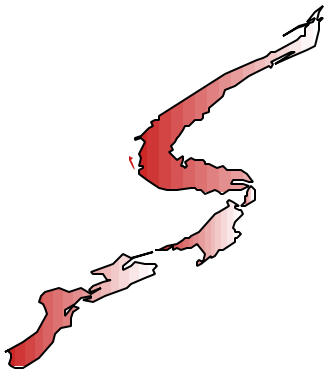
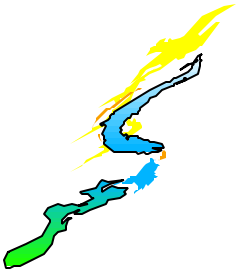


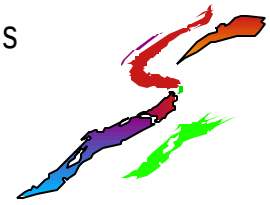
Network Layer Continued

G. A. Marin

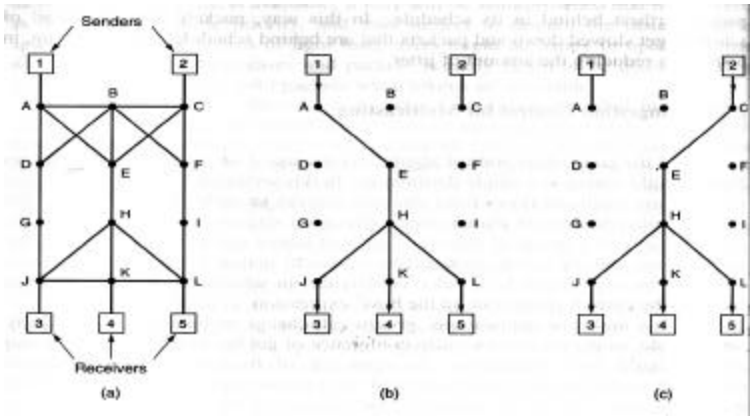


Congestion Control for Multicast

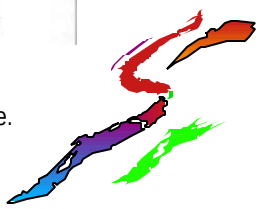
- Deals with many-to-many flows for which some congestion control is needed (eg., video conferencing).
- Difficult to reserve the correct amount of bandwidth optimally for each source-destination pair.
  - complicated as members join and leave the session
- RSVP-Resource Reservation Protocol- developed in the IP community to solve this problem.



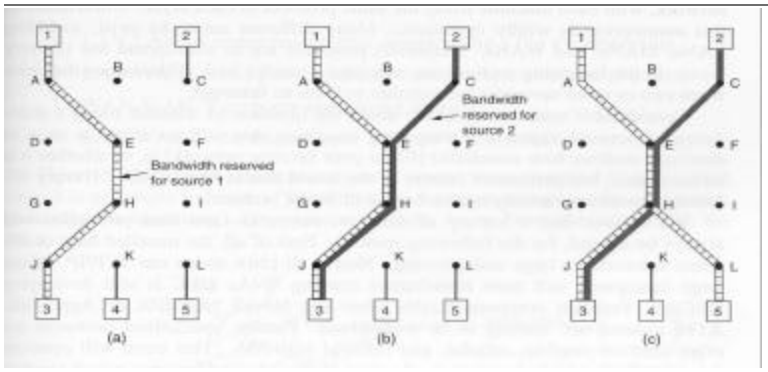
RSVP Example



1. Routers build two spanning trees for group 1 and group 2.
2. Any destination may send reservation msg back up spanning tree.
3. Routers at each step reserve necessary bandwidth/buffers.

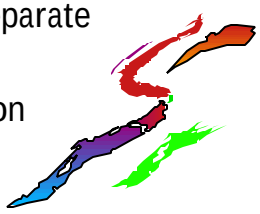


Reservations by hosts 3,3,5



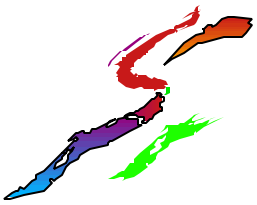
Different "programs" from hosts 1 and 2 require separate reservations.

Same program for different destinations can share on common links in spanning tree.



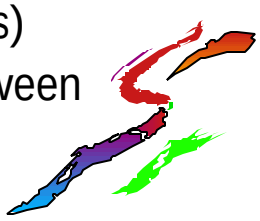
Internetworking

- An internet is a collection of disparate networks including LANs, MANs, WANs.
- Includes multiple protocols
  - TCP/IP
  - SNA
  - DECnet
  - Novell IPX
  - AppleTalk
  - ATM



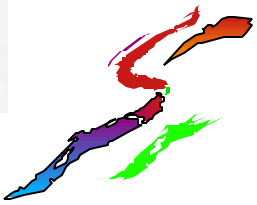
Gateways

- Repeaters (amplify signals on long cables)
- Bridges (verifies checksum and forwards frame to different network)
- Multiprotocol routers (forward packets between dissimilar networks)
- Transport Gateways (run separate transport sessions between gateways)
- Application Gateways (translate between different application formats and procedures)

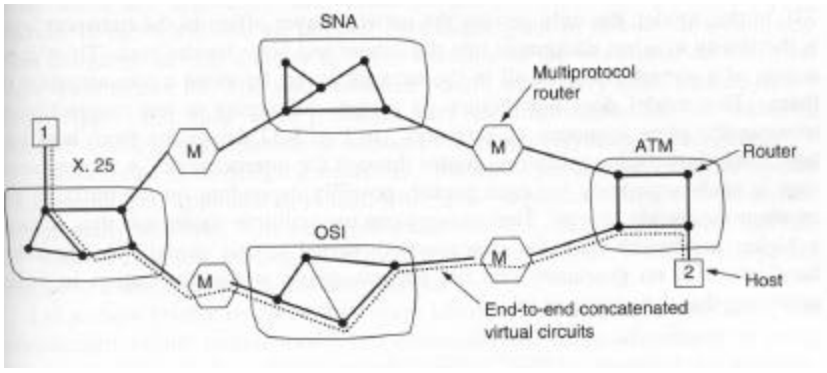


Differences Among Networks

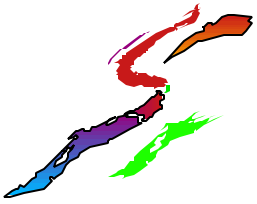
Item	Some Possibilities
Service offered	Connection-oriented versus connectionless
Protocols	IP, IPX, CLNP, AppleTalk, DECnet, etc.
Addressing	Flat (802) versus hierarchical (IP)
Multicasting	Present or absent (also broadcasting)
Packet size	Every network has its own maximum
Quality of service	May be present or absent; many different kinds
Error handling	Reliable, ordered, and unordered delivery
Flow control	Sliding window, rate control, other, or none
Congestion control	Leaky bucket, choke packets, etc.
Security	Privacy rules, encryption, etc.
Parameters	Different timeouts, flow specifications, etc.
Accounting	By connect time, by packet, by byte, or not at all



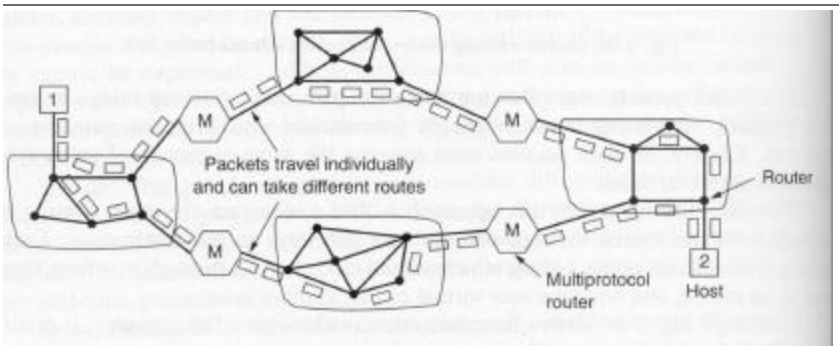
Concatenation of VC Subnets



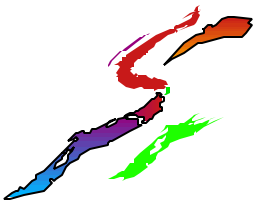
A sequence of VCs is set up through gateways. Each subnet must provide a service for it to be available end-to-end.



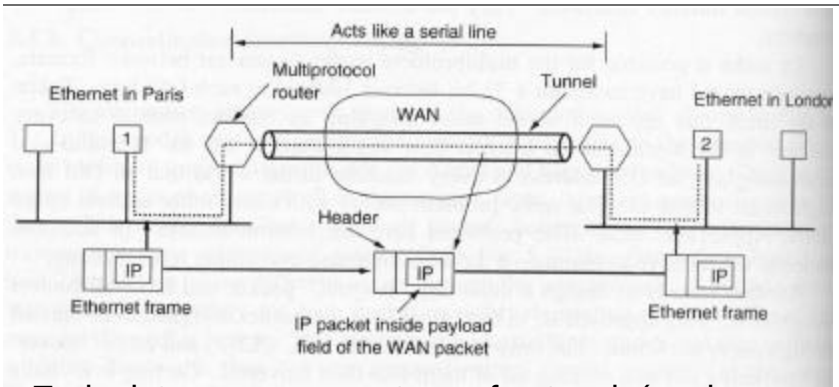
Connectionless Internetworking



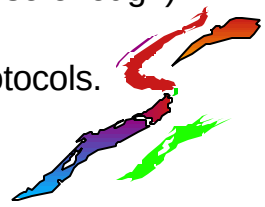
Different packets may take different routes.
No guarantee that they arrive in order.
Must deal with different address formats.
Only approach possible if subnets don't support VCs.



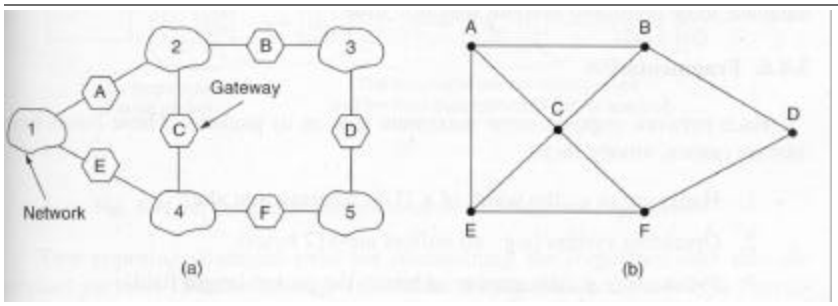
Tunneling - Special Case



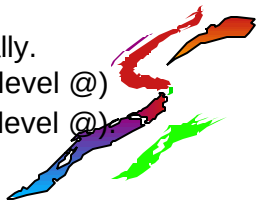
Endpoints are on same type of network (or close enough).
Different network in between.
Two multiprotocol routers understand both protocols.



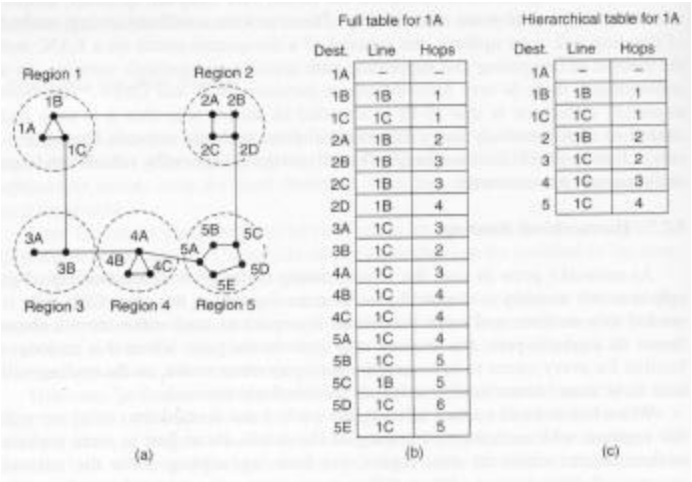
Internetwork Routing (among networks)



1. Use hierarchical routing: EGP between networks and IGP within.
2. Packet usually starts on LAN addressed to its router.
3. LAN delivers using the router's mac address.
4. This router will send to a gateway if headed externally.
5. Packet tunneled across next net if necessary (mac level @)
6. Process continues until reach destination (network level @)



Hierarchical Internetwork Routing



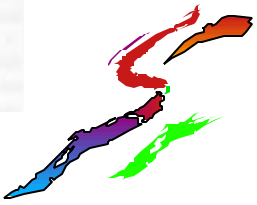
Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

Hierarchical table for 1A

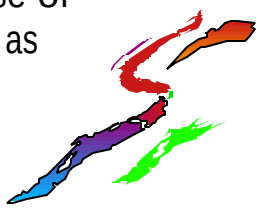
Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

Note that best path from 1A to 5C is via Region 2, but this sends via Region 3.



Fragmentation

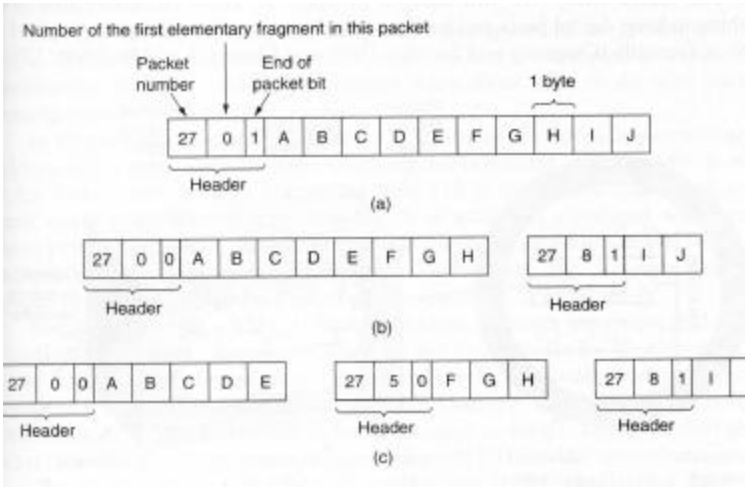
- Each network has a max allowable packet size.
  - Payloads range from 48 bytes (ATM) to 65K bytes for IP packets.
- If all networks don't agree, gateways break into fragments that must be reassembled.
- Fragments may be reassembed at each gateway or may be left for destination to reassemble.
- Note ATM is especially adept at this because of need to convert to/from cells. Referred to as SAR: segmentation and reassembly.

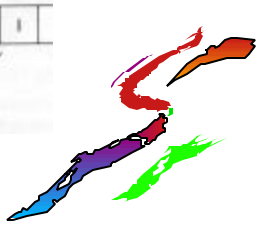


Tree Numbered Fragments

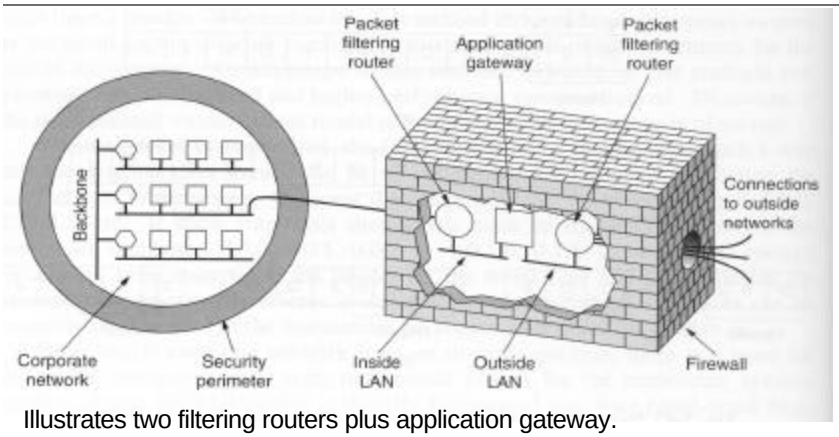
- First gateway breaks packet 0 into 0.0, 0.1, 0.2, 0.3, (say)
- Next gateway breaks packet 0.0 into 0.0.1, 0.0.2,... as needed.
- But suppose packet 0.1 is lost but 0.0, 0.2, 0.3 arrive.
- Transport layer times out and resends pkt 0.
- This time pkt 0 takes a different route and is fragmented into two larger packets 0.0 and 0.1.
- If old 0.0,0.2,0.3 still waiting then new 0.0 will be discarded and new (longer) 0.1 will be reassembled incorrectly.

Better Approach Agreed Elementary Fragment Size



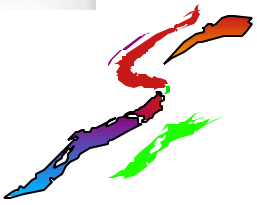


Firewalls

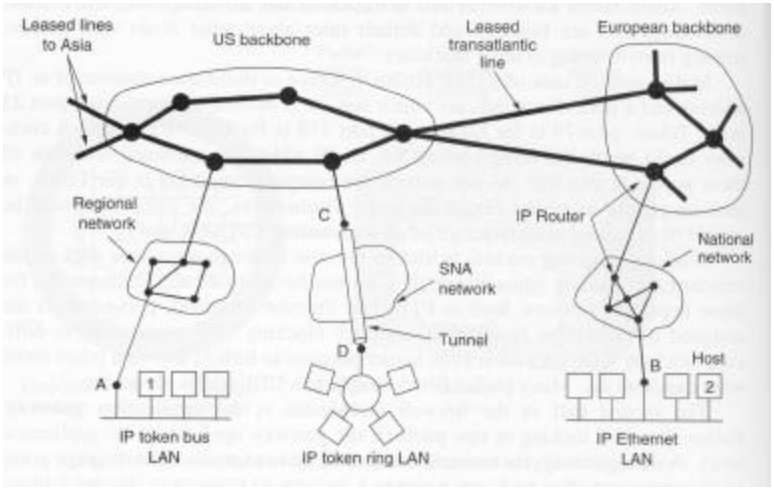


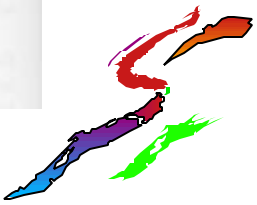
Illustrates two filtering routers plus application gateway. One router versions quite common. In a large corporation this configuration makes sure no path around application gateway. Can block all outside addresses for particular services (defined by IP port).

Application gateway may filter based on headers or even content.

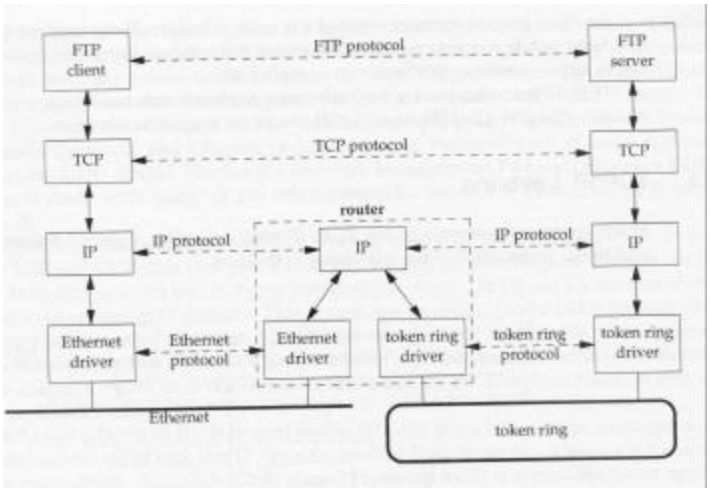


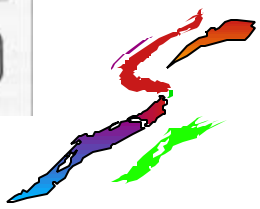
IP and the Internet



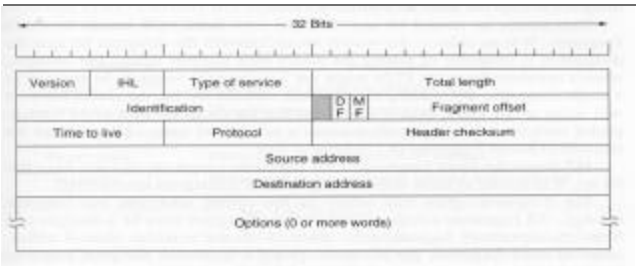


Basic Configuration: Two networks interconnected by a router.

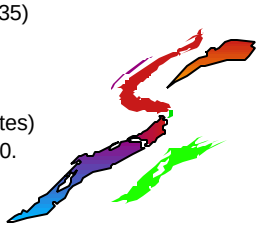




IP Header

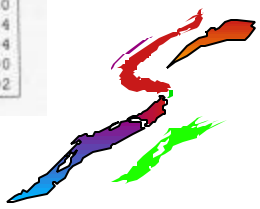


Version: version being used (IP4 or IP6 typical)
IHL: IP Header Length in 32-bit words (between 5 and 15) so max HL is 60 bytes.
TOS: 3-bit precedence field (ignored) 4 TOS bits followed by 0.
4-bits (min delay, max thruput, max reliability, min monetary cost)
Total Length: Length of IP datagram (not header) in bytes (implies max 65,535)
Identification: Uniquely identifies all fragments of a datagram.
DF: Don't Fragment (all routers must accept at least 576 byte datagrams)
MF: More Fragments (all fragments set except last one)
Fragment Offset: Where in datagram this fragment belongs (multiple of 8 bytes)
TTL: Intended to count time in seconds but usually counts hops. Toss when 0.
Protocol: Numbered uniquely as given in RFC 1700.
Header Checksum: Checks header only.
SA: Source address (32 bits)
DA: Destination address (32 bits)



RFC 1349 Recommended Values for TOS Field

Application	Minimize delay	Maximize throughput	Maximize reliability	Minimize monetary cost	Hex value
Telnet/Rlogin	1	0	0	0	0x10
FTP					
control	1	0	0	0	0x10
data	0	1	0	0	0x08
any bulk data	0	1	0	0	0x08
TFTP	1	0	0	0	0x10
SMTP					
command phase	1	0	0	0	0x10
data phase	0	1	0	0	0x08
DNS					
UDP query	1	0	0	0	0x10
TCP query	0	0	0	0	0x00
zone transfer	0	1	0	0	0x08
ICMP					
error	0	0	0	0	0x00
query	0	0	0	0	0x00
any IGP	0	0	1	0	0x04
SNMP	0	0	1	0	0x04
BOOTP	0	0	0	0	0x00
NNTP	0	0	0	1	0x02



Receiving Multiple Protocols