The Network Layer
Network Layer Design Issues

• Store-and-Forward Packet Switching
• Services Provided to the Transport Layer
• Implementation of Connectionless Service
• Implementation of Connection-Oriented Service
• Comparison of Virtual-Circuit and Datagram Subnets
Packet Switching (e.g., Internet)

• Data traffic divided into packets
  – Each packet contains a header (with address)
• Packets travel separately through network
  – Packet forwarding based on the header
  – Network nodes may store packets temporarily
• Destination reconstructs the message
Packet Switching: Statistical Multiplexing
IP Service: Best-Effort Packet Delivery

• Packet switching
  – Divide messages into a sequence of packets
  – Headers with source and destination address

• Best-effort delivery
  – Packets may be lost
  – Packets may be corrupted
  – Packets may be delivered out of order
IP Service Model: Why Packets?

- Data traffic is bursty
  - Logging in to remote machines
  - Exchanging e-mail messages
- Don’t want to waste reserved bandwidth
  - No traffic exchanged during idle periods
- Better to allow multiplexing
  - Different transfers share access to same links
- Packets can be delivered by most anything
  - RFC 2549: IP over Avian Carriers (aka birds)
- ... still, packet switching can be inefficient
  - Extra header bits on every packet
IP Service Model: Why Best-Effort?

• IP means never having to say you’re sorry...
  – Don’t need to reserve bandwidth and memory
  – Don’t need to do error detection & correction
  – Don’t need to remember from one packet to next

• Easier to survive failures
  – Transient disruptions are okay during failover

• ... but, applications do want efficient, accurate transfer of data in order, in a timely fashion
IP Service: Best-Effort is Enough

• No error detection or correction
  – Higher-level protocol can provide error checking

• Successive packets may not follow the same path
  – Not a problem as long as packets reach the destination

• Packets can be delivered out-of-order
  – Receiver can put packets back in order (if necessary)

• Packets may be lost or arbitrarily delayed
  – Sender can send the packets again (if desired)

• No network congestion control (beyond “drop”)
  – Sender can slow down in response to loss or delay
Layering in the IP Protocols

- HTTP
- Telnet
- FTP
- DNS
- RTP

Transmission Control Protocol (TCP)

User Datagram Protocol (UDP)

Internet Protocol

- SONET
- Ethernet
- ATM
History: Why IP Packets?

- IP proposed in the early 1970s
  - Defense Advanced Research Project Agency (DARPA)
- Goal: connect existing networks
  - To develop an effective technique for multiplexed utilization of existing interconnected networks
  - E.g., connect packet radio networks to the ARPAnet
- Motivating applications
  - Remote login to server machines
  - Inherently bursty traffic with long silent periods
- Prior ARPAnet experience with packet switching
  - Previous DARPA project
  - Demonstrated store-and-forward packet switching
Other Main Driving Goals (In Order)

• Communication should continue despite failures
  – Survive equipment failure or physical attack
  – Traffic between two hosts continue on another path

• Support multiple types of communication services
  – Differing requirements for speed, latency, & reliability
  – Bidirectional reliable delivery vs. message service

• Accommodate a variety of networks
  – Both military and commercial facilities
  – Minimize assumptions about the underlying network
Other Driving Goals, Somewhat Met

• Permit distributed management of resources
  – Nodes managed by different institutions
  – ... though this is still rather challenging

• Cost-effectiveness
  – Statistical multiplexing through packet switching
  – ... though packet headers and retransmissions wasteful

• Ease of attaching new hosts
  – Standard implementations of end-host protocols
  – ... though still need a fair amount of end-host software

• Accountability for use of resources
  – Monitoring functions in the nodes
  – ... though this is still fairly limited and immature
# IP Packet Structure

<table>
<thead>
<tr>
<th>4-bit Version</th>
<th>4-bit Header Length</th>
<th>8-bit Type of Service (TOS)</th>
<th>16-bit Total Length (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>32-bit Source IP Address</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>32-bit Destination IP Address</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Options (if any)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Payload</th>
</tr>
</thead>
</table>
The IP Protocol

The IPv4 (Internet Protocol) header.

<table>
<thead>
<tr>
<th>Version</th>
<th>IHL</th>
<th>Type of service</th>
<th>Total length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Identification</td>
<td>D M F</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Time to live</td>
<td>Fragment offset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protocol</td>
<td>Header checksum</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Options (0 or more words)</td>
<td></td>
</tr>
</tbody>
</table>
IP Packet Header Fields

• 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

• 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
IP Packet Header Fields (Continued)

• Total length (16 bits)
  – Number of bytes in the packet
  – Maximum size is 63,535 bytes ($2^{16} - 1$)
  – ... though underlying links may impose harder limits

• Fragmentation information (32 bits)
  – Packet identifier, flags, and fragment offset
  – Supports dividing a large IP packet into fragments
  – ... in case a link cannot handle a large IP packet

• Time-To-Live (8 bits)
  – Used to identify packets stuck in forwarding loops
  – ... and eventually discard them from the network
Time-to-Live (TTL) Field

• Potential robustness problem
  – Forwarding loops can cause packets to cycle forever
  – Confusing if the packet arrives much later

• Time-to-live field in packet header
  – TTL field decremented by each router on the path
  – Packet is discarded when TTL field reaches 0...
  – ...and “time exceeded” message is sent to the source
Application of TTL in Traceroute

• **Time-To-Live field in IP packet header**
  – Source sends a packet with a TTL of $n$
  – Each router along the path decrements the TTL
  – “TTL exceeded” sent when TTL reaches 0

• **Traceroute tool exploits this TTL behavior**

Send packets with TTL=1, 2, … and record source of “time exceeded” message
Example Traceroute: Berkeley to CNN

Hop number, IP address, DNS name

1  169.229.62.1  inr-daedalus-0.CS.Berkeley.EDU
2  169.229.59.225  soda-cr-1-1-soda-br-6-2
3  128.32.255.169  vlan242.inr-202-doecev.Berkeley.EDU
4  128.32.0.249  gigE6-0-0.inr-666-doecev.Berkeley.EDU
5  128.32.0.66  qsv-juniper--ucb-gw.calren2.net
6  209.247.159.109  POS1-0.hsipaccess1.SanJose1.Level3.net
7  *  
8  64.159.1.46  ?
9  209.247.9.170  pos8-0.hsa2.Atlanta2.Level3.net
10  66.185.138.33  pop2-atm-P0-2.atdn.net
11  *  
12  66.185.136.17  ?
13  64.236.16.52  pop1-atl-P4-0.atdn.net

No response from router

No name resolution
Try Running Traceroute Yourself

• On UNIX machine
  – Traceroute
  – E.g., “traceroute www.cnn.com” or “traceroute 12.1.1.1”

• On Windows machine
  – Tracert
  – E.g., “tracert www.cnn.com” or “tracert 12.1.1.1”

• Common uses of traceroute
  – Discover the topology of the Internet
  – Debug performance and reachability problems
IP Packet Header Fields (Continued)

- **Protocol (8 bits)**
  - Identifies the higher-level protocol
    - E.g., “6” for the Transmission Control Protocol (TCP)
    - E.g., “17” for the User Datagram Protocol (UDP)
  - Important for demultiplexing at receiving host
    - Indicates what kind of header to expect next

```plaintext
protocol=6
  IP header
  TCP header

protocol=17
  IP header
  UDP header
```
IP Packet Header Fields (Continued)

• Checksum (16 bits)
  – Sum of all 16-bit words in the IP packet header
  – If any bits of the header are corrupted in transit
  – ... the checksum won’t match at receiving host
  – Receiving host discards corrupted packets
    • Sending host will retransmit the packet, if needed

\[
134 \\
+ 212 \\
\hline
= 346
\]

\[
134 \\
+ 216 \\
\hline
= 350 \\
\text{Mismatch!}
\]
IP Packet Header (Continued)

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

Some of the IP options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Specifies how secret the datagram is</td>
</tr>
<tr>
<td>Strict source routing</td>
<td>Gives the complete path to be followed</td>
</tr>
<tr>
<td>Loose source routing</td>
<td>Gives a list of routers not to be missed</td>
</tr>
<tr>
<td>Record route</td>
<td>Makes each router append its IP address</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Makes each router append its address and timestamp</td>
</tr>
</tbody>
</table>
What if the Source Lies?

• Source address should be the sending host
  – But, who’s checking, anyway?
  – You could send packets with any source you want

• Why would someone want to do this?
  – Launch a denial-of-service attack
    • Send excessive packets to the destination
    • ... to overload the node, or the links leading to the node
  – Evade detection by “spoofing”
    • But, the victim could identify you by the source address
    • So, you can put someone else’s source address in the packets
  – Also, an attack against the spoofed host
    • Spoofed host is wrongly blamed
    • Spoofed host may receive return traffic from the receiver
IP Addressing and Forwarding
IP Address (IPv4)

- A unique 32-bit number
- Identifies an interface (on a host, on a router, ...)
- Represented in dotted-quad notation

12, 34, 158, 5

00001100, 00100010, 10011110, 00000101
Grouping Related Hosts

- The Internet is an “inter-network”
  - Used to connect *networks* together, not *hosts*
  - Needs a way to address a network (i.e., group of hosts)

**LAN** = Local Area Network  
**WAN** = Wide Area Network
IP Address Classes

(a) 7 24
    0 Network  Host

(b) 14 16
    1 0 Network  Host

(c) 21 8
    1 1 0 Network  Host
IP Addresses

32 Bits

Class | Network | Host | Range of host addresses
--- | --- | --- | ---
A | 0 | | 1.0.0.0 to 127.255.255.255
B | 10 | | 128.0.0.0 to 191.255.255.255
C | 110 | | 192.0.0.0 to 223.255.255.255
D | 1110 | | 224.0.0.0 to 239.255.255.255
E | 1111 | | 240.0.0.0 to 255.255.255.255
### Special IP addresses.

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0</td>
<td>0 0</td>
<td>0 0</td>
<td>0 0</td>
<td>0 0</td>
<td>0 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 1 1 1</td>
<td>...</td>
<td>1 1 1 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 2 7</td>
<td></td>
<td>(Anything)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **This host**
- **A host on this network**
- **Broadcast on the local network**
- **Broadcast on a distant network**
- **Loopback**
Subnets

A campus network consisting of LANs for various departments.
Subnets (2)

A class B network subnetted into 64 subnets.
Subnetted Address

Class B address

```
11111111111111111111111111111111  00000000
```

Subnet mask (255.255.255.0)
Scalability Challenge

• Suppose hosts had arbitrary addresses
  – Then every router would need a lot of information
  – ...to know how to direct packets toward the host

---

<table>
<thead>
<tr>
<th>1.2.3.4</th>
<th>5.6.7.8</th>
<th>2.4.6.8</th>
<th>1.2.3.5</th>
<th>5.6.7.9</th>
<th>2.4.6.9</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>host</td>
<td>... host</td>
<td>host</td>
<td>host</td>
<td>... host</td>
</tr>
</tbody>
</table>

LAN 1

LAN 2

WAN

forwarding table
Hierarchical Addressing in U.S. Mail

• Addressing in the U.S. mail
  – Zip code: 08540
  – Street: Olden Street
  – Building on street: 35
  – Room in building: 306
  – Name of occupant: Jennifer Rexford

• Forwarding the U.S. mail
  – Deliver letter to the post office in the zip code
  – Assign letter to mailman covering the street
  – Drop letter into mailbox for the building/room
  – Give letter to the appropriate person
Hierarchical Addressing: IP Prefixes

- Divided into network & host portions (left and right)
- 12.34.158.0/24 is a 24-bit prefix with $2^8$ addresses
IP Address and a 24-bit Subnet Mask

Address

12  
34  
158  
5  

00001100 00100010 10011110 00000101

11111111 11111111 11111111 00000000

Mask

255 255 255 0
Scalability Improved

• Number related hosts from a common subnet
  – 1.2.3.0/24 on the left LAN
  – 5.6.7.0/24 on the right LAN
Easy to Add New Hosts

- No need to update the routers
  - E.g., adding a new host 5.6.7.213 on the right
  - Doesn’t require adding a new forwarding entry
Address Allocation
Classful Addressing

• In the olden days, only fixed allocation sizes
  – Class A: 0*
    • Very large /8 blocks (e.g., MIT has 18.0.0.0/8)
  – Class B: 10*
    • Large /16 blocks (e.g., Princeton has 128.112.0.0/16)
  – Class C: 110*
    • Small /24 blocks (e.g., AT&T Labs has 192.20.225.0/24)
  – Class D: 1110*
    • Multicast groups
  – Class E: 11110*
    • Reserved for future use

• This is why folks use dotted-quad notation!
Classless Inter-Domain Routing (CIDR)

Use two 32-bit numbers to represent a network.
Network number = IP address + Mask

IP Address : 12.4.0.0   IP Mask: 255.254.0.0

Address:
00001100 00000100 00000000 00000000

Mask:
11111111 11111110 00000000 00000000

Network Prefix:

for hosts

Written as 12.4.0.0/15
## CDR – Classless InterDomain Routing

A set of IP address assignments.

<table>
<thead>
<tr>
<th>University</th>
<th>First address</th>
<th>Last address</th>
<th>How many</th>
<th>Written as</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cambridge</td>
<td>194.24.0.0</td>
<td>194.24.7.255</td>
<td>2048</td>
<td>194.24.0.0/21</td>
</tr>
<tr>
<td>Edinburgh</td>
<td>194.24.8.0</td>
<td>194.24.11.255</td>
<td>1024</td>
<td>194.24.8.0/22</td>
</tr>
<tr>
<td>Oxford</td>
<td>194.24.16.0</td>
<td>194.24.31.255</td>
<td>4096</td>
<td>194.24.16.0/20</td>
</tr>
</tbody>
</table>
CIDR: Hierarchal Address Allocation

- Prefixes are key to Internet scalability
  - Address allocated in contiguous chunks (prefixes)
  - Routing protocols and packet forwarding based on prefixes
  - Today, routing tables contain ~150,000-200,000 prefixes

12.0.0.0/8
  - 12.0.0.0/16
  - 12.1.0.0/16
  - 12.2.0.0/16
  - 12.3.0.0/16

  - 12.254.0.0/16

  - 12.3.0.0/24
    - 12.3.1.0/24
    - 12.3.2.0/24
    - 12.3.254.0/24

  - 12.253.0.0/19
    - 12.253.1.0/19
    - 12.253.2.0/19
    - 12.253.32.0/19
    - 12.253.64.0/19
    - 12.253.96.0/19
    - 12.253.128.0/19
    - 12.253.160.0/19
Scalability: Address Aggregation

Routers in the rest of the Internet just need to know how to reach 201.10.0.0/21. The provider can direct the IP packets to the appropriate customer.
But, Aggregation Not Always Possible

*Multi-homed* customer with 201.10.6.0/23 has two providers. Other parts of the Internet need to know how to reach these destinations through *both* providers.
Scalability Through Hierarchy

• Hierarchical addressing
  – Critical for scalable system
  – Don’t require everyone to know everyone else
  – Reduces amount of updating when something changes

• Non-uniform hierarchy
  – Useful for heterogeneous networks of different sizes
  – Initial class-based addressing was far too coarse
  – Classless InterDomain Routing (CIDR) helps

• Next few slides
  – History of the number of globally-visible prefixes
  – Plots are # of prefixes vs. time

Growth faster than improvements in equipment capability
CIDR Deployed (1994-1996): Much Flatter

Efforts to aggregate (even decreases after IETF meetings!)

Good use of aggregation, and peer pressure in CIDR report

Internet boom and increased multi-homing
Long-Term View (1989-2005): Post-Boom
Obtaining a Block of Addresses

• Separation of control
  – Prefix: assigned to an institution
  – Addresses: assigned by the institution to their nodes

• Who assigns prefixes?
  – Internet Corporation for Assigned Names and Numbers
    • Allocates large address blocks to Regional Internet Registries
  – Regional Internet Registries (RIRs)
    • E.g., ARIN (American Registry for Internet Numbers)
    • Allocates address blocks within their regions
    • Allocated to Internet Service Providers and large institutions
  – Internet Service Providers (ISPs)
    • Allocate address blocks to their customers
    • Who may, in turn, allocate to their customers...
Figuring Out Who Owns an Address

• Address registries
  – Public record of address allocations
  – Internet Service Providers (ISPs) should update when giving addresses to customers
  – However, records are notoriously out-of-date

• Ways to query
  – UNIX: “whois –h whois.arin.net 128.8.130.75”
  – http://www.arin.net/whois/
  – …
Example Output for 128.8.130.75

OrgName: University of Maryland
OrgID: UNIVER-262
Address: Office of Information Technology
Address: Patuxent Building
City: College Park
StateProv: MD PostalCode: 20742
Country: US

NetRange: 128.8.0.0 - 128.8.255.255
CIDR: 128.8.0.0/16
NetName: UMDNET
NetHandle: NET-128-8-0-0-1
Parent: NET-128-0-0-0-0
NetType: Direct Assignment
NameServer: NOC.UMD.EDU
NameServer: NS1.UMD.EDU
NameServer: NS2.UMD.EDU
NameServer: NASANS4.NASA.GOV
Comment:
RegDate:
Updated: 2004-04-12

RTechHandle: UM-ORG-ARIN
RTechName: UMD DNS Admin Role Account
RTechPhone: +1-301-405-3003
RTechEmail: dnsadmin@noc.net.umd.edu

OrgAbuseHandle: UARA-ARIN
OrgAbuseName: UMD Abuse Role Account
OrgAbusePhone: +1-301-405-8787
OrgAbuseEmail: abuse@umd.edu

OrgTechHandle: UM-ORG-ARIN
OrgTechName: UMD DNS Admin Role Account
OrgTechPhone: +1-301-405-3003
OrgTechEmail: dnsadmin@noc.net.umd.edu
Are 32-bit Addresses Enough?

• Not all that many unique addresses
  – \(2^{32} = 4,294,967,296\) (just over four billion)
  – Plus, some are reserved for special purposes
  – And, addresses are allocated in larger blocks

• And, many devices need IP addresses
  – Computers, PDAs, routers, tanks, toasters, …

• Long-term solution: a larger address space
  – IPv6 has 128-bit addresses \((2^{128} = 3.403 \times 10^{38})\)

• Short-term solutions: limping along with IPv4
  – Private addresses
  – Network address translation (NAT)
  – Dynamically-assigned addresses (DHCP)
Hard Policy Questions

• How much address space per geographic region?
  – Equal amount per country?
  – Proportional to the population?
  – What about addresses already allocated?

• Address space portability?
  – Keep your address block when you change providers?
  – Pro: avoid having to renumber your equipment
  – Con: reduces the effectiveness of address aggregation

• Keeping the address registries up to date?
  – What about mergers and acquisitions?
  – Delegation of address blocks to customers?
  – As a result, the registries are horribly out of date
Packet Forwarding
Hop-by-Hop Packet Forwarding

• Each router has a forwarding table
  – Maps destination addresses...
  – ... to outgoing interfaces
• Upon receiving a packet
  – Inspect the destination IP address in the header
  – Index into the table
  – Determine the outgoing interface
  – Forward the packet out that interface
• Then, the next router in the path repeats
  – And the packet travels along the path to the destination
Separate Table Entries Per Address

- If a router had a forwarding entry per IP address
  - Match destination address of incoming packet
  - ... to the forwarding-table entry
  - ... to determine the outgoing interface

<table>
<thead>
<tr>
<th>1.2.3.4</th>
<th>5.6.7.8</th>
<th>2.4.6.8</th>
<th>1.2.3.5</th>
<th>5.6.7.9</th>
<th>2.4.6.9</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>host</td>
<td>... host</td>
<td>host</td>
<td>host</td>
<td>... host</td>
</tr>
</tbody>
</table>

LAN 1 -> router -> WAN

LAN 2 -> router -> WAN
Separate Entry Per 24-bit Prefix

- If the router had an entry per 24-bit prefix
  - Look only at the top 24 bits of the destination address
  - Index into the table to determine the next-hop interface

```
1.2.3.4  1.2.3.7  1.2.3.156
  host    host    host

LAN 1

1.2.3.0/24
5.6.7.0/24
```

```
5.6.7.8  5.6.7.9  5.6.7.212
  host    host    host

LAN
```

forwarding table

February 15
CMSC417 Set 4
63
Separate Entry Classful Address

• If the router had an entry per classful prefix
  – Mixture of Class A, B, and C addresses
  – Depends on the first couple of bits of the destination

• Identify the mask automatically from the address
  – First bit of 0: class A address (/8)
  – First two bits of 10: class B address (/16)
  – First three bits of 110: class C address (/24)

• Then, look in the forwarding table for the match
  – E.g., 1.2.3.4 maps to 1.2.3.0/24
  – Then, look up the entry for 1.2.3.0/24
  – ... to identify the outgoing interface
CIDR Makes Packet Forwarding Harder

- There’s no such thing as a free lunch
  - CIDR allows efficient use of the limited address space
  - But, CIDR makes packet forwarding much harder
- Forwarding table may have many matches
  - E.g., table entries for 201.10.0.0/21 and 201.10.6.0/23
Longest Prefix Match Forwarding

• Forwarding tables in IP routers
  – Maps each IP prefix to next-hop link(s)

• Destination-based forwarding
  – Packet has a destination address
  – Router identifies longest-matching prefix
  – Cute algorithmic problem: very fast lookups

destination
201.10.6.17

forwarding table

outgoing link
Serial0/0.1

4.0.0.0/8
4.83.128.0/17
201.10.0.0/21
201.10.6.0/23
126.255.103.0/24
Simplest Algorithm is Too Slow

• Scan the forwarding table one entry at a time
  – See if the destination matches the entry
  – If so, check the size of the mask for the prefix
  – Keep track of the entry with longest-matching prefix

• Overhead is linear in size of the forwarding table
  – Today, that means 150,000-200,000 entries!
  – And, the router may have just a few nanoseconds
  – ... before the next packet is arriving

• Need greater efficiency to keep up with line rate
  – Better algorithms
  – Hardware implementations
Patricia Tree

• Store the prefixes as a tree
  – One bit for each level of the tree
  – Some nodes correspond to valid prefixes
  – ... which have next-hop interfaces in a table

• When a packet arrives
  – Traverse the tree based on the destination address
  – Stop upon reaching the longest matching prefix
Even Faster Lookups

• Patricia tree is faster than linear scan
  – Proportional to number of bits in the address
• Patricia tree can be made faster
  – Can make a k-ary tree
    • E.g., 4-ary tree with four children (00, 01, 10, and 11)
    – Faster lookup, though requires more space
• Can use special hardware
  – Content Addressable Memories (CAMs)
  – Allows look-ups on a key rather than flat address
• Huge innovations in the mid-to-late 1990s
  – After CIDR was introduced (in 1994)
  – … and longest-prefix match was a major bottleneck
Where do Forwarding Tables Come From?

- Routers have forwarding tables
  - Map prefix to outgoing link(s)
- Entries can be statically configured
  - E.g., “map 12.34.158.0/24 to Serial0/0.1”
- But, this doesn’t adapt
  - To failures
  - To new equipment
  - To the need to balance load
  - …
- That is where other technologies come in...
  - Routing protocols, DHCP, and ARP (later in course)
What End Hosts Sending to Others?

• End host with single network interface
  – PC with an Ethernet link
  – Laptop with a wireless link

• Don’t need to run a routing protocol
  – Packets to the host itself (e.g., 1.2.3.4/32)
    • Delivered locally
  – Packets to other hosts on the LAN (e.g., 1.2.3.0/24)
    • Sent out the interface
  – Packets to external hosts (e.g., 0.0.0.0/0)
    • Sent out interface to local gateway

• How this information is learned
  – Static setting of address, subnet mask, and gateway
  – Dynamic Host Configuration Protocol (DHCP)
What About Reaching the End Hosts?

• How does the last router reach the destination?

• Each interface has a persistent, global identifier
  – MAC (Media Access Control) address
  – Burned in to the adaptors Read-Only Memory (ROM)
  – Flat address structure (i.e., no hierarchy)

• Constructing an address resolution table
  – Mapping MAC address to/from IP address
  – Address Resolution Protocol (ARP)
Conclusions

• IP address
  – A 32-bit number
  – Allocated in prefixes
  – Non-uniform hierarchy for scalability and flexibility

• Packet forwarding
  – Based on IP prefixes
  – Longest-prefix-match forwarding

• We’ll cover some topics later
  – Routing protocols, DHCP, and ARP
Routing
Routing Algorithms

• The Optimality Principle
• Shortest Path Routing
• Flooding
• Distance Vector Routing
• Link State Routing
• Hierarchical Routing
• Broadcast Routing
• Multicast Routing
• Routing for Mobile Hosts
• Routing in Ad Hoc Networks
Routing Algorithms (2)

Conflict between fairness and optimality.
What is Routing?

• A famous quotation from RFC 791

  “A name indicates what we seek. An address indicates where it is. A route indicates how we get there.”

  -- Jon Postel
Routing vs. Forwarding

• Routing: control plane
  – Computing paths the packets will follow
  – Routers talking amongst themselves
  – Individual router *creating* a forwarding table

• Forwarding: data plane
  – Directing a data packet to an outgoing link
  – Individual router *using* a forwarding table
Data and Control Planes

- Processor
- Switching Fabric
- Line card

Data plane
Control plane
Router Physical Layout

- Switch
- Linecards

Juniper T series
Cisco 12000
Line Cards (Interface Cards, Adaptors)

- Interfacing
  - Physical link
  - Switching fabric

- Packet handling
  - Packet forwarding
  - Decrement time-to-live
  - Buffer management
    - Link scheduling
    - Packet filtering
    - Rate limiting
    - Packet marking
  - Measurement

[Diagram of line cards with to/from link and to/from switch, and a process flow including receive and transmit]
Switching Fabric

• Deliver packet inside the router
  – From incoming interface to outgoing interface
  – A small network in and of itself

• Must operate very quickly
  – Multiple packets going to same outgoing interface
  – Switch scheduling to match inputs to outputs

• Implementation techniques
  – Bus, crossbar, interconnection network, ...
  – Running at a faster speed (e.g., 2X) than links
  – Dividing variable-length packets into fixed-size cells
Packet Switching
Router Processor

• So-called “Loopback” interface
  – IP address of the CPU on the router
• Interface to network administrators
  – Command-line interface for configuration
  – Transmission of measurement statistics
• Handling of special data packets
  – Packets with IP options enabled
  – Packets with expired Time-To-Live field
• Control-plane software
  – Implementation of the routing protocols
  – Creation of forwarding table for the line cards
Where do Forwarding Tables Come From?

• Routers have forwarding tables
  – Map IP prefix to outgoing link(s)
• Entries can be statically configured
  – E.g., “map 12.34.158.0/24 to Serial0/0.1”
• But, this doesn’t adapt
  – To failures
  – To new equipment
  – To the need to balance load
• That is where routing protocols come in
Computing Paths Between Routers

- Routers need to know two things
  - Which router to use to reach a destination prefix
  - Which outgoing interface to use to reach that router

- just how routers reach each other
  - How you knows how to forward packets toward z
Fairness vs. Efficiency

Network with a conflict between fairness and efficiency.
The Optimality Principle

Each portion of a best path is also a best path; the union of them to a router is a tree called the sink tree.

Network

Sink tree of best paths to router B
Computing the Shortest Paths

(assuming you already know the topology)
Shortest-Path Routing

• Path-selection model
  – Destination-based
  – Load-insensitive (e.g., static link weights)
  – Minimum hop count or sum of link weights
Shortest-Path Problem

• Given: network topology with link costs
  – \( c(x,y) \): link cost from node \( x \) to node \( y \)
  – Infinity if \( x \) and \( y \) are not direct neighbors

• Compute: least-cost paths to all nodes
  – From a given source \( u \) to all other nodes
  – \( p(v) \): predecessor node along path from source to \( v \)
Dijkstra’s Shortest-Path Algorithm

- Iterative algorithm
  - After k iterations, know least-cost path to k nodes
- \( S \): nodes whose least-cost path definitively known
  - Initially, \( S = \{u\} \) where \( u \) is the source node
  - Add one node to \( S \) in each iteration
- \( D(v) \): current cost of path from source to node \( v \)
  - Initially, \( D(v) = c(u,v) \) for all nodes \( v \) adjacent to \( u \)
  - ... and \( D(v) = \infty \) for all other nodes \( v \)
  - Continually update \( D(v) \) as shorter paths are learned
Dijsktra’s Algorithm

1. Initialization:
   2. $S = \{u\}$
   3. for all nodes $v$
      4. if (v is adjacent to u)
         5. $D(v) = c(u,v)$
      6. else $D(v) = \infty$
   7.

8. Loop
   9. find w not in S with the smallest $D(w)$
   10. add w to S
   11. update $D(v)$ for all v adjacent to w and not in S:
       12. $D(v) = \min\{D(v), D(w) + c(w,v)\}$
   13. until all nodes in S
Dijkstra’s Algorithm Example

![Graph with Dijkstra's Algorithm Example](image)
Dijkstra’s Algorithm Example
Shortest-Path Tree

- Shortest-path tree from u
- Forwarding table at u

---

<table>
<thead>
<tr>
<th>link</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>v</td>
<td>(u,v)</td>
</tr>
<tr>
<td>w</td>
<td>(u,w)</td>
</tr>
<tr>
<td>x</td>
<td>(u,w)</td>
</tr>
<tr>
<td>y</td>
<td>(u,v)</td>
</tr>
<tr>
<td>z</td>
<td>(u,v)</td>
</tr>
<tr>
<td>s</td>
<td>(u,w)</td>
</tr>
<tr>
<td>t</td>
<td>(u,w)</td>
</tr>
</tbody>
</table>
Shortest Path Algorithm (2)

A network and first five steps in computing the shortest paths from A to D. Pink arrows show the sink tree so far.
Shortest Path Algorithm (3)

Start with the sink, all other nodes are unreachable

Relaxation step. Lower distance to nodes linked to newest member of the sink tree

```c
for (p = &state[0]; p < &state[n]; p++) {
    p->predecessor = -1;
    p->length = INFINITY;
    p->label = tentative;
}
state[t].length = 0; state[t].label = permanent;
k = t;
do {
    for (i = 0; i < n; i++)
        if (dist[k][i] != 0 && state[i].label == tentative) {
            if (state[k].length + dist[k][i] < state[i].length) {
                state[i].predecessor = k;
                state[i].length = state[k].length + dist[k][i];
            }
        }
} while (k != t);
```
Shortest Path Algorithm (4)

... 

```c
k = 0; min = INFINITY;
for (i = 0; i < n; i++)
    if (state[i].label == tentative && state[i].length < min) {
        min = state[i].length;
        k = i;
    }
state[k].label = permanent;
} while (k != s);
```

Find the lowest distance, add it to the sink tree, and repeat until done.
Dijkstra's algorithm to compute the shortest path through a graph.
Dijkstra's algorithm to compute the shortest path through a graph.
Learning the Topology

(by the routers talking among themselves)
Link-State Routing

• Each router keeps track of its incident links
  – Whether the link is up or down
  – The cost on the link
• Each router broadcasts the link state
  – To give every router a complete view of the graph
• Each router runs Dijkstra’s algorithm
  – To compute the shortest paths
  – ... and construct the forwarding table
• Example protocols
  – Open Shortest Path First (OSPF)
  – Intermediate System – Intermediate System (IS-IS)
Link State Routing

Each router must do the following:
1. Discover its neighbors, learn their network address.
2. Measure the delay or cost to each of its neighbors.
3. Construct a packet telling all it has just learned.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.
Learning about the Neighbors

(a) Nine routers and a LAN. (b) A graph model of (a).
Measuring Line Cost

A subnet in which the East and West parts are connected by two lines.
Building Link State Packets

(a) A subnet.  (b) The link state packets for this subnet.
Distributing the Link State Packets

The packet buffer for router B in the previous slide

<table>
<thead>
<tr>
<th>Source</th>
<th>Seq.</th>
<th>Age</th>
<th>Send flags</th>
<th>ACK flags</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>21</td>
<td>60</td>
<td>0 1 1</td>
<td>1 0 0</td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>21</td>
<td>60</td>
<td>1 1 0</td>
<td>0 0 1</td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>21</td>
<td>59</td>
<td>0 1 0</td>
<td>1 0 1</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>20</td>
<td>60</td>
<td>1 0 1</td>
<td>0 1 0</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>21</td>
<td>59</td>
<td>1 0 0</td>
<td>0 1 1</td>
<td></td>
</tr>
</tbody>
</table>
Detecting Topology Changes

• Beaconing
  – Periodic “hello” messages in both directions
  – Detect a failure after a few missed “hellos”

• Performance trade-offs
  – Detection speed
  – Overhead on link bandwidth and CPU
  – Likelihood of false detection
Broadcasting the Link State

• Flooding
  – Node sends link-state information out its links
  – And then the next node sends out all of its links
  – ... except the one where the information arrived

(a)  
(b)  
(c)  
(d)
Broadcasting the Link State

• Reliable flooding
  – Ensure all nodes receive link-state information
  – ... and that they use the latest version

• Challenges
  – Packet loss
  – Out-of-order arrival

• Solutions
  – Acknowledgments and retransmissions
  – Sequence numbers
  – Time-to-live for each packet
When to Initiate Flooding

• Topology change
  – Link or node failure
  – Link or node recovery

• Configuration change
  – Link cost change

• Periodically
  – Refresh the link-state information
  – Typically (say) 30 minutes
  – Corrects for possible corruption of the data
When the Routers Disagree

(during transient periods)
Convergence

• Getting consistent routing information to all nodes
  – E.g., all nodes having the same link-state database

• Consistent forwarding after convergence
  – All nodes have the same link-state database
  – All nodes forward packets on shortest paths
  – The next router on the path forwards to the next hop
Transient Disruptions

• Detection delay
  – A node does not detect a failed link immediately
  – ... and forwards data packets into a “blackhole”
  – Depends on timeout for detecting lost hellos
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
Convergence Delay

• Sources of convergence delay
  – Detection latency
  – Flooding of link-state information
  – Shortest-path computation
  – Creating the forwarding table

• Performance during convergence period
  – Lost packets due to blackholes and TTL expiry
  – Looping packets consuming resources
  – Out-of-order packets reaching the destination

• Very bad for VoIP, online gaming, and video
Reducing Convergence Delay

• Faster detection
  – Smaller hello timers
  – Link-layer technologies that can detect failures

• Faster flooding
  – Flooding immediately
  – Sending link-state packets with high-priority

• Faster computation
  – Faster processors on the routers
  – Incremental Dijkstra’s algorithm

• Faster forwarding-table update
  – Data structures supporting incremental updates
Scaling Link-State Routing

- Overhead of link-state routing
  - Flooding link-state packets throughout the network
  - Running Dijkstra’s shortest-path algorithm
- Introducing hierarchy through “areas”
Some Properties

• Routing is a distributed algorithm
  – React to changes in the topology
  – Compute the paths through the network

• Shortest-path link state routing
  – Flood link weights throughout the network
  – Compute shortest paths as a sum of link weights
  – Forward packets on next hop in the shortest path

• Convergence process
  – Changing from one topology to another
  – Transient periods of inconsistency across routers
Distance Vector Routing

(a) A subnet. (b) Input from A, I, H, K, and the new routing table for J.
Distance Vector Algorithm

- $c(x,v) = \text{cost for direct link from } x \text{ to } v$
  - Node $x$ maintains costs of direct links $c(x,v)$
- $D_x(y) = \text{estimate of least cost from } x \text{ to } y$
  - Node $x$ maintains distance vector $D_x = [D_x(y): y \in N]$
- Node $x$ maintains its neighbors’ distance vectors
  - For each neighbor $v$, $x$ maintains $D_v = [D_v(y): y \in N]$
- Each node $v$ periodically sends $D_v$ to its neighbors
  - And neighbors update their own distance vectors
  - $D_x(y) \leftarrow \min_v \{c(x,v) + D_v(y)\}$ for each node $y \in N$
- Over time, the distance vector $D_x$ converges
Distance Vector Algorithm

**Iterative, asynchronous:** each local iteration caused by:
- Local link cost change
- Distance vector update message from neighbor

**Distributed:**
- Each node notifies neighbors *only* when its DV changes
- Neighbors then notify their neighbors if necessary

**Each node:**

*wait* for (change in local link cost or message from neighbor)

*recompute* estimates

if distance to any destination has changed, *notify* neighbors
## Distance Vector Example: Step 1

### Optimum 1-hop paths

<table>
<thead>
<tr>
<th>Table for A</th>
<th>Table for B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dst</strong></td>
<td><strong>Cst</strong></td>
</tr>
<tr>
<td>A</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>4</td>
</tr>
<tr>
<td>C</td>
<td>∞</td>
</tr>
<tr>
<td>D</td>
<td>∞</td>
</tr>
<tr>
<td>E</td>
<td>2</td>
</tr>
<tr>
<td>F</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table for C</th>
<th>Table for D</th>
<th>Table for E</th>
<th>Table for F</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dst</strong></td>
<td><strong>Cst</strong></td>
<td><strong>Hop</strong></td>
<td><strong>Dst</strong></td>
</tr>
<tr>
<td>A</td>
<td>∞</td>
<td>–</td>
<td>A</td>
</tr>
<tr>
<td>B</td>
<td>∞</td>
<td>–</td>
<td>B</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>D</td>
<td>1</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>E</td>
<td>∞</td>
<td>–</td>
<td>E</td>
</tr>
<tr>
<td>F</td>
<td>1</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>
Distance Vector Example: Step 2

Optimum 2-hop paths

<table>
<thead>
<tr>
<th>Table for A</th>
<th>Table for B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dst</td>
<td>Cst</td>
</tr>
<tr>
<td>A</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>4</td>
</tr>
<tr>
<td>C</td>
<td>7</td>
</tr>
<tr>
<td>D</td>
<td>7</td>
</tr>
<tr>
<td>E</td>
<td>2</td>
</tr>
<tr>
<td>F</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table for C</th>
<th>Table for D</th>
<th>Table for E</th>
<th>Table for F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dst</td>
<td>Cst</td>
<td>Hop</td>
<td>Dst</td>
</tr>
<tr>
<td>A</td>
<td>7</td>
<td>F</td>
<td>A</td>
</tr>
<tr>
<td>B</td>
<td>2</td>
<td>F</td>
<td>B</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>D</td>
<td>1</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>E</td>
<td>4</td>
<td>F</td>
<td>E</td>
</tr>
<tr>
<td>F</td>
<td>1</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>
Distance Vector Example: Step 3

Optimum 3-hop paths

<table>
<thead>
<tr>
<th>Table for A</th>
<th>Table for B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dst</strong></td>
<td><strong>Cst</strong></td>
</tr>
<tr>
<td>A</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>4</td>
</tr>
<tr>
<td>C</td>
<td>6</td>
</tr>
<tr>
<td>D</td>
<td>7</td>
</tr>
<tr>
<td>E</td>
<td>2</td>
</tr>
<tr>
<td>F</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table for C</th>
<th>Table for D</th>
<th>Table for E</th>
<th>Table for F</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dst</strong></td>
<td><strong>Cst</strong></td>
<td><strong>Hop</strong></td>
<td><strong>Dst</strong></td>
</tr>
<tr>
<td>A</td>
<td>6</td>
<td>F</td>
<td>A</td>
</tr>
<tr>
<td>B</td>
<td>2</td>
<td>F</td>
<td>B</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>D</td>
<td>1</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>E</td>
<td>4</td>
<td>F</td>
<td>E</td>
</tr>
<tr>
<td>F</td>
<td>1</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>
Distance Vector: Link Cost Changes

Link cost changes:
- Node detects local link cost change
- Updates the distance table
- If cost change in least cost path, notify neighbors

"good news travels fast"
Distance Vector: Link Cost Changes

Link cost changes:

- Good news travels fast
- Bad news travels slow - “count to infinity” problem!

![Distance Vector Diagram]

algorithm continues on!

\[ \text{c}(X,Y) \text{ change} \]
Distance Vector Routing

The count-to-infinity problem.
Distance Vector: Poison Reverse

If Z routes through Y to get to X:

- Z tells Y its (Z’s) distance to X is infinite (so Y won’t route to X via Z)
- Still, can have problems when more than 2 routers are involved
Routing Information Protocol (RIP)

- Distance vector protocol
  - Nodes send distance vectors every 30 seconds
  - ... or, when an update causes a change in routing
- Link costs in RIP
  - All links have cost 1
  - Valid distances of 1 through 15
  - ... with 16 representing infinity
  - Small “infinity” → smaller “counting to infinity” problem
- RIP is limited to fairly small networks
  - E.g., used in some campus networks
Comparison of LS and DV Routing

Message complexity

- **LS**: with n nodes, E links, $O(nE)$ messages sent
- **DV**: exchange between neighbors only

Speed of Convergence

- **LS**: relatively fast
- **DV**: convergence time varies
  - May be routing loops
  - Count-to-infinity problem

Robustness: what happens if router malfunctions?

**LS**:
- Node can advertise incorrect link cost
- Each node computes only its own table

**DV**:
- DV node can advertise incorrect path cost
- Each node’s table used by others (error propagates)
Similarities of LS and DV Routing

• Shortest-path routing
  – Metric-based, using link weights
  – Routers share a common view of how good a path is
• As such, commonly used *inside* an organization
  – RIP and OSPF are mostly used as *intradomain* protocols
  – E.g., Princeton uses RIP, and AT&T uses OSPF
• But the Internet is a “network of networks”
  – How to stitch the many networks together?
  – When networks may not have common goals
  – … and may not want to share information
Hierarchical Routing

(a) Hierarchical routing diagram

(b) Full table for 1A

(c) Hierarchical table for 1A
Broadcast Routing

- **Broadcast** sends a packet to all nodes
  - RPF (Reverse Path Forwarding): send broadcast received on the link to the source out all remaining links
  - Alternatively, can build and use sink trees at all nodes

**Network**

**Sink tree for I** is efficient broadcast

**RPF from I** is larger than sink tree
Multicast Routing (1) – Dense Case

- **Multicast** sends to a subset of the nodes called a group
  - Uses a different tree for each group and source

![Network with groups 1 & 2](multicast_network.png)

![Spanning tree from source S](spanning_tree.png)

![Multicast tree from S to group 1](multicast_tree1.png)

![Multicast tree from S to group 2](multicast_tree2.png)
Multicast Routing (2) – Sparse Case

- CBT (Core-Based Tree) uses a single tree to multicast
  - Tree is the sink tree from core node to group members

Sink tree from core to group 1

Multicast is send to the core then down when it reaches the sink tree
Anycast Routing

**Anycast** sends a packet to one (nearest) group member

- Anycast routes to group 1
- Apparent topology of sink tree to “node” 1
Routing for Mobile Hosts

A WAN to which LANs, MANs, and wireless cells are attached.
Routing for Mobile Hosts

- Mobile hosts can be reached via a home agent
  - Fixed home agent tunnels packets to reach the mobile host; reply can optimize path for subsequent packets
  - No changes to routers or fixed hosts
Routing in Ad Hoc Networks

Possibilities when the routers are mobile:

1. Military vehicles on battlefield.
   - No infrastructure.

2. A fleet of ships at sea.
   - All moving all the time

3. Emergency works at earthquake.
   - The infrastructure destroyed.

4. A gathering of people with notebook computers.
   - In an area lacking 802.11.
Route Discovery

- (a) Range of A's broadcast.
- (b) After B and D have received A's broadcast.
- (c) After C, F, and G have received A's broadcast.
- (d) After E, H, and I have received A's broadcast.

Shaded nodes are new recipients. Arrows show possible reverse routes.
Route Discovery (2)

<table>
<thead>
<tr>
<th>Source address</th>
<th>Request ID</th>
<th>Destination address</th>
<th>Source sequence #</th>
<th>Dest. sequence #</th>
<th>Hop count</th>
</tr>
</thead>
</table>

Format of a ROUTE REQUEST packet.
Route Discovery (3)

<table>
<thead>
<tr>
<th>Source address</th>
<th>Destination address</th>
<th>Destination sequence #</th>
<th>Hop count</th>
<th>Lifetime</th>
</tr>
</thead>
</table>

Format of a ROUTE REPLY packet.
Route Maintenance

(a) D's routing table before G goes down.
(b) The graph after G has gone down.
(a) A set of 32 node identifiers arranged in a circle. The shaded ones correspond to actual machines. The arcs show the fingers from nodes 1, 4, and 12. The labels on the arcs are the table indices.

(b) Examples of the finger tables.
Congestion Control Algorithms

- General Principles of Congestion Control
- Congestion Prevention Policies
- Congestion Control in Virtual-Circuit Subnets
- Congestion Control in Datagram Subnets
- Load Shedding
- Jitter Control
When too much traffic is offered, congestion sets in and performance degrades sharply.
Congestion Control (3) – Approaches

Network must do its best with the offered load

– Different approaches at different timescales
– Nodes should also reduce offered load (Transport)
Traffic-Aware Routing

Choose routes depending on traffic, not just topology

- E.g., use $EI$ for West-to-East traffic if $CF$ is loaded
- But take care to avoid oscillations
Admission Control

- Admission control allows a new traffic load only if the network has sufficient capacity, e.g., with virtual circuits
  - Can combine with looking for an uncongested route
Traffic Throttling

Congested routers signal hosts to slow down traffic
- ECN (Explicit Congestion Notification) marks packets and receiver returns signal to sender
Load Shedding (1)

When all else fails, network will drop packets (shed load)
Can be done end-to-end or link-by-link
Link-by-link (right) produces rapid relief
Load Shedding (2)

End-to-end (right) takes longer to have an effect, but can better target the cause of congestion.
General Principles of Congestion Control

1. Monitor the system.
   – detect when and where congestion occurs.
2. Pass information to where action can be taken.
3. Adjust system operation to correct the problem.
# Congestion Prevention Policies

<table>
<thead>
<tr>
<th>Layer</th>
<th>Policies</th>
</tr>
</thead>
</table>
| Transport  | • Retransmission policy  
• Out-of-order caching policy  
• Acknowledgement policy  
• Flow control policy  
• Timeout determination |
| Network    | • Virtual circuits versus datagram inside the subnet  
• Packet queueing and service policy  
• Packet discard policy  
• Routing algorithm  
• Packet lifetime management |
| Data link  | • Retransmission policy  
• Out-of-order caching policy  
• Acknowledgement policy  
• Flow control policy |
Congestion Control in Virtual-Circuit Subnets

(a) A congested subnet. (b) A redrawn subnet, eliminates congestion and a virtual circuit from A to B.
Jitter Control

(a) High jitter.  (b) Low jitter.
Quality of Service

• Application requirements
• Traffic shaping
• Packet scheduling
• Admission control
• Integrated services
• Differentiated services
Application Requirements (1)

Different applications care about different properties.

<table>
<thead>
<tr>
<th>Application</th>
<th>Bandwidth</th>
<th>Delay</th>
<th>Jitter</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>File sharing</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Web access</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Remote login</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Audio on demand</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Video on demand</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Telephony</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Videoconferencing</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>

“High” means a demanding requirement, e.g., low delay.
Application Requirements (2)

Network provides service with different kinds of QoS (Quality of Service) to meet application requirements

<table>
<thead>
<tr>
<th>Network Service</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constant bit rate</td>
<td>Telephony</td>
</tr>
<tr>
<td>Real-time variable bit rate</td>
<td>Videoconferencing</td>
</tr>
<tr>
<td>Non-real-time variable bit rate</td>
<td>Streaming a movie</td>
</tr>
<tr>
<td>Available bit rate</td>
<td>File transfer</td>
</tr>
</tbody>
</table>

Example of QoS categories from ATM networks
Categories of QoS and Examples

1. Constant bit rate
   • Telephony
2. Real-time variable bit rate
   • Compressed videoconferencing
3. Non-real-time variable bit rate
   • Watching a movie on demand
4. Available bit rate
   • File transfer
Buffering

Smoothing the output stream by buffering packets.

Packet departs source

Packet arrives at buffer

Packet removed from buffer

Time in buffer

Gap in playback
Traffic shaping regulates the average rate and burstiness of data entering the network

- Lets us make guarantees
Traffic Shaping (2)

Token/Leaky bucket limits both the average rate (R) and short-term burst (B) of traffic

- For token, bucket size is B, water enters at rate R and is removed to send; opposite for leaky.

Leaky bucket (need not full to send)

Token bucket (need some water to send)
The Leaky Bucket Algorithm

(a) A leaky bucket with water.  
(b) a leaky bucket with packets.
Host traffic
R=200 Mbps
B=16000 KB

Shaped by
R=200 Mbps
B=9600 KB

Shaped by
R=200 Mbps
B=0 KB

Smaller bucket size delays traffic and reduces burstiness
The Token Bucket Algorithm

(a) Before.  (b) After.
Packet Scheduling (1)

Kinds of resources can potentially be reserved for different flows:

1. Bandwidth.
2. Buffer space.
3. CPU cycles.
Packet Scheduling (1)

Packet scheduling divides router/link resources among traffic flows with alternatives to FIFO (First In First Out)

Example of round-robin queuing
Packet Scheduling (2)

Fair Queueing approximates bit-level fairness with different packet sizes; weights change target levels.

\[ F_i = \max(A_i, F_{i-1}) + \frac{L_i}{W} \]

Packets may be sent out of arrival order.

Finish virtual times determine transmission order.

---

CN5E by Tanenbaum & Wetherall, © Pearson Education-Prentice Hall and D. Wetherall, 2011
Admission Control (1)

Admission control takes a traffic flow specification and decides whether the network can carry it.

- Sets up packet scheduling to meet QoS

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token bucket rate</td>
<td>Bytes/sec</td>
</tr>
<tr>
<td>Token bucket size</td>
<td>Bytes</td>
</tr>
<tr>
<td>Peak data rate</td>
<td>Bytes/sec</td>
</tr>
<tr>
<td>Minimum packet size</td>
<td>Bytes</td>
</tr>
<tr>
<td>Maximum packet size</td>
<td>Bytes</td>
</tr>
</tbody>
</table>

Example flow specification
Admission Control (2)

Construction to guarantee bandwidth $B$ and delay $D$:

- Shape traffic source to a $(R, B)$ token bucket
- Run WFQ with weight $W$ / all weights > $R/capacity$
- Holds for all traffic patterns, all topologies
Integrated Services (1)

Design with QoS for each flow; handles multicast traffic.

Admission with RSVP (Resource ReSerVation Protocol):

- Receiver sends a request back to the sender
- Each router along the way reserves resources
- Routers merge multiple requests for same flow
- Entire path is set up, or reservation not made
RSVP-The ReSerVation Protocol

(a) A network,  (b) The multicast spanning tree for host 1.  
(c) The multicast spanning tree for host 2.
Integrated Services (2)

R3 reserves flow from S1

R3 reserves flow from S2

R5 reserves flow from S1; merged with R3 at H

Merge
Differentiated Services (1)

- Design with classes of QoS; customers buy what they want
  - Expedited class is sent in preference to regular class
  - Less expedited traffic but better quality for applications

CN5E by Tanenbaum & Wetherall, © Pearson Education-Prentice Hall and D. Wetherall, 2011
Assured Forwarding

A possible implementation of the data flow for assured forwarding.
Differentiated Services (2)

Implementation of DiffServ:

- Customers mark desired class on packet
- ISP shapes traffic to ensure markings are paid for
- Routers use WFQ to give different service levels
Design Principles for Internet

1. Make sure it works.
2. Keep it simple.
3. Make clear choices.
4. Exploit modularity.
5. Expect heterogeneity.
6. Avoid static options and parameters.
7. Look for a good design; it need not be perfect.
8. Be strict when sending and tolerant when receiving.
9. Think about scalability.
Collection of Subnetworks

The Internet is an interconnected collection of many networks.
The Network Layer in the Internet

• The IP Protocol
• IP Addresses
• Internet Control Protocols
• OSPF – The Interior Gateway Routing Protocol
• BGP – The Exterior Gateway Routing Protocol
• Internet Multicasting
• Mobile IP
• IPv6
Internetworking joins multiple, different networks into a single larger network

- How networks differ »
- How networks can be connected »
- Tunneling »
- Internetwork routing »
- Packet fragmentation »
Connecting Networks

A collection of interconnected networks.

Diagram of networks:
- Mainframe
- SNA network
- ATM network
- Router
- Switch
- FDDI ring
- Connection to Internet
- Ethernet
- Notebook computer
- 802.11
## How Networks Differ

Some of the many ways networks can differ.

<table>
<thead>
<tr>
<th>Item</th>
<th>Some Possibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service offered</td>
<td>Connection oriented versus connectionless</td>
</tr>
<tr>
<td>Protocols</td>
<td>IP, IPX, SNA, ATM, MPLS, AppleTalk, etc.</td>
</tr>
<tr>
<td>Addressing</td>
<td>Flat (802) versus hierarchical (IP)</td>
</tr>
<tr>
<td>Multicasting</td>
<td>Present or absent (also broadcasting)</td>
</tr>
<tr>
<td>Packet size</td>
<td>Every network has its own maximum</td>
</tr>
<tr>
<td>Quality of service</td>
<td>Present or absent; many different kinds</td>
</tr>
<tr>
<td>Error handling</td>
<td>Reliable, ordered, and unordered delivery</td>
</tr>
<tr>
<td>Flow control</td>
<td>Sliding window, rate control, other, or none</td>
</tr>
<tr>
<td>Congestion control</td>
<td>Leaky bucket, token bucket, RED, choke packets, etc.</td>
</tr>
<tr>
<td>Security</td>
<td>Privacy rules, encryption, etc.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Different timeouts, flow specifications, etc.</td>
</tr>
<tr>
<td>Accounting</td>
<td>By connect time, by packet, by byte, or not at all</td>
</tr>
</tbody>
</table>
How Networks Can Be Connected

Internetworking based on a common network layer – IP

Packet mapped to a VC here

Common protocol (IP) carried all the way
Internetworking using concatenated virtual circuits.
Connectionless Internetworking

Packets travel individually and can take different routes

A connectionless internet.
Tunneling

Tunneling a packet from Paris to London.

Acts like a serial line

Ethernet in Paris

Multiprotocol router

WAN

Ethernet in London

Header

IP packet inside payload field of the WAN packet

Ethernet frame
Tunneling (1)

Connects two networks through a middle one
- Packets are encapsulated over the middle
Tunneling analogy:
- tunnel is a link; packet can only enter/exit at ends
Internetwork Routing

(a) An internetwork.  (b) A graph of the internetwork.
Packet Fragmentation (1)

Packet size issues:

1. Hardware
2. Operating system
3. Protocols
4. Compliance with (inter)national standard.
5. Reduce error-induced retransmissions
6. Prevent packet occupying channel too long.
Packet Fragmentation (1)

- Networks have different packet size limits for many reasons
  - Large packets sent with fragmentation & reassembly

Transparent – packets fragmented / reassembled in each network

Non-transparent – fragments are reassembled at destination
Packet Fragmentation (2)

- Example of IP-style fragmentation:

Original packet: (10 data bytes)

Fragmented: (to 8 data bytes)

Re-fragmented: (to 5 bytes)
Packet Fragmentation (3)

Fragmentation when the elementary data size is 1 byte.

(a) Original packet, containing 10 data bytes.
Packet Fragmentation (4)

Fragmentation when the elementary data size is 1 byte
(b) Fragments after passing through a network with maximum packet size of 8 payload bytes plus header.
Packet Fragmentation (5)

Fragmentation when the elementary data size is 1 byte

(c) Fragments after passing through a size 5 gateway.
Path MTU Discovery avoids network fragmentation

- Routers return MTU (Max. Transmission Unit) to source and discard large packets
Network Layer in the Internet (1)

- IP Version 4
- IP Addresses
- IP Version 6
- Internet Control Protocols
- Label Switching and MPLS
- OSPF—An Interior Gateway Routing Protocol
- BGP—The Exterior Gateway Routing Protocol
- Internet Multicasting
- Mobile IP
Network Layer in the Internet (2)

IP has been shaped by guiding principles:

- Make sure it works
- Keep it simple
- Make clear choices
- Exploit modularity
- Expect heterogeneity
- Avoid static options and parameters
- Look for good design (not perfect)
- Strict sending, tolerant receiving
- Think about scalability
- Consider performance and cost
Network Layer in the Internet (3)

- Internet is an interconnected collection of many networks that is held together by the IP protocol.
IPv4 (Internet Protocol) header is carried on all packets and has fields for the key parts of the protocol:
IP Addresses (1) – Prefixes

Addresses are allocated in blocks called prefixes

- Prefix is determined by the network portion
- Has $2^L$ addresses aligned on $2^L$ boundary
- Written address/length, e.g., 18.0.31.0/24
IP Addresses (2) – Subnets

Subnetting splits up IP prefix to help with management

ISP gives network a single prefix

Network divides it into subnets internally
IP Addresses (3) – Aggregation

Aggregation joins multiple IP prefixes into a single larger prefix to reduce routing table size.

ISP advertises a single prefix

ISP customers have different prefixes
Packets are forwarded to the entry with the **longest matching prefix** or smallest address block

- Complicates forwarding but adds flexibility

Except for this part!  
Main prefix goes this way
IP Addresses (5) – Classful Addressing

Old addresses came in blocks of fixed size (A, B, C)

- Carries size as part of address, but lacks flexibility
- Called classful (vs. classless) addressing

<table>
<thead>
<tr>
<th>Class</th>
<th>Network</th>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>110</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>1110</td>
<td>Multicast address</td>
</tr>
<tr>
<td>E</td>
<td>1111</td>
<td>Reserved for future use</td>
</tr>
</tbody>
</table>
IP Addresses (6) – NAT

NAT (Network Address Translation) box maps one external IP address to many internal IP addresses

- Uses TCP/UDP port to tell connections apart
- Violates layering; very common in homes, etc.
NAT – Network Address Translation

Packet before translation

Packet after translation

Company LAN

Company router

Server

PC

10.0.0.1

198.60.42.12

NAT box/firewall

Leased line

ISP's router

Boundary of company premises
IP Version 6 (1)

Major upgrade in the 1990s due to impending address exhaustion, with various other goals:

- Support billions of hosts
- Reduce routing table size
- Simplify protocol
- Better security
- Attention to type of service
- Aid multicasting
- Roaming host without changing address
- Allow future protocol evolution
- Permit coexistence of old, new protocols, ...

Deployment has been slow & painful, but may pick up pace now that addresses are all but exhausted
IP Version 6 (2)

IPv6 protocol header has much longer addresses (128 vs. 32 bits) and is simpler (by using extension headers)
The IPv6 fixed header (required).

<table>
<thead>
<tr>
<th>Version</th>
<th>Diff. Serv.</th>
<th>Flow label</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payload length</td>
<td>Next header</td>
<td>Hop limit</td>
</tr>
</tbody>
</table>

- Source address (16 bytes)
- Destination address (16 bytes)
## IPv6 extension headers

<table>
<thead>
<tr>
<th>Extension header</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hop-by-hop options</td>
<td>Miscellaneous information for routers</td>
</tr>
<tr>
<td>Destination options</td>
<td>Additional information for the destination</td>
</tr>
<tr>
<td>Routing</td>
<td>Loose list of routers to visit</td>
</tr>
<tr>
<td>Fragmentation</td>
<td>Management of datagram fragments</td>
</tr>
<tr>
<td>Authentication</td>
<td>Verification of the sender’s identity</td>
</tr>
<tr>
<td>Encrypted security payload</td>
<td>Information about the encrypted contents</td>
</tr>
</tbody>
</table>
IP Version 6 (3)

The hop-by-hop extension header for large datagrams (jumbograms).
IP Version 6 (4)

The extension header for routing.
Internet Control Protocols (1)

IP works with the help of several control protocols:

- **ICMP** is a companion to IP that returns error info
  - Required, and used in many ways, e.g., for traceroute
- **ARP** finds Ethernet address of a local IP address
  - Glue that is needed to send any IP packets
  - Host queries an address and the owner replies
- **DHCP** assigns a local IP address to a host
  - Gets host started by automatically configuring it
  - Host sends request to server, which grants a lease
Main ICMP (Internet Control Message Protocol) types:

<table>
<thead>
<tr>
<th>Message type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination unreachable</td>
<td>Packet could not be delivered</td>
</tr>
<tr>
<td>Time exceeded</td>
<td>Time to live field hit 0</td>
</tr>
<tr>
<td>Parameter problem</td>
<td>Invalid header field</td>
</tr>
<tr>
<td>Source quench</td>
<td>Choke packet</td>
</tr>
<tr>
<td>Redirect</td>
<td>Teach a router about geography</td>
</tr>
<tr>
<td>Echo and Echo reply</td>
<td>Check if a machine is alive</td>
</tr>
<tr>
<td>Timestamp request/reply</td>
<td>Same as Echo, but with timestamp</td>
</tr>
<tr>
<td>Router advertisement/solicitation</td>
<td>Find a nearby router</td>
</tr>
</tbody>
</table>
Internet Control Protocols (3)

- ARP (Address Resolution Protocol) lets nodes find target Ethernet addresses from their IP addresses
ARP—The Address Resolution Protocol

Three interconnected /24 networks: two Ethernets and an FDDI ring.
Dynamic Host Configuration Protocol

Operation of DHCP.
Transmitting a TCP segment using IP, MPLS, and PPP.
Label Switching and MPLS (2)

Forwarding an IP packet through an MPLS network
OSPF—Interior Routing Protocol (1)

OSPF computes routes for a single network (e.g., ISP)

- Models network as a graph of weighted edges

Network:

Graph:

Broadcast LAN modeled as a well-connected node
OSPF—Interior Routing Protocol (2)

OSPF divides one large network (Autonomous System) into areas connected to a backbone area

- Helps to scale; summaries go over area borders

One Autonomous System

Area border router  |  Backbone router  |  AS border router  |  Internal router

Area 2 (stub)       |  Area 0 (backbone) |  Area 1
OSPF—Interior Routing Protocol (3)

OSPF (Open Shortest Path First) is link-state routing:
- Uses messages below to reliably flood topology
- Then runs Dijkstra to compute routes

<table>
<thead>
<tr>
<th>Message type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>Used to discover who the neighbors are</td>
</tr>
<tr>
<td>Link state update</td>
<td>Provides the sender’s costs to its neighbors</td>
</tr>
<tr>
<td>Link state ack</td>
<td>Acknowledges link state update</td>
</tr>
<tr>
<td>Database description</td>
<td>Announces which updates the sender has</td>
</tr>
<tr>
<td>Link state request</td>
<td>Requests information from the partner</td>
</tr>
</tbody>
</table>
BGP—Exterior Routing Protocol (1)

BGP (Border Gateway Protocol) computes routes across interconnected, autonomous networks

—Key role is to respect networks’ policy constraints

Example policy constraints:

• No commercial traffic for educational network
• Never put Iraq on route starting at Pentagon
• Choose cheaper network
• Choose better performing network
• Don’t go from Apple to Google to Apple
BGP—Exterior Routing Protocol (2)

Common policy distinction is transit vs. peering:

- Transit carries traffic for pay; peers for mutual benefit
- AS1 carries AS2↔AS4 (Transit) but not AS3 (Peer)
BGP—Exterior Routing Protocol (3)

- BGP propagates messages along policy-compliant routes
  - Message has prefix, AS path (to detect loops) and next-hop IP (to send over the local network)
Internet Multicasting

Groups have a reserved IP address range (class D)

- Membership in a group handled by IGMP (Internet Group Management Protocol) that runs at routers

Routes computed by protocols such as PIM:

- Dense mode uses RPF with pruning
- Sparse mode uses core-based trees

IP multicasting is not widely used except within a single network, e.g., datacenter, cable TV network.
Mobile IP

- Goals
- Mobile host use home IP address anywhere.
- No software changes to fixed hosts
- No changes to router software, tables
- Packets for mobile hosts – restrict detours
- No overhead for mobile host at home.
Mobile IP

- Mobile hosts can be reached via a home agent
  - Fixed home agent tunnels packets to reach the mobile host; reply can optimize path for subsequent packets
  - No changes to routers or fixed hosts