Internetworking

Internetworking, Concatenated Virtual Circuits, Connectionless Internetworking, Tunneling, Internetwork Routing, Fragmentation
Internetworking

- So far we have viewed single protocols, assuming there is a homogeneous network, where each machine uses the same protocol in each layer.
- In practice, existing LANs, MANs, and WANs use numerous protocols in every layer.
- In an “ideal world” networks can start using some sort of common protocols in each layer but the installed base of different networks is large - nearly all personal computers run TCP/IP, while large businesses have mainframes running IBM's SNA, etc.
Internetworking

• This trend will continue for years due to legacy problems, new technology, and other factors.

• Another reason for keeping the variety is that as computers and networks get cheaper, the place where decisions get made moves downward in organizations, that are unlikely to follow some united approach.

• Also different networks (e.g., ATM and wireless) have radically different technology, so as new hardware developments occur, new software will be created to fit the new hardware – so new technologies will bring new networks and new protocols.
Internetworking

- The next slide presents an example of connection of different networks - a corporate network with multiple locations tied together by a wide area ATM network, where an FDDI optical backbone is used to connect an Ethernet, an 802.11 wireless LAN, and the corporate data center's SNA mainframe network.

- The purpose of interconnecting all these networks is to allow users on any of them to communicate with users on all the other ones and also to allow users on any of them to access data on any of them.
Connecting Networks

A collection of interconnected networks.

- Mainframe
- SNA network
- ATM network
- Router
- Switch
- FDDI ring
- Connection to Internet
- Ethernet
- 802.11
- Notebook computer
How networks differ

• Network differences are a lot – there are different modulation techniques or frame formats in the physical and data link layers, which we shall leave aside here

• What we look at are some of the differences that can occur in the network layer, which makes internetworking more difficult than operating within a single network – a list of such differences is in the next slide
### How networks 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>

Some of the many ways networks can differ.
How networks differ

• Many problems can occur at the interfaces between different networks - when packets from a connection-oriented network go through a connectionless one, they may be reordered – situation that the sender does not expect and the receiver is not prepared to deal with

• Protocol conversions are needed, which is not always easy to implement

• Address conversions will also be needed – so some kind of directory system is required

• Differing maximum packet sizes can be also a major issue – how to pass an 8000-byte packet through a network with max size is 1500 bytes?
How networks differ

- Some other issues are:
- passing multicast packets through a network that does not support multicasting
- differing qualities of service
- Error, flow, and congestion control
- security mechanisms, parameter settings, accounting rules, and even national privacy laws
Connecting networks

• Networks can be interconnected by different devices, as we saw earlier

• In the network layer, routers connect two networks - a router that can handle multiple protocols is called a multiprotocol router

• How different it is when connecting two networks by switch or by router – in the next slide source S, wants to send a packet to the destination machine, D

• These machines are on different Ethernets, connected by a switch (on the left)
How Networks Can Be Connected

(a) Two Ethernets connected by a switch.
(b) Two Ethernets connected by routers.
Connecting networks

• S encapsulates the packet in a frame and sends it on its way - it arrives at the switch, which then determines that the frame is for LAN 2 by looking at its MAC address, so the switch just removes the frame from LAN 1 and deposits it on LAN 2

• On the right – the LANs are connected by pair of routers (point-to-point line between them)

• The frame from S is picked up by the router and the packet removed from the frame's data field. The router examines the address in the packet (e.g., an IP address) and looks up in its routing table – according to it, the router takes a decision to send the packet to the remote router (probably encapsulated in a different kind of frame, according to the line protocol)

• At the far end, the packet is put into the data field of an Ethernet frame and deposited onto LAN 2
Connecting networks

• The essential difference between the switched (or bridged) case and the routed case is that the switch (or bridge) transports the entire frame on the basis of its MAC address.

• The router on the other hand extracts the packet from the frame and uses the address from the packet to decide where to send it.

• Unlike routers, switches do not have to understand the network layer protocol used to switch packets.
Concatenated Virtual Circuits

- A sequence of virtual circuits is set up from the source through one or more gateways to the destination - each gateway maintains tables telling which virtual circuits pass through it, where they are to be routed, and what the new virtual-circuit number is
- This scheme works best when all the networks have roughly the same properties
- If the source machine is on a network that does guarantee reliable delivery but one of the intermediate networks can lose packets, the concatenation has fundamentally changed the nature of the service
- Concatenated virtual circuits are also common in the transport layer - it is possible to build a bit pipe using SNA, which terminates in a gateway, and have a TCP connection go from the gateway to the next gateway
Internetworking using concatenated virtual circuits.
Connectionless Internetworking

- The datagram model is an alternative to the concatenated virtual circuits - the only service the network layer offers to the transport layer is the ability to inject datagrams into the subnet.
- This model does not require all packets belonging to one connection to traverse the same sequence of gateways - a routing decision is made separately for each packet, depending on various factors at the moment.
- Can use multiple routes and thus achieve a higher bandwidth than the concatenated virtual-circuit s.
- However, there is no guarantee that the packets arrive at the destination in order, if they arrive at all.
Connectionless Internetworking

A connectionless internet.
Internetworking with concatenated virtual-circuits

- Internetworking can be approached with the concatenated virtual-circuit model (same advantages as using virtual circuits within a single subnet: buffers can be reserved in advance, sequencing can be guaranteed, short headers can be used, and the troubles caused by delayed duplicate packets can be avoided and same disadvantages: table space required in the routers for each open connection, no alternate routing to avoid congested areas, and vulnerability to router failures along the path. It also has the disadvantage of being difficult, if not impossible, to implement if one of the networks involved is an unreliable datagram network)
Internetworking with datagrams

• The datagram approach to internetworking has similar properties as those of datagram subnets: more potential for congestion and more potential for adapting to it, robustness, and longer headers - adaptive routing algorithms are possible - just as they are within a single datagram network.

• A major advantage of the datagram approach to internetworking - can be used over subnets with no virtual circuits inside. Many LANs, mobile networks (e.g., aircraft and naval fleets), and even some WANs fall into this category. When an internet includes one of these, serious problems occur if the internetworking strategy is based on virtual circuits.
Tunneling

- Handling the general case of making two different networks interwork is very difficult.
- However, there is a common special case where the source and destination hosts are on the same type of network, but there is a different network in between.
- Example - an international bank with a TCP/IP-based Ethernet in Paris, a TCP/IP-based Ethernet in London, and a non-IP wide area network in between, as shown in the next slide.
Tunneling

Tunneling a packet from Paris to London.

Acts like a serial line

Ethernet in Paris

Multiprotocol router

WAN

Tunnel

Ethernet in London

1. Ethernet frame

IP

2. Ethernet frame

IP

IP packet inside payload field of the WAN packet
Tunneling

• In such cases – **tunneling** is used

• To send an IP packet to host 2, host 1 constructs the packet containing the IP address of host 2, inserts it into an Ethernet frame addressed to the Paris multiprotocol router, and puts it on the Ethernet. When the multiprotocol router gets the frame, it removes the IP packet, inserts it in the payload field of the WAN network layer packet, and addresses the latter to the WAN address of the London multiprotocol router. When it gets there, the London router removes the IP packet and sends it to host 2 inside an Ethernet frame

• The WAN can be seen as a big tunnel extending from one multiprotocol router to the other. The IP packet just travels from one end of the tunnel to the other
Tunneling

• The multiprotocol router has to understand IP and WAN packets

• An analogy - a person driving her car from Paris to London. Within France, the car goes on its own, but when it hits the English Channel, it is loaded into a high-speed train and transported to England through the Channel Tunnel as cars are not permitted to drive through it - the car is being carried as freight

• When the car gets on the English roads - it continues on its own - tunneling of packets through a foreign network works the same way
Tunneling

Tunneling a car from France to England.
Internetwork Routing

• Routing through an internetwork is similar to routing within a single subnet, but with some added complications

• In the next slide five networks are connected by six (possibly multiprotocol) routers. Making a graph model of this situation is complicated by the fact that every router can directly access (i.e., send packets to) every other router connected to any network to which it is connected

• So router B can directly access A and C via network 2 and also D via network 3 – as in the graph on the right
Internetwork Routing

(a) An internetwork. (b) A graph of the internetwork.
Internetwork Routing

• Once the graph has been constructed, known routing algorithms (like distance vector and link state algorithms) can be applied to the set of multiprotocol routers.

• Thus we have a two-level routing algorithm: within each network an interior gateway protocol is used, but between the networks, an exterior gateway protocol is used ("gateway" is an older term for "router").

• Each network is independent, so they may all use different algorithms and each such network is often referred to as an Autonomous System (AS).
Internetwork Routing

• Let a packet start on its LAN addressed to the local multiprotocol router (in the MAC layer header) - after getting there, the network layer code decides which multiprotocol router to forward the packet to, using its own routing tables

• If that router can be reached using the packet's native network protocol, the packet is forwarded there directly - otherwise it is tunneled there, encapsulated in the protocol required by the intervening network. This process is repeated until the packet reaches the destination network
Internetwork Routing

• One difference between internetwork routing and intranetwork routing is that internetwork routing may cross international boundaries – in such cases various laws may apply (as Sweden's strict privacy laws about exporting personal data about Swedish citizens from Sweden or Canadian law saying that data traffic originating in Canada and ending in Canada may not leave the country – i.e. traffic from Windsor, Ontario to Vancouver may not be routed via nearby Detroit, even if that route is the fastest and cheapest
Internetwork Routing

• Another difference between interior and exterior routing is the cost - within a single network, a single charging algorithm normally applies

• Different networks may be under different managements, so one route may be less expensive than another

• Also the quality of service offered by different networks may be different, and this may be a reason to choose one route over another
Fragmentation

• Each network imposes some maximum size on its packets. These limits are due to:

1. Hardware (size of an Ethernet frame)
2. Operating system (buffers are 512 bytes)
3. Protocols (the number of bits in the packet length field)
4. Compliance with (inter)national standard
5. Reducing error-induced retransmissions to some level
6. Prevent one packet from occupying the channel too long

Because of these factors network designers are not free to choose any maximum packet size they wish - max payloads range from 48 bytes (ATM cells) to 65,515 bytes (IP packets), although the payload size in higher layers is often larger
Fragmentation

• Problem - when a large packet is put on a network whose maximum packet size is too small
• The only solution to the problem is to allow gateways to break up packets into fragments, sending each fragment as a separate internet packet
• The difficulty here is the reverse process and even packet-switching networks have trouble putting the fragments back together again
Fragmentation

- There are two strategies for recombining the fragments back
- The first one is to make **fragmentation transparent to** any **subsequent networks** through which the packet must pass on its way to the ultimate destination – next slide at the top – the small-packet network has gateways (most likely, specialized routers) that interface to other networks
- When an oversized packet arrives at a gateway, the gateway breaks it up into fragments - each one addressed to the same exit gateway, where the pieces are recombined - passage through the small-packet network has been made transparent. Subsequent networks are not even aware that fragmentation has occurred
Fragmentation

(a) Transparent fragmentation.

(b) Nontransparent fragmentation.
Fragmentation

• Transparent fragmentation has some problems:
  • the exit gateway must know when it has received all the pieces, so either a count field or an "end of packet" bit must be provided.
  • all packets must exit via the same gateway - not allowing some fragments to follow different routes may lead to performance degradation
  • the overhead required to repeatedly reassemble and then refragment a large packet passing through a series of small-packet networks
Fragmentation

• The second strategy is to refrain from recombining fragments at any intermediate gateways - once a packet has been fragmented, each fragment is treated as though it were an original packet

• All fragments pass through the exit gateway (or gateways), as shown in the lower half of the slide - recombination occurs only at the destination host and this is how IP works
Fragmentation

- Nontransparent fragmentation also has some problems
- It requires every host to be able to do reassembly
- When a large packet is fragmented, the total overhead increases because each fragment must have a header (in the first method the overhead disappears as soon as the small-packet network is exited)
- Nontransparent fragmentation has the advantage that multiple exit gateways can be used and higher performance can be achieved, unless concatenated virtual-circuit model is being used (then - no advantage)
Fragmentation

• The fragments must be numbered so that the original data can be reconstructed

• One way of numbering a tree model - when packet 0 must be split up, the pieces are 0.0, 0.1, 0.2, etc. if they are to be further fragmented - the pieces are 0.0.0, 0.0.1, 0.0.2, . . . , 0.1.0, 0.1.1, 0.1.2, etc.

• Enough fields must be reserved in the header for the worst case so that the scheme is sufficient to ensure that all the pieces can be correctly reassembled at the destination, no matter what order they arrive in
Fragmentation

• If even one network loses or discards packets, end-to-end retransmissions are needed

• If a 1024-bit packet is fragmented equal-sized fragments, 0.0, 0.1, 0.2, and 0.3, then fragment 0.1 is lost, but the other parts arrive at the destination, so at some point the source times out and retransmits the original packet again – this time the route taken passes through a network with a 512-bit limit, so two fragments are generated - when the new fragment 0.1 arrives at the destination, the receiver will think this is the missing piece from the first transmission and reconstruct the packet incorrectly

• Hence - two sequence fields in the internet header are requires : the original packet number + the fragment number
Fragmentation

- There is a trade-off between the size of the elementary fragment and the number of bits in the fragment number.
- The elementary fragment size is presumed to be acceptable to every network, subsequent fragmentation of an internet packet containing several fragments causes no problem. The ultimate limit here is to have the elementary fragment be a single bit or byte, with the fragment number then being the bit or byte offset within the original packet, as shown in the next slide.
Fragmentation

(a) Transparent fragmentation.  (b) Nontransparent fragmentation.