ sec)
  - Every time new measurement comes in (= successful original transmission), collapse RTO back to $2 \times$ EstimatedRTT

Karn/Partridge in action

Jacobson/Karels Algorithm

- Problem: need to better capture variability in RTT
  - Directly measure deviation
- Deviation = $|\text{SampleRTT} - \text{EstimatedRTT}|$
- EstimatedDeviation: exponential average of Deviation
- $\text{RTO} = \text{EstimatedRTT} + 4 \times \text{EstimatedDeviation}$

With Jacobson/Karels

What does TCP do?

Most of our previous ideas, but some key differences
- Checksum
- Sequence numbers are byte offsets
- Receiver sends cumulative acknowledgements (like GBN)
- Receivers do not drop out-of-sequence packets (like SR)
- Introduces fast retransmit: optimization that uses duplicate ACKs to trigger early retransmission
- Sender maintains a single retransmission timer (like GBN) and retransmits on timeout
TCP Header: What’s left?

<table>
<thead>
<tr>
<th>Source port</th>
<th>Destination port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence number</td>
<td>Acknowledgment</td>
</tr>
<tr>
<td>HdrLen</td>
<td>Flags</td>
</tr>
<tr>
<td>Checksum</td>
<td>Advertised window</td>
</tr>
<tr>
<td>Options (variable)</td>
<td>Urgent pointer</td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
</tbody>
</table>

- "Must Be Zero" 8 bits reserved
- Number of 4-byte words in TCP header: 5 = no options

TCP Connection Establishment and Initial Sequence Numbers

<table>
<thead>
<tr>
<th>Source port</th>
<th>Destination port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence number</td>
<td>Acknowledgment</td>
</tr>
<tr>
<td>HdrLen</td>
<td>Flags</td>
</tr>
<tr>
<td>Checksum</td>
<td>Urgent pointer</td>
</tr>
<tr>
<td>Options (variable)</td>
<td>Data</td>
</tr>
</tbody>
</table>

Initial Sequence Number (ISN)

- Sequence number for the very first byte
- Why not just use ISN = 0?
- Practical issue
  - IP addresses and port #s uniquely identify a connection
  - Eventually, though, these port #s do get used again
  - … small chance an old packet is still in flight
- TCP therefore requires changing ISN
- Hosts exchange ISNs when they establish a connection

Establishing a TCP Connection

- Three-way handshake to establish connection
  - Host A sends a SYN (open; "synchronize sequence numbers") to host B
  - Host B returns a SYN acknowledgment (SYN ACK)
  - Host A sends an ACK to acknowledge the SYN ACK

Each host tells its ISN to the other host.
TCP Header

<table>
<thead>
<tr>
<th>Flags</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN</td>
<td></td>
</tr>
<tr>
<td>ACK</td>
<td></td>
</tr>
<tr>
<td>FIN</td>
<td></td>
</tr>
<tr>
<td>RST</td>
<td></td>
</tr>
<tr>
<td>PSH</td>
<td></td>
</tr>
<tr>
<td>URG</td>
<td></td>
</tr>
<tr>
<td>Options (variable)</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
</tbody>
</table>

Step 1: A’s Initial SYN Packet

<table>
<thead>
<tr>
<th>Flags</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN</td>
<td></td>
</tr>
<tr>
<td>ACK</td>
<td></td>
</tr>
<tr>
<td>FIN</td>
<td></td>
</tr>
<tr>
<td>RST</td>
<td></td>
</tr>
<tr>
<td>PSH</td>
<td></td>
</tr>
<tr>
<td>URG</td>
<td></td>
</tr>
<tr>
<td>Advertised window</td>
<td>5</td>
</tr>
<tr>
<td>Options (variable)</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
</tbody>
</table>

A tells B it wants to open a connection...

Step 2: B’s SYN-ACK Packet

<table>
<thead>
<tr>
<th>Flags</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN</td>
<td></td>
</tr>
<tr>
<td>ACK</td>
<td></td>
</tr>
<tr>
<td>FIN</td>
<td></td>
</tr>
<tr>
<td>RST</td>
<td></td>
</tr>
<tr>
<td>PSH</td>
<td></td>
</tr>
<tr>
<td>URG</td>
<td></td>
</tr>
<tr>
<td>Advertised window</td>
<td>5</td>
</tr>
<tr>
<td>Options (variable)</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
</tbody>
</table>

B tells A it accepts, and is ready to hear the next byte...

... upon receiving this packet, A can start sending data

Step 3: A’s ACK of the SYN-ACK

<table>
<thead>
<tr>
<th>Flags</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN</td>
<td></td>
</tr>
<tr>
<td>ACK</td>
<td></td>
</tr>
<tr>
<td>FIN</td>
<td></td>
</tr>
<tr>
<td>RST</td>
<td></td>
</tr>
<tr>
<td>PSH</td>
<td></td>
</tr>
<tr>
<td>URG</td>
<td></td>
</tr>
<tr>
<td>Advertised window</td>
<td>20</td>
</tr>
<tr>
<td>Options (variable)</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
</tbody>
</table>

A tells B it’s likewise okay to start sending

... upon receiving this packet, B can start sending data

Timing Diagram: 3-Way Handshaking

What if the SYN Packet Gets Lost?

- Suppose the SYN packet gets lost
  - Packet is lost inside the network, or:
  - Server discards the packet (e.g., it’s too busy)

- Eventually, no SYN-ACK arrives
  - Sender sets a timer and waits for the SYN-ACK
  - … and retransmits the SYN if needed

- How should the TCP sender set the timer?
  - Hard to guess a reasonable length of time to wait
  - SHOULD (RFCs 1122 & 2988) use default of 3 seconds
  - Some implementations instead use 8 seconds
SYN Loss and Web Downloads

- User clicks on a hypertext link
  - Browser creates a socket and does a "connect"
  - The "connect" triggers the OS to transmit a SYN
- If the SYN is lost…
  - 3-6 seconds of delay: can be very long
  - User may become impatient
  - … and click the hyperlink again, or click "reload"
- User triggers an "abort" of the "connect"
  - Browser creates a new socket and another "connect"
  - Essentially, forces a faster send of a new SYN packet!
  - Sometimes very effective, and the page comes quickly

Tearing Down the Connection

Normal Termination, One Side At A Time

- Finish (FIN) to close and receive remaining bytes
  - FIN occupies one byte in the sequence space
- Other host acks the byte to confirm
- Closes A’s side of the connection, but not B’s
  - Until B likewise sends a FIN
  - Which A then acks

Normal Termination, Both Together

- Same as before, but B sets FIN with their ack of A’s FIN

Abrupt Termination

- A sends a RESET (RST) to B
  - E.g., because application process on A crashed
- That’s it
  - B does not ack the RST
  - Thus, RST is not delivered reliably
  - And: any data in flight is lost
  - But: if B sends anything more, will elicit another RST

TCP Header

<table>
<thead>
<tr>
<th>Source port</th>
<th>Destination port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence number</td>
<td>Acknowledgment</td>
</tr>
<tr>
<td>AckLen</td>
<td>Flags</td>
</tr>
<tr>
<td>Checksum</td>
<td>Urgent pointer</td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
</tbody>
</table>
TCP State Transitions

- CLOSED
- LISTEN
- SYN_RCVD
- SYN_SENT
- ESTABLISHED
- CLOSE_WAIT
- LAST_ACK
- CLOSING
- TIME_WAIT
- FIN_WAIT_2
- FIN_WAIT_1

TCP Header

- Source port
- Destination port
- Sequence number
- Acknowledgment
- HdrLen
- Flags
- Advertised window
- Checksum
- Urgent pointer
- Options (variable)
- Data

An Simpler View of the Client Side

- CLOSED
- SYN_SENT
- TIME_WAIT
- ESTABLISHED
- FIN_WAIT

TCP Header

- Source port
- Destination port
- Sequence number
- Acknowledgment
- HdrLen
- Flags
- Advertised window
- Checksum
- Urgent pointer
- Options (variable)
- Data

Recap: Sliding Window (so far)

- What does TCP do?
  - ARQ windowing, set-up, tear-down
- Flow Control in TCP
  - Both sender & receiver maintain a window
  - Left edge of window:
    - Sender: beginning of unacknowledged data
    - Receiver: beginning of undelivered data
  - Right edge: Left edge + constant
    - constant only limited by buffer size in the transport layer
Solution: Advertised Window (Flow Control)

- Receiver uses an “Advertised Window” (W) to prevent sender from overflowing its window
  - Receiver indicates value of W in ACKs
  - Sender limits number of bytes it can have in flight \( \leq W \)

Sliding Window w/ Flow Control

- Sender: window advances when new data ack’d
- Receiver: window advances as receiving process consumes data
- Receiver advertises to the sender where the receiver window currently ends (“righthand edge”)
  - Sender agrees not to exceed this amount
Advertised Window Limits Rate

• Sender can send no faster than W/RTT bytes/sec
• Receiver only advertises more space when it has consumed old arriving data
• In original TCP design, that was the sole protocol mechanism controlling sender’s rate
• What’s missing?

TCP

• The concepts underlying TCP are simple
  – acknowledgments (feedback)
  – timers
  – sliding windows
  – buffer management
  – sequence numbers

TCP

• The concepts underlying TCP are simple
• But tricky in the details
• Do the details matter?

TCP

• The concepts underlying TCP are simple
• But tricky in the details

Sizing Windows for Congestion Control

• What are the problems?
• How might we address them?
We have seen:
- **Flow control**: adjusting the sending rate to keep from overwhelming a slow receiver

Now let’s attend…
- **Congestion control**: adjusting the sending rate to keep from overloading the network

**Congestion is undesirable**

**Typical queuing system** with bursty arrivals

- Average Packet delay vs Load
- Average Packet loss vs Load

*Must balance utilization versus delay and loss*

**Who Takes Care of Congestion?**

- **Network? End hosts? Both?**
- **TCP’s approach:**
  - **End hosts** adjust sending rate
  - Based on *implicit feedback* from network

- Not the only approach
  - A consequence of history rather than planning

**Some History: TCP in the 1980s**

- Sending rate only limited by flow control
  - Packet drops $\rightarrow$ senders (repeatedly!) retransmit a full window’s worth of packets

- Led to “congestion collapse” starting Oct. 1986
  - Throughput on the NSF network dropped from 32Kbits/s to 40bits/sec

- “Fixed” by Van Jacobson’s development of TCP’s congestion control (CC) algorithms

**Jacobson’s Approach**

- Extend TCP’s existing window-based protocol but adapt the window size in response to congestion
  - required no upgrades to routers or applications!
  - patch of a few lines of code to TCP implementations

- A pragmatic and effective solution
  - but many other approaches exist

- Extensively improved on since
  - topic now sees less activity in ISP contexts
  - but is making a comeback in datacenter environments
### Three Issues to Consider

- Discovering the available (bottleneck) bandwidth
- Adjusting to variations in bandwidth
- Sharing bandwidth between flows

### Discovering available bandwidth

- Pick sending rate to match bottleneck bandwidth
  - Without any *a priori* knowledge
  - Could be gigabit link, could be a modem

### Adjusting to variations in bandwidth

- Adjust rate to match *instantaneous* bandwidth
  - Assuming you have rough idea of bandwidth

### Multiple flows and sharing bandwidth

**Two Issues:**
- Adjust total sending rate to match bandwidth
- Allocation of bandwidth between flows

### Reality

Congestion control is a resource allocation problem involving many flows, many links, and complicated global dynamics
**View from a single flow**

- **Knee** – point after which
  - Throughput increases slowly
  - Delay increases fast

- **Cliff** – point after which
  - Throughput starts to drop to zero (congestion collapse)
  - Delay approaches infinity

**General Approaches**

(0) Send without care
- Many packet drops

(1) Reservations
- Pre-arrange bandwidth allocations
- Requires negotiation before sending packets
- Low utilization

(2) Pricing
- Don’t drop packets for the high-bidders
- Requires payment model

(3) Dynamic Adjustment
- Hosts probe network; infer level of congestion; adjust
- Network reports congestion level to hosts; hosts adjust
- Combinations of the above
- Simple to implement but suboptimal, messy dynamics

All three techniques have their place
- Generality of dynamic adjustment has proven powerful
- Doesn’t presume business model, traffic characteristics, application requirements; does assume good citizenship
TCP’s Approach in a Nutshell

- TCP connection has window
  - Controls number of packets in flight
- Sending rate: ~Window/RTT
- Vary window size to control sending rate

All These Windows...

- Congestion Window: CWND
  - How many bytes can be sent without overflowing routers
  - Computed by the sender using congestion control algorithm
- Flow control window: AdvertisedWindow (RWND)
  - How many bytes can be sent without overflowing receiver’s buffers
  - Determined by the receiver and reported to the sender
- Sender-side window = minimum\{CWND, RWND\}
  - Assume for this material that RWND >> CWND

Note

- This lecture will talk about CWND in units of MSS
  - (Recall MSS: Maximum Segment Size, the amount of payload data in a TCP packet)
  - This is only for pedagogical purposes
- In reality this is a LIE: Real implementations maintain CWND in bytes

Two Basic Questions

- How does the sender detect congestion?
- How does the sender adjust its sending rate?
  - To address three issues
    - Finding available bottleneck bandwidth
    - Adjusting to bandwidth variations
    - Sharing bandwidth

Detecting Congestion

- Packet delays
  - Tricky: noisy signal (delay often varies considerably)
- Router tell endhosts they’re congested
- Packet loss
  - Fail-safe signal that TCP already has to detect
  - Complication: non-congestive loss (checksum errors)
- Two indicators of packet loss
  - No ACK after certain time interval: timeout
  - Multiple duplicate ACKs

Not All Losses the Same

- Duplicate ACKs: isolated loss
  - Still getting ACKs
- Timeout: much more serious
  - Not enough dupacks
  - Must have suffered several losses
- We will adjust rate differently for each case
Rate Adjustment

- Basic structure:
  - Upon receipt of ACK (of new data): increase rate
  - Upon detection of loss: decrease rate

- How we increase/decrease the rate depends on the phase of congestion control we’re in:
  - Discovering available bottleneck bandwidth vs.
  - Adjusting to bandwidth variations

Bandwidth Discovery with Slow Start

- Goal: estimate available bandwidth
  - start slow (for safety)
  - but ramp up quickly (for efficiency)

- Consider
  - RTT = 100ms, MSS=1000bytes
  - Window size to fill 1Mbps of BW = 12.5 packets
  - Window size to fill 1Gbps = 12,500 packets
  - Either is possible!

“Slow Start” Phase

- Sender starts at a slow rate but increases exponentially until first loss

- Start with a small congestion window
  - Initially, CWND = 1
  - So, initial sending rate is MSS/RTT

- Double the CWND for each RTT with no loss

Slow Start in Action

- For each RTT: double CWND

- Simpler implementation: for each ACK, CWND += 1

Adjusting to Varying Bandwidth

- Slow start gave an estimate of available bandwidth

- Now, want to track variations in this available bandwidth, oscillating around its current value
  - Repeated probing (rate increase) and backoff (rate decrease)

- TCP uses: “Additive Increase Multiplicative Decrease” (AIMD)
  - We’ll see why shortly…

AIMD

- Additive increase
  - Window grows by one MSS for every RTT with no loss
  - For each successful RTT, CWND = CWND + 1
  - Simple implementation:
    - for each ACK, CWND = CWND + 1/CWND

- Multiplicative decrease
  - On loss of packet, divide congestion window in half
  - On loss, CWND = CWND/2
Leads to the TCP “Sawtooth”

Slow-Start vs. AIMD

- When does a sender stop Slow-Start and start Additive Increase?
- Introduce a “slow start threshold” ($ssthresh$)
  - Initialized to a large value
  - On timeout, $ssthresh = \text{CWND}/2$
- When $\text{CWND} = ssthresh$, sender switches from slow-start to AIMD-style increase

Why AIMD?

Recall: Three Issues

- Discovering the available (bottleneck) bandwidth
  - Slow Start
- Adjusting to variations in bandwidth
  - AIMD
- Sharing bandwidth between flows

Goals for bandwidth sharing

- Efficiency: High utilization of link bandwidth
- Fairness: Each flow gets equal share
**Why AIMD?**

- Some rate adjustment options: Every RTT, we can
  - Multiplicative increase or decrease: CWND → CWND \( a \times \text{CWND} \)
  - Additive increase or decrease: CWND → CWND + \( b \)

- Four alternatives:
  - AIAD: gentle increase, gentle decrease
  - AIMD: gentle increase, drastic decrease
  - MIAD: drastic increase, gentle decrease
  - MIMD: drastic increase and decrease

**Simple Model of Congestion Control**

- Two users
  - rates \( x_1 \) and \( x_2 \)
- Congestion when \( x_1 + x_2 > 1 \)
- Unused capacity when \( x_1 + x_2 < 1 \)
- Fair when \( x_1 = x_2 \)

**Example**

<table>
<thead>
<tr>
<th>Efficient: ( x_1 + x_2 = 1 ) Fair</th>
<th>Congested: ( x_1 + x_2 = 1.2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0.2, 0.5)</td>
<td>(0.7, 0.5)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inefficient: ( x_1 + x_2 = 0.7 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0.5, 0.5)</td>
</tr>
</tbody>
</table>

**AIAD**

- Increase: \( x + a_I \)
- Decrease: \( x - a_D \)
- Does not converge to fairness

**MIMD**

- Increase: \( x \times b_I \)
- Decrease: \( x \times b_D \)
- Does not converge to fairness

**Recall: Three Issues**

- Discovering the available (bottleneck) bandwidth
  - Slow Start
- Adjusting to variations in bandwidth
  - AIMD
- Sharing bandwidth between flows
AIMD

- Increase: $x + a_i$
- Decrease: $x \cdot b_D$
- Converges to fairness

Why is AIMD fair?
(a pretty animation...)

Two competing sessions:
- Additive increase gives slope of 1, as throughput increases
- Multiplicative decrease decreases throughput proportionally

AIAD Sharing Dynamics

TCP Congestion Control
(Gruesome) Details

Implementation

- State at sender
  - CWND (initialized to a small constant)
  - ssthresh (initialized to a large constant)
  - [Also dupACKcount and timer, as before]

- Events
  - ACK (new data)
  - dupACK (duplicate ACK for old data)
  - Timeout
Event: ACK (new data)

- If CWND < ssthresh
  - CWND += 1

- Else
  - CWND = CWND + 1/CWND

**Slow start phase**

**“Congestion Avoidance” phase** (additive increase)

Event: TimeOut

- On Timeout
  - ssthresh ← CWND/2
  - CWND ← 1

Event: dupACK

- dupACKcount ++

- If dupACKcount = 3 /* fast retransmit */
  - ssthresh = CWND/2
  - CWND = CWND/2

**Example**

Slow-start restart: Go back to CWND = 1 MSS, but take advantage of knowing the previous value of CWND

- What does TCP do?
  - ARQ windowing, set-up, tear-down
  - Flow Control in TCP
  - Congestion Control in TCP
  - AIMD, Fast-Recovery
One Final Phase: Fast Recovery

- The problem: congestion avoidance too slow in recovering from an isolated loss

Example (in units of MSS, not bytes)

- Consider a TCP connection with:
  - CWND=10 packets
  - Last ACK was for packet # 101
    - i.e., receiver expecting next packet to have seq. no. 101
  - 10 packets [101, 102, 103,..., 110] are in flight
    - Packet 101 is dropped

The problem – A timeline

- ACK 101 (due to 102) cwnd=10 dupACK#1 (no xmit)
- ACK 101 (due to 103) cwnd=10 dupACK#2 (no xmit)
- ACK 101 (due to 104) cwnd=10 dupACK#3 (no xmit)
  - RETRANSMIT 101 ssthresh=5 cwnd= 5
  - ACK 101 (due to 105) cwnd=5 + 1/5 (no xmit)
  - ACK 101 (due to 106) cwnd=5 + 2/5 (no xmit)
  - ACK 101 (due to 107) cwnd=5 + 3/5 (no xmit)
  - ACK 101 (due to 108) cwnd=5 + 4/5 (no xmit)
  - ACK 101 (due to 109) cwnd=5 + 5/5 (no xmit)
  - ACK 101 (due to 110) cwnd=5 + 6/5 (no xmit)
  - ACK 111 (due to 101) only now can we transmit new packets
  - Plus no packets in flight so ACK “locking” (to increase CWND) stalls for another RTT

Solution: Fast Recovery

Idea: Grant the sender temporary “credit” for each dupACK so as to keep packets in flight

- If dupACKcount = 3
  - ssthresh = cwnd/2
  - cwnd = ssthresh + 3
- While in fast recovery
  - cwnd = cwnd + 1 for each additional duplicate ACK
- Exit fast recovery after receiving new ACK
  - set cwnd = ssthresh

Example

- Consider a TCP connection with:
  - CWND=10 packets
  - Last ACK was for packet # 101
    - i.e., receiver expecting next packet to have seq. no. 101
  - 10 packets [101, 102, 103,..., 110] are in flight
    - Packet 101 is dropped

Timeline

- ACK 101 (due to 102) cwnd=10 dup#1
- ACK 101 (due to 103) cwnd=10 dup#2
- ACK 101 (due to 104) cwnd=10 dup#3
  - RETRANSMIT 101 ssthresh=5 cwnd= 8 (5+3)
  - ACK 101 (due to 105) cwnd=9 (no xmit)
  - ACK 101 (due to 106) cwnd=10 (no xmit)
  - ACK 101 (due to 107) cwnd=11 (xmit 111)
  - ACK 101 (due to 108) cwnd=12 (xmit 112)
  - ACK 101 (due to 109) cwnd=13 (xmit 113)
  - ACK 101 (due to 110) cwnd=14 (xmit 114)
  - ACK 111 (due to 101) cwnd = 5 (xmit 115) exiting fast recovery
  - Packets 111-114 already in flight
  - ACK 112 (due to 111) cwnd = 5 + 1/5 back in congestion avoidance
Putting it all together:
The TCP State Machine (partial)

- How are ssthresh, CWND and dupACKcount updated for each event that causes a state transition?

TCP Flavors

- TCP-Tahoe
  - cwnd = 1 on triple dupACK
- TCP-Reno
  - cwnd = 1 on timeout
  - cwnd = CWND/2 on triple dupack
- TCP-newReno
  - TCP-Reno + improved fast recovery
- TCP-SACK
  - incorporates selective acknowledgements

What does TCP do?
- ARQ windowing, set-up, tear-down
- Flow Control in TCP
- Congestion Control in TCP
  - AIMD, Fast-Recovery, Throughput

TCP Throughput Equation

A Simple Model for TCP Throughput
Some implications: (1) Fairness

Throughput, \( B = \frac{3}{2} \frac{1}{\sqrt{RTT \cdot p}} \)

- Flows get throughput inversely proportional to RTT
  - Is this fair?

Some Implications:
(2) How does this look at high speed?

- Assume that RTT = 100ms, MSS=1500bytes
- What value of \( p \) is required to go 100Gbps?
  - Roughly \( 2 \times 10^{-12} \)
- How long between drops?
  - Roughly 16.6 hours
- How much data has been sent in this time?
  - Roughly 6 petabits
- These are not practical numbers!

Some implications:
(3) Rate-based Congestion Control

Throughput, \( B = \frac{3}{2} \frac{1}{\sqrt{RTT \cdot p}} \)

- One can dispense with TCP and just match eqtn:
  - Equation-based congestion control
  - Measure drop percentage \( p \), and set rate accordingly
  - Useful for streaming applications

Some Implications: (4) Lossy Links

- TCP assumes all losses are due to congestion
- What happens when the link is lossy?
  - Throughput \( \sim \frac{1}{\sqrt{p}} \) where \( p \) is loss prob.
  - This applies even for non-congestion losses!

Other Issues: Cheating

- Cheating pays off
- Some favorite approaches to cheating:
  - Increasing CWND faster than 1 per RTT
  - Using large initial CWND
  - Opening many connections

Increasing CWND Faster

\( x \) increases by 2 per RTT
\( y \) increases by 1 per RTT

Limit rates:
\( x = 2y \)
- What does TCP do?
  - ARQ windowing, set-up, tear-down
- Flow Control in TCP
- Congestion Control in TCP
  - AIMD, Fast-Recovery, Throughput
- Limitations of TCP Congestion Control

A Closer look at problems with TCP Congestion Control

TCP State Machine

TCP State Machine
TCP Flavors

- **TCP-Tahoe**
  - \( \text{CWND} = \frac{1}{2} \) on triple dupACK

- **TCP-Reno**
  - \( \text{CWND} = 1 \) on timeout
  - \( \text{CWND} = \text{CWND}/2 \) on triple dupACK

- **TCP-newReno**
  - TCP-Reno + improved fast recovery

- **TCP-SACK**
  - incorporates selective acknowledgements

Interoperability

- How can all these algorithms coexist? Don’t we need a single, uniform standard?

- What happens if I’m using Reno and you are using Tahoe, and we try to communicate?

TCP Throughput Equation

\[
\text{Throughput} = \frac{1}{2} \sqrt{\frac{1}{\text{RTT}} \sqrt{p}}
\]

- Flows get throughput inversely proportional to RTT
- TCP unfair in the face of heterogeneous RTTs!
Implications (2): High Speed TCP

\[
\text{Throughput} = \sqrt[3]{\frac{1}{2 \times \text{RTT} \sqrt{p}}}
\]

- Assume RTT = 100ms, MSS=1500 bytes
- What value of \( p \) is required to reach 100Gbps throughput
  \(- \approx 2 \times 10^{-12}\)
- How long between drops?
  \(- \approx 16.6 \text{ hours}\)
- How much data has been sent in this time?
  \(- \approx 6 \text{ petabits}\)
- These are not practical numbers!

Adapting TCP to High Speed

- Once past a threshold speed, increase CWND faster
  - A proposed standard [Floyd'03]: once speed is past some threshold, change equation to \( p^3 \) rather than \( p^2 \)
  - Let the additive constant in AIMD depend on CWND
- Other approaches?
  - Multiple simultaneous connections (hack but works today)
  - Router-assisted approaches (will see shortly)

Implications (3): Rate-based CC

\[
\text{Throughput} = \sqrt[3]{\frac{1}{2 \times \text{RTT} \sqrt{p}}}
\]

- TCP throughput is “choppy”
  \(- \text{ repeated swings between } W/2 \text{ to } W \)
- Some apps would prefer sending at a steady rate
  \(- \text{ e.g., streaming apps} \)
- A solution: “Equation-Based Congestion Control”
  \(- \text{ ditch TCP's increase/decrease rules and just follow the equation} \)
  \(- \text{ measure drop percentage } p, \text{ and set rate accordingly} \)
- Following the TCP equation ensures we’re “TCP friendly”
  \(- \text{ i.e., use no more than TCP does in similar setting} \)

Other Limitations of TCP Congestion Control

(4) Loss not due to congestion?

- TCP will confuse any loss event with congestion
- Flow will cut its rate
  \(- \text{ Throughput } \sim 1/\sqrt{p} \text{ where } p \text{ is loss prob.} \)
  \(- \text{ Applies even for non-congestion losses!} \)
- We’ll look at proposed solutions shortly...

(5) How do short flows fare?

- 50% of flows have < 1500B to send; 80% < 100KB
- Implication (1): short flows never leave slow start!
  \(- \text{ short flows never attain their fair share} \)
- Implication (2): too few packets to trigger dupACKs
  \(- \text{ Isolated loss may lead to timeouts} \)
  \(- \text{ At typical timeout values of } \approx 500\text{ms, might severely impact flow completion time} \)
(6) TCP fills up queues → long delays

- A flow deliberately overshoots capacity, until it experiences a drop

- Means that delays are large for everyone
  - Consider a flow transferring a 10GB file sharing a bottleneck link with 10 flows transferring 100B

(7) Cheating

- Three easy ways to cheat
  - Increasing CWND faster than +1 MSS per RTT

Increasing CWND Faster

- Limit rates: $x = 2y$

Open Many Connections

Assume
- A starts 10 connections to B
- D starts 1 connection to E
- Each connection gets about the same throughput

Then A gets 10 times more throughput than D

(7) Cheating

- Three easy ways to cheat
  - Increasing CWND faster than +1 MSS per RTT
  - Opening many connections
  - Using large initial CWND

- Why hasn’t the Internet suffered a congestion collapse yet?
(8) CC intertwined with reliability

- Mechanisms for CC and reliability are tightly coupled
  - CWND adjusted based on ACKs and timeouts
  - Cumulative ACKs and fast retransmit/recovery rules
- Complicates evolution
  - Consider changing from cumulative to selective ACKs
  - A failure of modularity, not layering
- Sometimes we want CC but not reliability
  - e.g., real-time applications
  - Sometimes we want reliability but not CC (?)

Recap: TCP problems

- Misled by non-congestion losses
  - Fills up queues leading to high delays
  - Short flows complete before discovering available capacity
  - AIMD impractical for high speed links
  - Sawtooth discovery too choppy for some apps
  - Unfair under heterogeneous RTTs
  - Tight coupling with reliability mechanisms
  - Endhosts can cheat

Could fix many of these with some help from routers!

Router-Assisted Congestion Control

- Three tasks for CC:
  - Isolation/fairness
  - Adjustment
  - Detecting congestion

Fairness: General Approach

- Routers classify packets into "flows"
  - [For now] flows are packets between same source/destination
- Each flow has its own FIFO queue in router
- Router services flows in a fair fashion
  - When line becomes free, take packet from next flow in a fair order
- What does "fair" mean exactly?
Max-Min Fairness

- Given set of bandwidth demands $r_i$ and total bandwidth $C$, max-min bandwidth allocations are:
  $$a_i = \min(f, r_i)$$
  where $f$ is the unique value such that $\text{Sum}(a_i) = C$

Example

- $C = 10$; $r_1 = 8, r_2 = 6, r_3 = 2$; $N = 3$
- $C/3 = 3.33 →$
  - Can service all of $r_3$
  - Remove $r_3$ from the accounting: $C = C - r_3 = 8$; $N = 2$
- $C/2 = 4 →$
  - Can’t service all of $r_1$ or $r_2$
  - So hold them to the remaining fair share: $f = 4$

Max-Min Fairness

- Given set of bandwidth demands $r_i$ and total bandwidth $C$, max-min bandwidth allocations are:
  $$a_i = \min(f, r_i)$$
  where $f$ is the unique value such that $\text{Sum}(a_i) = C$

  - Property:
    - If you don’t get full demand, no one gets more than you

  - This is what round-robin service gives if all packets are the same size

How do we deal with packets of different sizes?

- Mental model: Bit-by-bit round robin (“fluid flow”)

- Can you do this in practice?

- No, packets cannot be preempted

- But we can approximate it
  - This is what “fair queuing” routers do

Fair Queuing (FQ)

- For each packet, compute the time at which the last bit of a packet would have left the router if flows are served bit-by-bit
- Then serve packets in the increasing order of their deadlines

Example

- For each flow, compute the time at which the last bit of a packet would have left the router
- Serve packets in the increasing order of their deadlines
- This is what “fair queuing” routers do
Fair Queuing (FQ)

- Think of it as an implementation of round-robin generalized to the case where not all packets are equal sized
- Weighted fair queuing (WFQ): assign different flows different shares
- Today, some form of WFQ implemented in almost all routers
  - Not the case in the 1980-90s, when CC was being developed
  - Mostly used to isolate traffic at larger granularities (e.g., per-prefix)

FQ vs. FIFO

- FQ advantages:
  - Isolation: cheating flows don’t benefit
  - Bandwidth share does not depend on RTT
  - Flows can pick any rate adjustment scheme they want
- Disadvantages:
  - More complex than FIFO: per flow queue/state, additional per-packet book-keeping

FQ in the big picture

- FQ does not eliminate congestion \(\rightarrow\) it just manages the congestion

Fairness is a controversial goal

- What if you have 8 flows, and I have 4?
  - Why should you get twice the bandwidth
- What if your flow goes over 4 congested hops, and mine only goes over 1?
  - Why shouldn’t you be penalized for using more scarce bandwidth?
- And what is a flow anyway?
  - TCP connection
  - Source-Destination pair?
  - Source?

Router-Assisted Congestion Control

- CC has three different tasks:
  - Isolation/fairness
  - Rate adjustment
  - Detecting congestion
Why not just let routers tell endhosts what rate they should use?

- Packets carry “rate field”
- Routers insert “fair share” $f$ in packet header
  - Calculated as with FQ
- End-hosts set sending rate (or window size) to $f$
  - Hopefully (still need some policing of endhosts!)
- This is the basic idea behind the “Rate Control Protocol” (RCP) from Dukkipati et al. ’07

Flow Completion Time: TCP vs. RCP (Ignore XCP)

Why the improvement?

Router-Assisted Congestion Control

- CC has three different tasks:
  - Isolation/fairness
  - Rate adjustment
  - Detecting congestion

Explicit Congestion Notification (ECN)

- Single bit in packet header; set by congested routers
  - If data packet has bit set, then ACK has ECN bit set
- Many options for when routers set the bit
  - Tradeoff between (link) utilization and (packet) delay
- Congestion semantics can be exactly like that of drop
  - I.e., endhost reacts as though it saw a drop
- Advantages:
  - Don’t confuse corruption with congestion; recovery w/ rate adjustment
  - Can serve as an early indicator of congestion to avoid delays
  - Easy (easier) to incrementally deploy

One final proposal: Charge people for congestion!

- Use ECN as congestion markers
- Whenever I get an ECN bit set, I have to pay $5
- Now, there’s no debate over what a flow is, or what fair is…
- Idea started by Frank Kelly here in Cambridge
  - “optimal” solution, backed by much math
  - Great idea: simple, elegant, effective
  - Unclear that it will impact practice — although London congestion works
Some TCP issues outstanding...

Synchronized Flows
• Aggregate window has same dynamics
• Therefore buffer occupancy has same dynamics
• Rule-of-thumb still holds.

Many TCP Flows
• Independent, desynchronized
• Central limit theorem says the aggregate becomes Gaussian
• Variance (buffer size) decreases as $N$ increases

TCP in detail

• What does TCP do?
  – ARQ windowing, set-up, tear-down
• Flow Control in TCP
• Congestion Control in TCP
  – AIMD, Fast-Recovery, Throughput
• Limitations of TCP Congestion Control
• Router-assisted Congestion Control

Recap

• TCP:
  – somewhat hacky
  – but practical/deployable
  – good enough to have raised the bar for the deployment of new, more optimal, approaches
  – though the needs of datacenters might change the status quos
Topic 6 – Applications

- Overview
- Infrastructure Services (DNS)
- Traditional Applications (web)
- Multimedia Applications (SIP)
- P2P Networks

Client-server architecture

- server:
  - always-on host
  - permanent IP address
  - server farms for scaling
- clients:
  - communicate with server
  - may be intermittently connected
  - may have dynamic IP addresses
  - do not communicate directly with each other

Pure P2P architecture

- no always-on server
- arbitrary end systems directly communicate
- peers are intermittently connected and change IP addresses

Highly scalable but difficult to manage

Hybrid of client-server and P2P

Skype
- voice-over-IP P2P application
- centralized server: finding address of remote party:
- client-client connection: direct (not through server)

Instant messaging
- chatting between two users is P2P
- centralized service: client presence detection/location
  - user registers its IP address with central server when it comes online
  - user contacts central server to find IP addresses of buddies

Addressing processes

- to receive messages, process must have identifier
- host device has unique 32-bit IP address
- Or does IP address of host on which process runs suffice for identifying the process?
  - A: No, many processes can be running on same host

- identifier includes both IP address and port numbers associated with process on host.
- Example port numbers:
  - HTTP server: 80
  - Mail server: 25
- to send HTTP message to yuba.stanford.edu web server:
  - IP address: 171.64.74.58
  - Port number: 80
- more shortly...

Recall: Multiplexing is a service provided by (each) layer too!

Multiplexing

Lower channel

Demultiplexing

Application: one web-server multiple sets of content
Host: one machine multiple services
Network: one physical box multiple addresses (like vns.cl.cam.ac.uk)

UNIX:/etc/protocols = examples of different transport-protocols on top of IP
UNIX:/etc/services = examples of different (TCP/UDP) services – by port

(These files are an example of a (static)
App-layer protocol defines

- Types of messages exchanged, e.g., request, response
- Message syntax: what fields in messages & how fields are delineated
- Message semantics: meaning of information in fields
- Rules for when and how processes send & respond to messages

Public-domain protocols:
- defined in RFCs
- allows for interoperability
  - e.g., HTTP, SMTP

Proprietary protocols:
- e.g., Skype

What transport service does an app need?

Data loss
- some apps (e.g., audio) can tolerate some loss
- other apps (e.g., file transfer, telnet) require 100% reliable data transfer

Throughput
- some apps (e.g., multimedia) require minimum amount of throughput to be "effective"
- other apps ("elastic apps") make use of whatever throughput they get

Timing
- some apps (e.g., Internet telephony, interactive games) require low delay to be "effective"

Security
- Encryption, data integrity, ...

Shocked?
I seriously doubt it...
Recall the two most common TCP and UDP

Naming

- Internet has one global system of addressing: IP
  - By explicit design

- And one global system of naming: DNS
  - Almost by accident

- At the time, only items worth naming were hosts
  - A mistake that causes many painful workarounds

- Everything is now named relative to a host
  - Content is most notable example (URL structure)

Logical Steps in Using Internet

- Human has name of entity she wants to access
  - Content, host, etc.

- Invokes an application to perform relevant task
  - Using that name

- App invokes DNS to translate name to address

- App invokes transport protocol to contact host
  - Using address as destination

Addresses vs Names

- Scope of relevance:
  - App/user is primarily concerned with names
  - Network is primarily concerned with addresses

- Timescales:
  - Name lookup once (or get from cache)
  - Address lookup on each packet

- When moving a host to a different subnet:
  - The address changes
  - The name does not change

- When moving content to a differently named host
  - Name and address both change!

Relationship Between Names & Addresses

- Addresses can change underneath
  - Move www.bbc.co.uk to 212.58.246.92
  - Humans/Apps should be unaffected

- Name could map to multiple IP addresses
  - www.bbc.co.uk to multiple replicas of the Web site
  - Enables
    - Load-balancing
    - Reducing latency by picking nearby servers

- Multiple names for the same address
  - E.g., aliases like www.bbc.co.uk and bbc.co.uk
  - Mnemonic stable name, and dynamic canonical name
  - Canonical name = actual name of host
Mapping from Names to Addresses

- Originally: per-host file /etc/hosts
  - SRI (Menlo Park) kept master copy
  - Downloaded regularly
  - Flat namespace
- Single server not resilient, doesn’t scale
  - Adopted a distributed hierarchical system
- Two intertwined hierarchies:
  - Infrastructure: hierarchy of DNS servers
  - Naming structure: www.bbc.co.uk

Domain Name System (DNS)

- Top of hierarchy: Root
  - Location hardwired into other servers
- Next Level: Top-level domain (TLD) servers
  - .com, .edu, etc.
  - .uk, .au, .to, etc.
  - Managed professionally
- Bottom Level: Authoritative DNS servers
  - Actually do the mapping
  - Can be maintained locally or by a service provider

Distributed Hierarchical Database

DNS Root Servers

- 13 root servers (see http://www.root-servers.org/)
  - Labeled A through M
  - Does this scale?

DNS Root

- Located in Virginia, USA
- How do we make the root scale?
Using DNS

- Two components
  - Local DNS servers
  - Resolver software on hosts
- Local DNS server ("default name server")
  - Usually near the endhosts that use it
  - Local hosts configured with local server (e.g., `/etc/resolv.conf`) or learn server via DHCP
- Client application
  - Extract server name (e.g., from the URL)
  - Do `gethostbyname()` to trigger resolver code

DNS name resolution **recursive** example

**Recursive query**
- Puts burden of name resolution on contacted name server
- Heavy load?

**Iterative example**

How Does Resolution Happen?

- Host at `cl.cam.ac.uk` wants IP address for `www.stanford.edu`
- **Iterative** example

Recursive and Iterative Queries - **Hybrid** case

- **Recursive** query
  - Ask server to get answer for you
  - E.g., requests 1, 2 and responses 9, 10
- **Iterative** query
  - Ask server who to ask next
  - E.g., all other request-response pairs

DNS Caching

- Performing all these queries takes time
  - And all this before actual communication takes place
  - E.g., 1-second latency before starting Web download
- **Caching** can greatly reduce overhead
  - The top-level servers very rarely change
  - Popular sites (e.g., www.bbc.co.uk) visited often
  - Local DNS server often has the information cached
- How DNS caching works
  - DNS servers cache responses to queries
  - Responses include a "time to live" (TTL) field
  - Server deletes cached entry after TTL expires

Negative Caching

- Remember things that don’t work
  - Misspellings like bbc.co.uk and www.bbc.com.uk
  - These can take a long time to fail the first time
  - Good to remember that they don’t work
  - ... so the failure takes less time the next time around
- But: negative caching is **optional**
  - And not widely implemented
Reliability

- DNS servers are replicated (primary/secondary)
  - Name service available if at least one replica is up
  - Queries can be load-balanced between replicas
- Usually, UDP used for queries
  - Need reliability: must implement this on top of UDP
  - Spec supports TCP too, but not always implemented
- Try alternate servers on timeout
  - Exponential backoff when retrying same server
- Same identifier for all queries
  - Don't care which server responds

DNS Measurements (MIT data from 2000)

- What is being looked up?
  - ~60% requests for A records
  - ~25% for PTR records
  - ~5% for MX records
  - ~6% for ANY records
- How long does it take?
  - Median ~100msec (but 90th percentile ~500msec)
  - 80% have no referrals; 99.9% have fewer than four
- Query packets per lookup: ~2.4
  - But this is misleading....

DNS Measurements (MIT data from 2000)

- Does DNS give answers?
  - ~23% of lookups fail to elicit an answer!
  - ~13% of lookups result in NXDOMAIN (or similar)
    - Mostly reverse lookups
    - Only ~64% of queries are successful!
    - How come the web seems to work so well?
- ~63% of DNS packets in unanswered queries!
  - Failing queries are frequently retransmitted
  - 99.9% successful queries have ≤2 retransmissions

DNS Measurements (MIT data from 2000)

- Top 10% of names accounted for ~70% of lookups
  - Caching should really help!
- 9% of lookups are unique
  - Cache hit rate can never exceed 91%
- Cache hit rates ~75%
  - But caching for more than 10 hosts doesn't add much

A Common Pattern....

- Distributions of various metrics (file lengths, access patterns, etc.) often have two properties:
  - Large fraction of total metric in the top 10%
  - Sizable fraction (~10%) of total fraction in low values
- Not an exponential distribution
  - Large fraction is in top 10%
  - But low values have very little of overall total
- Lesson: have to pay attention to both ends of dist.
- Here: caching helps, but not a panacea

Moral of the Story

- If you design a highly resilient system, many things can be going wrong without you noticing it!

and this is a good thing
Cache Poisoning, an old badness example

• Suppose you are a Bad Guy and you control the name server for foobar.com. You receive a request to resolve www.foobar.com and reply:

Evidence of the attack disappears 5 seconds later!

DNS and Security

• No way to verify answers
  – Opens up DNS to many potential attacks
  – DNSSEC fixes this

• Most obvious vulnerability: recursive resolution
  – Using recursive resolution, host must trust DNS server
  – When at Starbucks, server is under their control
  – And can return whatever values it wants

• More subtle attack: Cache poisoning
  – Those “additional” records can be anything!

Why is the web so successful?

• What do the web, youtube, facebook, tumblr, twitter, flickr, …… have in common?
  – The ability to self-publish

• Self-publishing that is easy, independent, free

• No interest in collaborative and idealistic endeavor
  – People aren’t looking for Nirvana (or even Xanadu)
  – People also aren’t looking for technical perfection

• Want to make their mark, and find something neat
  – Two sides of the same coin, creates synergy
  – “Performance” more important than dialogue…. 

Web Components

• Infrastructure:
  – Clients
  – Servers
  – Proxies

• Content:
  – Individual objects (files, etc.)
  – Web sites (coherent collection of objects)

• Implementation
  – HTML: formatting content
  – URL: naming content
  – HTTP: protocol for exchanging content

Any content not just HTML!

HTML: HyperText Markup Language

• A Web page has:
  – Base HTML file
  – Referenced objects (e.g., images)

• HTML has several functions:
  – Format text
  – Reference images
  – Embed hyperlinks (HREF)

URL Syntax

```plaintext
protocol : //hostname[ : port ][ /directorypath ] /resource
```

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol</td>
<td>http, ftp, https, smtp, rtsp, etc.</td>
</tr>
<tr>
<td>hostname</td>
<td>DNS name, IP address</td>
</tr>
<tr>
<td>port</td>
<td>Defaults to protocol’s standard port e.g. http: 80; https: 443</td>
</tr>
<tr>
<td>directory path</td>
<td>Hierarchical, reflecting file system</td>
</tr>
<tr>
<td>resource</td>
<td>Identifies the desired resource</td>
</tr>
</tbody>
</table>

Can also extend to program executions:

http://us.f413.mail.yahoo.com/ym/ShowLetter?box=0B%40Bulk&MsgId=2604_1744106_29699_12123_1261_0_289_17_3052_128957110&smailaccount=email&date=2019-11-04&issue=19
http://www.example.com/view=summary

HyperText Transfer Protocol (HTTP)

- Request-response protocol
- Reliance on a global namespace
- Resource metadata
- Stateless
- ASCII format

Steps in HTTP Request

- HTTP Client initiates TCP connection to server
  - SYN
  - SYNACK
  - ACK
- Client sends HTTP request to server
  - Can be piggybacked on TCP's ACK
- HTTP Server responds to request
- Client receives the request, terminates connection
- TCP connection termination exchange

How many RTTs for a single request?

Different Forms of Server Response

- Return a file
  - URL matches a file (e.g., /www/index.html)
  - Server returns file as the response
  - Server generates appropriate response header
- Generate response dynamically
  - URL triggers a program on the server
  - Server runs program and sends output to client
- Return meta-data with no body

HTTP Resource Meta-Data

- Meta-data
  - Info about a resource, stored as a separate entity
- Examples:
  - Size of resource, last modification time, type of content
- Usage example: Conditional GET Request
  - If unchanged, “HTTP/1.1 304 Not Modified”
  - No body in the server’s response, only a header

HTTP is Stateless

- Each request-response treated independently
  - Servers not required to retain state
- Good: Improves scalability on the server-side
  - Failure handling is easier
  - Can handle higher rate of requests
  - Order of requests doesn’t matter
- Bad: Some applications need persistent state
  - Need to uniquely identify user or store temporary info
  - e.g., Shopping cart, user profiles, usage tracking, …
State in a Stateless Protocol:

Cookies

- Client-side state maintenance
  - Client stores small state on behalf of server
  - Client sends state in future requests to the server
- Can provide authentication

HTTP Performance

- Most Web pages have multiple objects
  - e.g., HTML file and a bunch of embedded images
- How do you retrieve those objects (naively)?
  - One item at a time
- Put stuff in the optimal place?
  - Where is that precisely?
    - Enter the Web cache and the CDN

Fetch HTTP Items: Stop & Wait

Improving HTTP Performance:

Concurrent Requests & Responses

- Use multiple connections in parallel
- Does not necessarily maintain order of responses

- Client = ☐
- Server = ☐
- Network = ☐ Why?

Improving HTTP Performance:

Pipelined Requests & Responses

- Batch requests and responses
  - Reduce connection overhead
  - Multiple requests sent in a single batch
  - Maintains order of responses
  - Item 1 always arrives before item 2
- How is this different from concurrent requests/responses?
  - Single TCP connection

Improving HTTP Performance:

Persistent Connections

- Enables multiple transfers per connection
  - Maintain TCP connection across multiple requests
  - Including transfers subsequent to current page
  - Client or server can tear down connection
- Performance advantages:
  - Avoid overhead of connection set-up and tear-down
  - Allow TCP to learn more accurate RTT estimate
  - Allow TCP congestion window to increase
    - i.e., leverage previously discovered bandwidth
- Default in HTTP/1.1
HTTP evolution

- 1.0 – one object per TCP: simple but slow
- Parallel connections - multiple TCP, one object each: wastes b/w, may be svr limited, out of order
- 1.1 pipelining – aggregate retrieval time: ordered, multiple objects sharing single TCP
- 1.1 persistent – aggregate TCP overhead: lower overhead in time, increase overhead at ends (e.g., when should/do you close the connection?)

Scorecard: Getting n Small Objects

Time dominated by latency

- One-at-a-time: ~2n RTT
- Persistent: ~(n+1)RTT
- M concurrent: ~2[n/m] RTT
- Pipelined: ~2 RTT
- Pipelined/Persistent: ~2 RTT first time, RTT later

Scorecard: Getting n Large Objects

Time dominated by bandwidth

- One-at-a-time: ~nF/B
- M concurrent: ~[n/m] F/B
  – assuming shared with large population of users
- Pipelined and/or persistent: ~nF/B
  – The only thing that helps is getting more bandwidth..

Improving HTTP Performance: Caching

- Many clients transfer same information
  – Generates redundant server and network load
  – Clients experience unnecessary latency

- Why does caching work?
  – Exploits locality of reference
- How well does caching work?
  – Very well, up to a limit
  – Large overlap in content
  – But many unique requests

Improving HTTP Performance: Caching: How

- Modifier to GET requests:
  – If-modified-since – returns “not modified” if resource not modified since specified time
- Response header:
  – Expires – how long it’s safe to cache the resource
  – No-cache – ignore all caches; always get resource directly from server

Improving HTTP Performance: Caching: Why

- Motive for placing content closer to client:
  – User gets better response time
  – Content providers get happier users
  – Network gets reduced load
Improving HTTP Performance:
Caching on the Client

Example: Conditional GET Request
- Return resource only if it has changed at the server
  - Save server resources!

GET /~awm22/win HTTP/1.1
Host: www.cl.cam.ac.uk
User-Agent: Mozilla/4.0.3
If-Modified-Since: Sun, 27 Aug 2006 22:25:50 GMT

- HOW?
  - Client specifies “if-modified-since” time in request
  - Server compares this against “last modified” time of desired resource
  - Server returns “304 Not Modified” if resource has not changed
  - ... or a “200 OK” with the latest version otherwise

Improving HTTP Performance:
Caching with Reverse Proxies

Cache documents close to server
- decrease server load
- Typically done by content providers
- Only works for static(*) content
  (*) static can also be snapshots of dynamic content

Clients
ISP
ISP
ISP
ISP
Reverse proxies
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISP
ISA
Hosting: Multiple Sites Per Machine

- Multiple Web sites on a single machine
  - Hosting company runs the Web server on behalf of multiple sites (e.g., www.foo.com and www.bar.com)
- Problem: GET /index.html
- Solutions:
  - Multiple server processes on the same machine
    - Have a separate IP address (or port) for each server
  - Include site name in HTTP request
    - Single Web server process with a single IP address
    - Client includes "Host" header (e.g., Host: www.foo.com)
    - Required header with HTTP/1.1

Hosting: Multiple Machines Per Site

- Replicate popular Web site across many machines
  - Helps to handle the load
  - Places content closer to clients
- Helps when content isn’t cacheable
- Problem: Want to direct client to particular replica
  - Balance load across server replicas
  - Pair clients with nearby servers

Multi-Hosting at Single Location

- Single IP address, multiple machines
  - Run multiple machines behind a single IP address
  
  ![Load Balancer Diagram]

  - Ensure all packets from a single TCP connection go to the same replica

Multi-Hosting at Several Locations

- Multiple addresses, multiple machines
  - Same name but different addresses for all of the replicas
  - Configure DNS server to return closest address

CDN examples round-up

- CDN using DNS
  - DNS has information on loading/distribution/location

- CDN using anycast
  - same address from DNS name but local routes

- CDN based on rewriting HTML URLs
  - (akami example just covered – akami uses DNS too)

SIP – Session Initiation Protocol

Session?

Anyone smell an OSI / ISO standards document burning?
SIP - VoIP

Establishing communication through SIP proxies.

SIP?

- SIP – bringing the fun/complexity of telephony to the Internet
  - User location
  - User availability
  - User capabilities
  - Session setup
  - Session management
    - (e.g. “call forwarding”)

H.323 – ITU

- Why have one standard when there are at least two….
- The full H.323 is hundreds of pages
  - The protocol is known for its complexity – an ITU hallmark
- SIP is not much better
  - IETF grew up and became the ITU….

Multimedia Applications

Message flow for a basic SIP session

The (still?) missing piece: Resource Allocation for Multimedia Applications

I can ‘differentiate’ VoIP from data but…
I can only control data going into the Internet

Multimedia Applications

- Resource Allocation for Multimedia Applications

Admission control using session control protocol.
Resource Allocation for Multimedia Applications

So where does it happen?
Inside single institutions or domains of control… (Universities, Hospitals, big corp…)

What about my aDSL/CABLE/etc. it combines voice and data?
Phone company controls the multiplexing on the line and throughout their own network too…..

Co-ordination of SIP signaling and resource reservation.

P2P – efficient network use that annoys the ISP

Pure P2P architecture

- no always-on server
- arbitrary end systems directly communicate
- peers are intermittently connected and change IP addresses

Three topics:
- File distribution
- Searching for information
- Case Study: Skype

File Distribution: Server-Client vs P2P

Question: How much time to distribute file from one server to N peers?

File distribution time: server-client

- server sequentially sends N copies:
  - \(NF/u_s\) time
- client i takes \(F/d_i\) time to download

\[
\text{Time to distribute } F \text{ to } N \text{ clients using client/server approach} = d_{ss} = \max \left\{ \frac{NF}{u_s}, \frac{F}{\min(d)} \right\}
\]

increases linearly in \(N\) (for large \(N\))

File distribution time: P2P

- server must send one copy:
  - \(F/u_s\) time
- client i takes \(F/d_i\) time to download
- \(NF\) bits must be downloaded (aggregate)
  - fastest possible upload rate: \(u_s + \sum u_i\)

\[
d_{2P} = \max \left\{ \frac{F}{u_s}, \frac{F}{\min(d)} + \frac{NF}{u_s + \sum u_i} \right\}
\]
Server-client vs. P2P: example

Client upload rate = \( u \), \( f/u = 1 \) hour, \( u = 10u_s \), \( d_{\text{min}} \geq u_s \)

File distribution: BitTorrent*

*rather old BitTorrent

BitTorrent (1)

- file divided into 256KB chunks.
- peer joining torrent:
  - has no chunks, but will accumulate them over time
  - registers with tracker to get list of peers, connects to subset of peers ("neighbors")
- while downloading, peer uploads chunks to other peers.
- peers may come and go
- once peer has entire file, it may (selfishly) leave or (altruistically) remain

BitTorrent (2)

Pulling Chunks

- at any given time, different peers have different subsets of file chunks
- periodically, a peer (Alice) asks each neighbor for list of chunks that they have.
- Alice sends requests for her missing chunks
  - rarest first

Sending Chunks: Tit-for-tat

- Alice sends chunks to four neighbors currently sending her chunks at the highest rate
- re-evaluate top 4 every 10 secs
- every 30 secs: randomly select another peer, starts sending chunks
- newly chosen peer may join top 4
- "optimistically unchoke"

Distributed Hash Table (DHT)

- DHT = distributed P2P database
- Database has (key, value) pairs;
  - key: ss number; value: human name
  - key: content type; value: IP address
- Peers query DB with key
  - DB returns values that match the key
- Peers can also insert (key, value) peers

BitTorrent: Tit-for-tat

(1) Alice "optimistically unchokes" Bob
(2) Alice becomes one of Bob’s top-four providers; Bob reciprocates
(3) Bob becomes one of Alice’s top-four providers

With higher upload rate, can find better trading partners & get file faster!
Distributed Hash Table (DHT)

- DHT = distributed P2P database
- Database has (key, value) pairs;
  - key: ss number; value: human name
  - key: content type; value: IP address
- Peers query DB with key
  - DB returns values that match the key
- Peers can also insert (key, value) peers

DHT Identifiers

- Assign integer identifier to each peer in range [0, \(2^n\)-1].
  - Each identifier can be represented by n bits.
- Require each key to be an integer in same range.
- To get integer keys, hash original key.
  - eg, key = h("Game of Thrones season 4")
  - This is why they call it a distributed "hash" table

How to assign keys to peers?

- Central issue:
  - Assigning (key, value) pairs to peers.
- Rule: assign key to the peer that has the closest ID.
- Convention in lecture: closest is the immediate successor of the key.
- Ex: n=4; peers: 1,3,4,5,8,10,12,14;
  - key = 13, then successor peer = 14
  - key = 15, then successor peer = 1

Circular DHT (1)

- Each peer only aware of immediate successor and predecessor.
- "Overlay network"

Circular DHT with Shortcuts

- Each peer keeps track of IP addresses of predecessor, successor, short cuts.
- Reduced from 6 to 2 messages.
- Possible to design shortcuts so \(O(\log N)\) neighbors, \(O(\log N)\) messages in query
Peer Churn

To handle peer churn, require each peer to know the IP address of its two successors.
- Each peer periodically pings its two successors to see if they are still alive.

- Peer 5 abruptly leaves
- Peer 4 detects; makes 8 its immediate successor; asks 8 who its immediate successor is; makes 8’s immediate successor its second successor.
- What if peer 13 wants to join?

P2P Case study: Skype (pre-Microsoft)

- inherently P2P: pairs of users communicate.
- proprietary application-layer protocol (inferred via reverse engineering)
- hierarchical overlay with SNs
- Index maps usernames to IP addresses; distributed over SNs

Peers as relays

- Problem when both Alice and Bob are behind "NATs".
  - NAT prevents an outside peer from initiating a call to insider peer
- Solution:
  - Using Alice’s and Bob’s SNs, Relay is chosen
  - Each peer initiates session with relay
  - Peers can now communicate through NATs via relay

Summary.

- Apps need protocols too
- We covered examples from
  - Traditional Applications (web)
  - Scaling and Speeding the web (CDN/Cache tricks)
- Infrastructure Services (DNS)
  - Cache and Hierarchy
- Multimedia Applications (SIP)
  - Extremely hard to do better than worst-effort
- P2P Network examples
Topic 7: Datacenters

What we will cover

• Characteristics of a datacenter environment
  – goals, constraints, workloads, etc.
• How and why DC networks are different (vs. WAN)
  – e.g., latency, geo, autonomy, ...
• How traditional solutions fare in this environment
  – e.g., IP, Ethernet, TCP, ARP, DHCP
• Not details of how datacenter networks operate

Disclaimer

• Material is emerging (not established) wisdom
• Material is incomplete
  – many details on how and why datacenter networks operate aren’t public

Why Datacenters?

Your <public-life, private-life, banks, government> live in my datacenter.

Security, Privacy, Control, Cost, Energy, (breaking) received wisdom; all this and more come together into sharp focus in datacenters.

Do I need to labor the point?

What goes into a datacenter (network)?

• Servers organized in racks

What goes into a datacenter (network)?

• Servers organized in racks
• Each rack has a ‘Top of Rack’ (ToR) switch
What goes into a datacenter (network)?

- Servers organized in racks
- Each rack has a 'Top of Rack' (ToR) switch
- An ‘aggregation fabric’ interconnects ToR switches

Example 1

Brocade reference design

Example 2

Cisco reference design

Observations on DC architecture

- Regular, well-defined arrangement
- Hierarchical structure with rack/aggr/core layers
- Mostly homogenous within a layer
- Supports communication between servers and between servers and the external world

Contrast: ad-hoc structure, heterogeneity of WANs

What’s new?
SCALE!

How big exactly?

• 1M servers [Microsoft]
  – less than google, more than amazon

• > $1B to build one site [Facebook]

• > $20M/month/site operational costs [Microsoft ’09]

But only O(10-100) sites

What’s new?

• Scale
• Service model
  – user-facing, revenue generating services
  – multi-tenancy
  – jargon: SaaS, PaaS, DaaS, IaaS, ...

Implications

• Scale
  – need scalable solutions (duh)
  – improving efficiency, lowering cost is critical
  \( \rightarrow \) ‘scale out’ solutions w/ commodity technologies

• Service model
  – performance means $$
  – virtualization for isolation and portability

Multi-Tier Applications

• Applications decomposed into tasks
  – Many separate components
  – Running in parallel on different machines

Componentization leads to different types of network traffic

• ”North-South traffic”
  – Traffic between external clients and the datacenter
  – Handled by front-end (web) servers, mid-tier application servers, and back-end databases
  – Traffic patterns fairly stable, though diurnal variations
Componentization leads to different types of network traffic

- **“North-South traffic”**
  - Traffic between external clients and the datacenter
  - Handled by front-end (web) servers, mid-tier application servers, and back-end databases
  - Traffic patterns fairly stable, though diurnal variations

- **“East-West traffic”**
  - Traffic between machines in the datacenter
  - Comm within "big data" computations (e.g. Map Reduce)
  - Traffic may shift on small timescales (e.g., minutes)
What’s different about DC networks?

**Characteristics**
- Huge scale:
  - ~20,000 switches/routers
  - contrast: AT&T ~500 routers
- Limited geographic scope
- Single administrative domain
  - Can deviate from standards, invent your own, etc.
  - “Green field” deployment is still feasible
- Control over one/both endpoints
  - can change (say) addressing, congestion control, etc.
  - can add mechanisms for security/policy/etc. at the endpoints (typically in the hypervisor)
- Control over the placement of traffic source/sink
  - e.g., map-reduce scheduler chooses where tasks run
  - alters traffic pattern (what traffic crosses which links)
- Regular/planned topologies (e.g., trees/fat-trees)
  - Contrast: ad-hoc WAN topologies (dictated by real-world geography and facilities)

What’s different about DC networks?

**Characteristics**
- Huge scale:
- Limited geographic scope:
  - High bandwidth: 10/40/100G
  - Contrast: Cable/cDSL/WiFi
  - Very low RTT: 10s of microseconds
  - Contrast: 100s of milliseconds in the WAN
What’s different about DC networks?

Characteristics

- Huge scale
- Limited geographic scope
- Single administrative domain
- Control over one/both endpoints
- Control over the placement of traffic source/sink
- Regular/planned topologies (e.g., trees/fat-trees)
- Limited heterogeneity
  - link speeds, technologies, latencies, ...

Goals

- Extreme bisection bandwidth requirements
  - recall: all that east-west traffic
  - target: any server can communicate at its full link speed
  - problem: server’s access link is 10Gbps!

Full Bisection Bandwidth

- Build multi-stage ‘Fat Trees’ out of k-port switches
  - k/2 ports up, k/2 down
  - Supports k^3/4 hosts:
    - 48 ports, 27,648 hosts

A “Scale Out” Design

- To realize full bisectional throughput, routing must spread traffic across paths
- Enter load-balanced routing
  - How? (1) Let the network split traffic/flows at random (e.g., ECMP protocol -- RFC 2991/2992)
  - How? (2) Centralized flow scheduling?
  - Many more research proposals

What’s different about DC networks?

Goals

- Extreme bisection bandwidth requirements
- Extreme latency requirements
  - real money on the line
  - current target: 1μs RTTs
  - how? cut-through switches making a comeback
    - reduces switching time
What’s different about DC networks?

**Goals**

- Extreme bisection bandwidth requirements
- Extreme latency requirements
  - real money on the line
  - current target: 1μs RTTs
  - how? cut-through switches making a comeback
  - how? avoid congestion
    - reduces queuing delay

---

**An example problem at scale - INCAST**

![Diagram of INCAST](image)

- Synchronized mice collide.
  - Caused by Partition/Aggregate.
- \[ \text{RTO}_{\text{agg}} = 300 \text{ ms} \]
- TCP timeout

---

**Incast Workload Overfills Buffers**

- Big flows buildup queues.
  - Increased latency for short flows.

---

**Queue Buildup**

- Measurements in Bing cluster
  - For 90% packets: RTT < 1ms
  - For 10% packets: 1ms < RTT < 15ms
Link-Layer Flow Control
Common between switches but this is flow-control to the end host too...

- Another idea to reduce incast is to employ Link-Layer Flow Control.....

Recall: the Data-Link can use specially coded symbols in the coding to say “Stop” and “Start”

Link Layer Flow Control
But it’s worse than you imagine....

Double down on trouble...

Did I mention this is Link-Layer?

That means no IP control traffic, no routing messages....

A whole system waiting for one machine

Incast is very unpleasant.

Reducing the impact of HOL in Link Layer Flow Control can be done through priority queues and overtaking....

What’s different about DC networks?

Goals
- Extreme bisection bandwidth requirements
- Extreme latency requirements
- Predictable, deterministic performance
- Differentiating between tenants is key
  - e.g., "No traffic between VMs of tenant A and tenant B"
  - "Tenent X cannot consume more than XGb/s"
  - "Tenant Y’s traffic is low priority"

What’s different about DC networks?

Goals
- Extreme bisection bandwidth requirements
- Extreme latency requirements
- Predictable, deterministic performance
- Differentiating between tenants is key
- Scalability (of course)
  - Q: How’s that Ethernet spanning tree looking?
What’s different about DC networks?

Goals
• Extreme bisection bandwidth requirements
• Extreme latency requirements
• Predictable, deterministic performance
• Differentiating between tenants is key
• Scalability (of course)
• Cost/efficiency
  – focus on commodity solutions, ease of management
  – some debate over the importance in the network case

Summary
• new characteristics and goals
• some liberating, some constraining
• scalability is the baseline requirement
• more emphasis on performance
• less emphasis on heterogeneity
• less emphasis on interoperability

Computer Networking UROP
• Assessed Practicals for Computer Networking.
  – so supervisors can set/use work
  – so we can have a Computer Networking tick
    running over summer 2017

Talk to me.

Part 2 projects for 17-18
• Fancy doing something at scale or speed?

Talk to me.