The Network Layer Functions:
Congestion Control

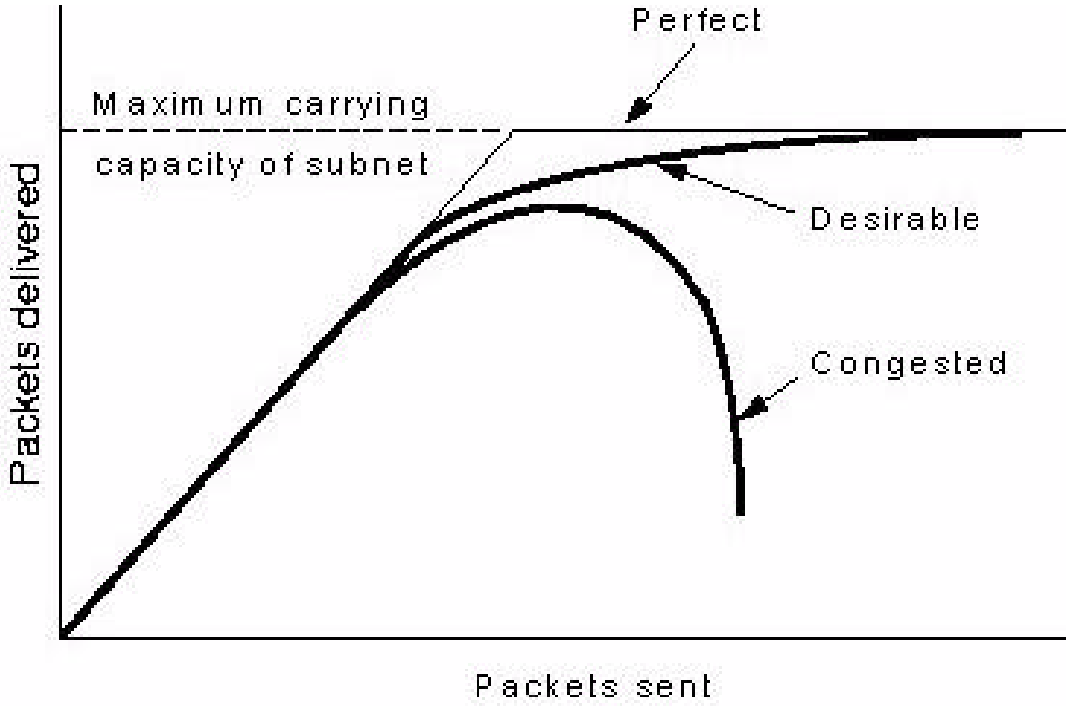
- **Network Congestion:**

  Characterized by presence of a large number of packets (load) being routed in all or portions of the subnet that exceeds its link and router capacities (resources) resulting in a performance slowdown.

- **Steps of closed-loop congestion control:**

1. **Congestion detection: System monitoring**
2. **Transmit the information to parts of the network where corrective measures are possible.**
3. **Adjust network operation parameters (routing procedures etc.) to correct the problem.**

Congestion Detection



Can utilize two techniques:

- **Notification from packet switches (routers).**
- **Infer congestion from packet loss:**
  - **Packet loss can be used to detect congestion because packet loss due hardware failure is very rare.**
  - **Sender can infer congestion from packet loss through missing acknowledgments.**
  - **Rate or percentage of lost packets can be used to gauge degree of congestion.**

Policies Affecting Network Congestion

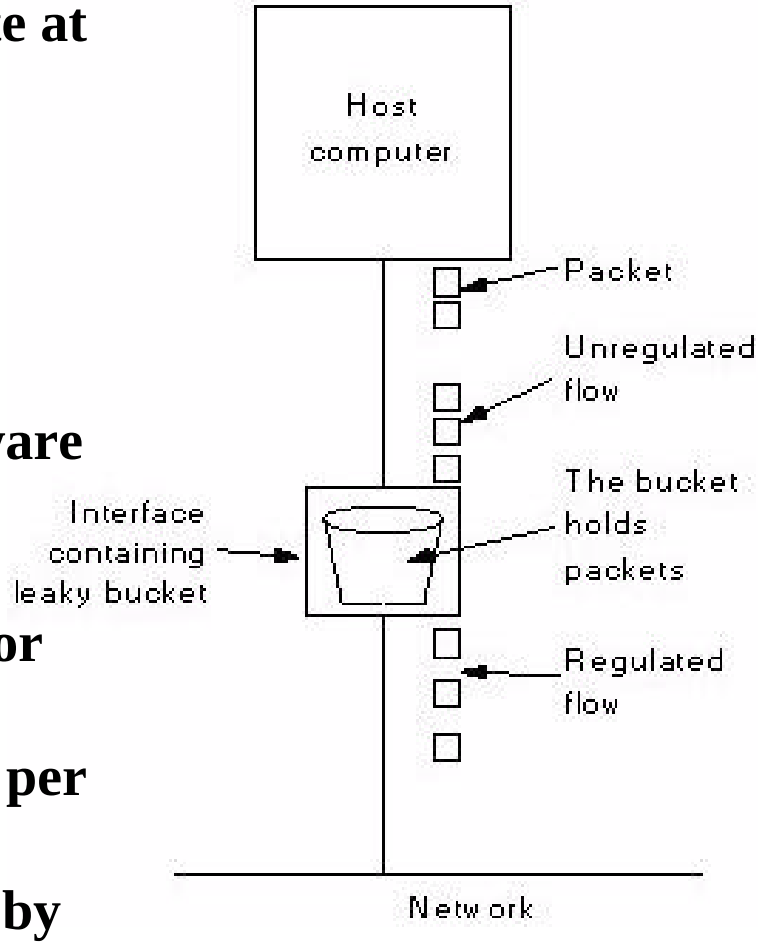
Layer	Policies
Transport	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy • Timeout determination
Network	• Virtual circuits versus datagram inside the subnet • Packet queueing and service policy • Packet discard policy • Routing algorithm • Packet lifetime management
Data link	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy

Congestion Control Methods

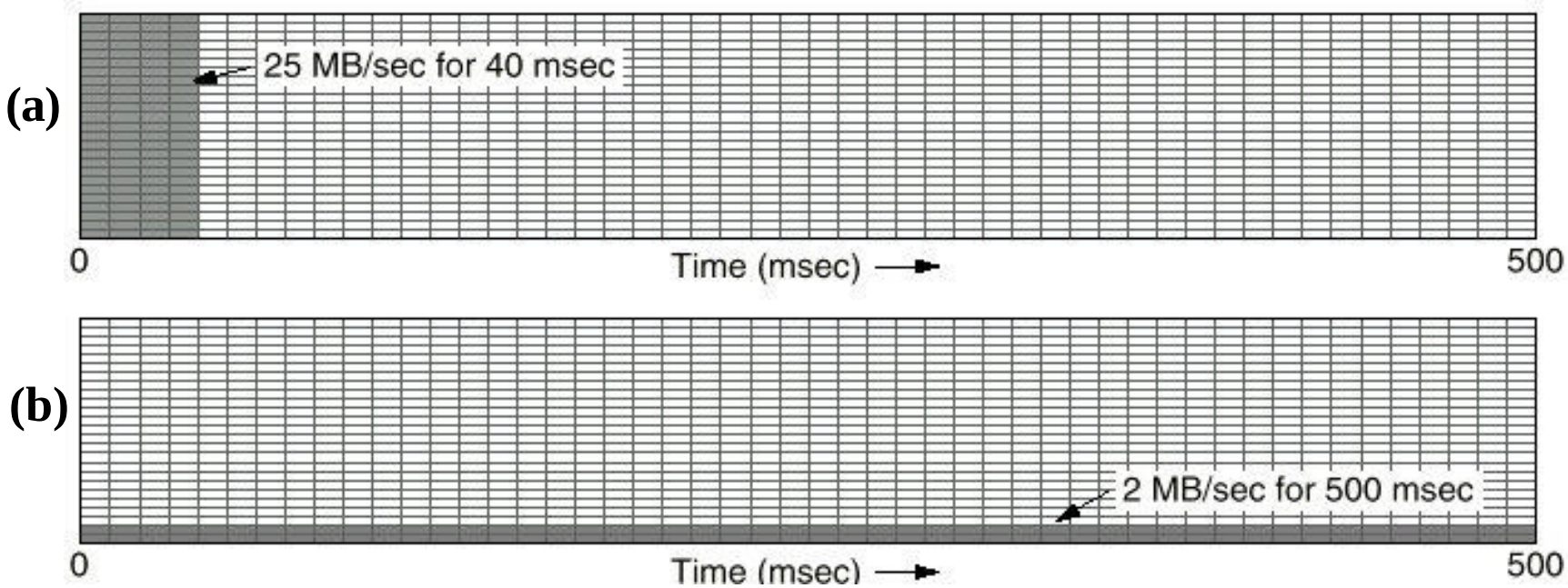
- **Traffic Shaping:**
  - **Heavily used in VC subnets including ATM networks.**
  - **Avoid bursty traffic by producing more uniform output at the hosts.**
  - **Representative examples: Leaky Bucket, Token Bucket.**
- **Admission Control:**
  - **Used in VC subnets.**
  - **Once congestion has been detected in part of the subnet, no additional VCs are created until the congestion level is reduced.**
- **Choke Packets:**
  - **Used in both datagram and VC subnets.**
  - **When a high level of line traffic is detected, a choke packet is sent to source host to reduce traffic.**
  - **Variation Hop-by-Hop choke packets.**
- **Load Shedding:**
  - **Used only when other congestion control methods in place fail.**
  - **When capacity is reached, routers or switches may discard a number of incoming packets to reduce their load.**

Congestion Control Algorithms: The Leaky Bucket

- **A traffic shaping method that aims at creating a uniform transmission rate at the hosts.**
- **Used in ATM networks.**
- **An output queue of finite length is connected between the sending host and the network.**
- **Either built into the network hardware interface or implemented by the operating system.**
- **One packet (for fixed-size packets) or a number of bytes (for variable-size packets) are allowed into the queue per clock cycle.**
- **Congestion control is accomplished by discarding packets arriving from the host when the queue is full.**



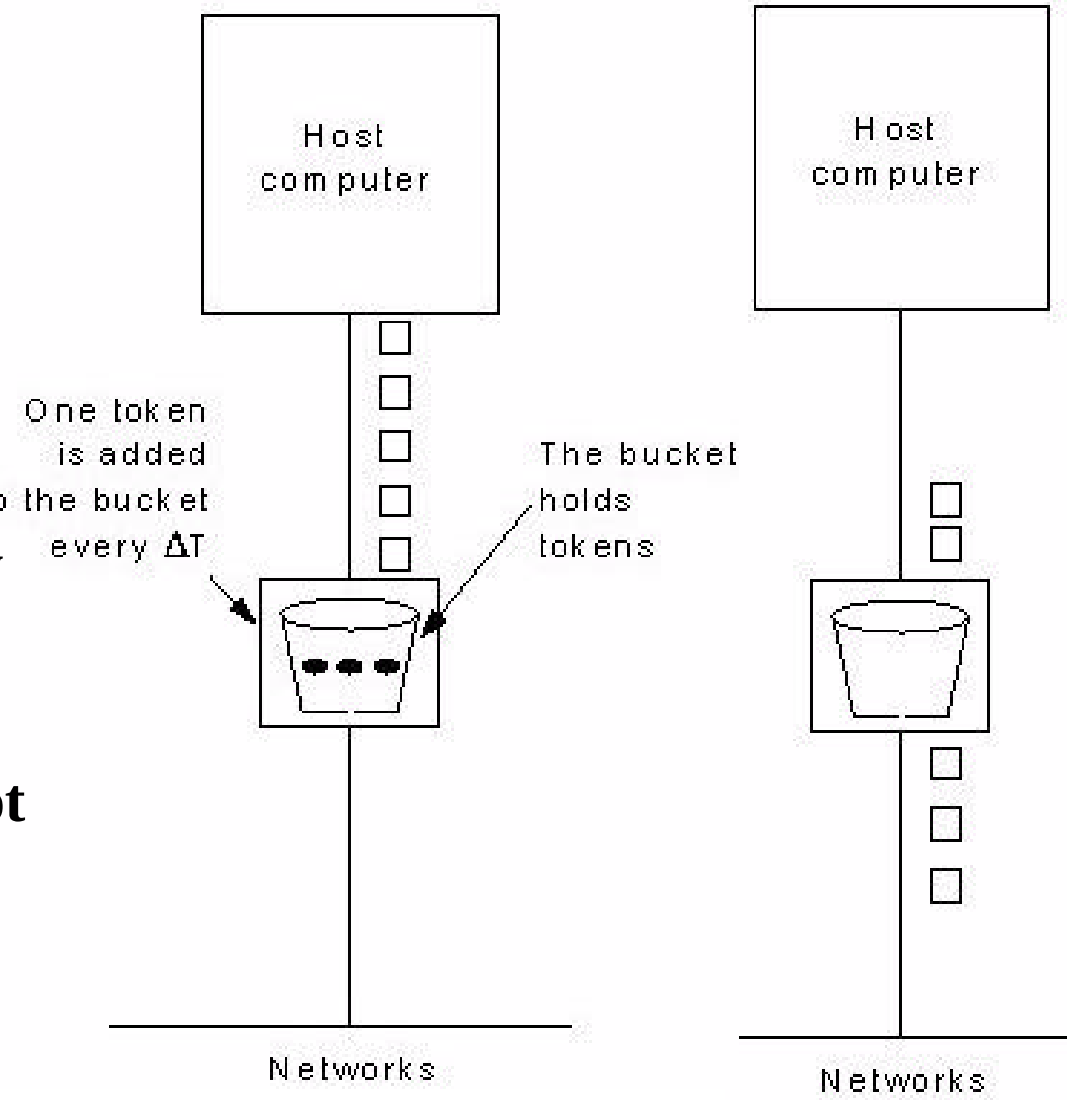
Leaky Bucket Traffic Rate Example



(a) Input to a leaky bucket from host
(b) Output from a leaky bucket.

Congestion Control Algorithms: The Token Bucket

- **An output queue is connected to the host where tokens are generated and a finite number is stored at the rate of ΔT**
- **Packets from the host can be transmitted only if enough tokens exist.**
- **When the queue is full tokens are discarded not packets.**
- **Implemented using a variable that counts tokens.**



Congestion Control Algorithms: Choke Packets

- Used in both VC and datagram subnets.
- A variable "*u*" is associated by the router to reflect the recent utilization of an output line:

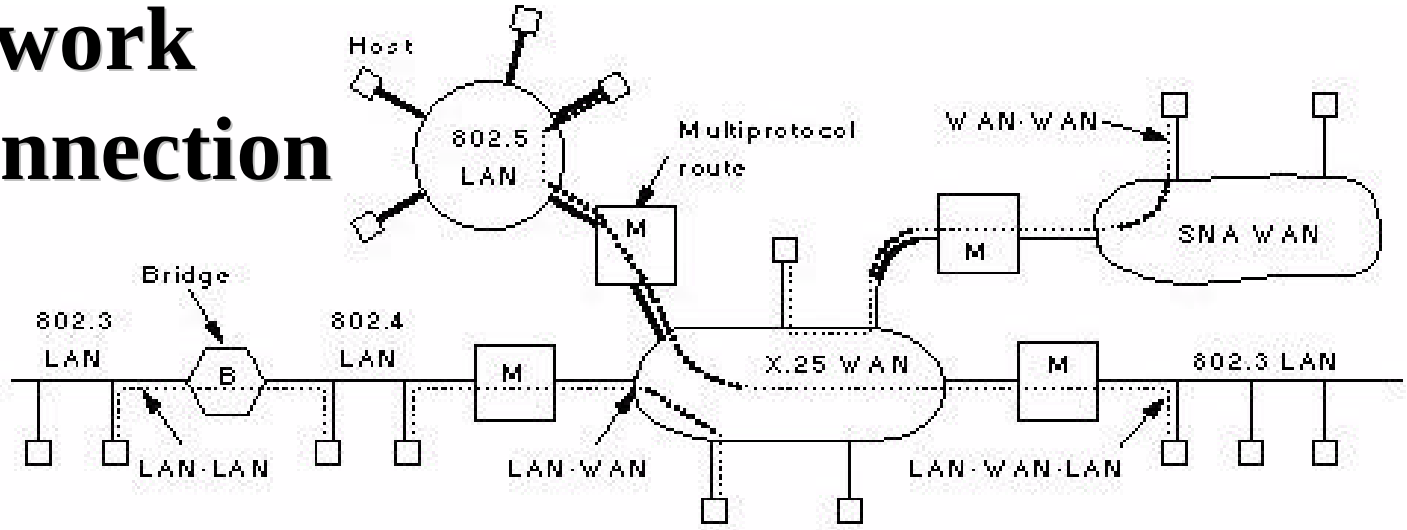
$$u = au_{old} + (1 - a) f$$

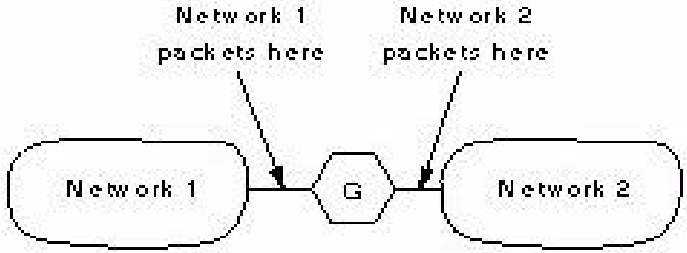
- When "*u*" goes above a given threshold, the corresponding line enters a warning state.
- Each new packet is checked if its output line is in warning state if so:
  - The router sends a choke packet to the source host with the packet destination.
  - The original packet is tagged (no new choke packets are generated).
- A host receiving a choke packet should reduce the traffic to the specified destination.
- A variation (Hop-by-Hop Choke Packets) operate similarly but take effect at each hop while choke packets travel back to the source.

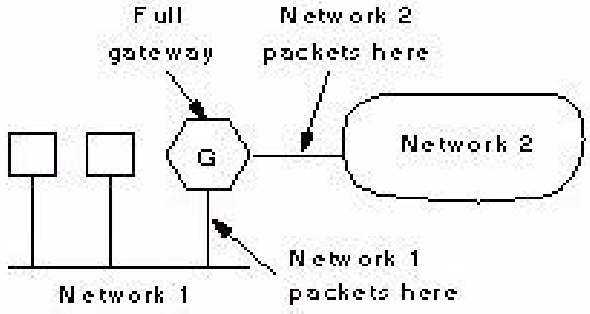
INTERNETWORKING

- **When several network types with different media, topology and protocols, are connected to form a larger network:**
  - **UNIX: TCP/IP**
  - **Mainframe networks: IBM's SNA, DEC's DECnet**
  - **PC LANs: Novell: NCP/IPX, AppleTalk**
  - **ATM, wireless networks etc.**
- **The "black box" converter unit used to connect two different networks depend on the layer of connection:**
  - **Layer 1 (physical): Repeaters, bit level**
  - **Layer 2 (data link): Bridges, data link frames**
  - **Layer 3 (network): Multiprotocol routers, packets**
  - **Layer 4 (transport): Transport gateways**
  - **Above 4 (application): Application gateways.**

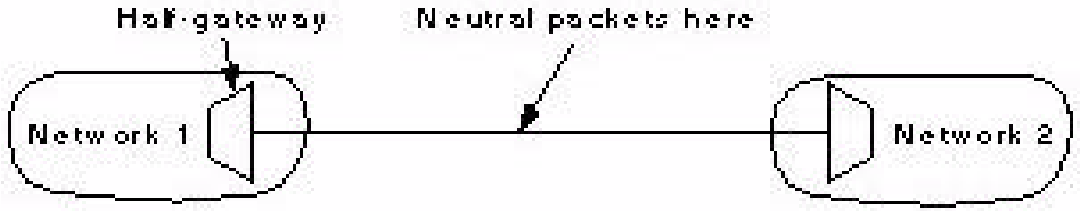
Network Interconnection







A full gateway two WANs **A full gateway LAN-WAN**



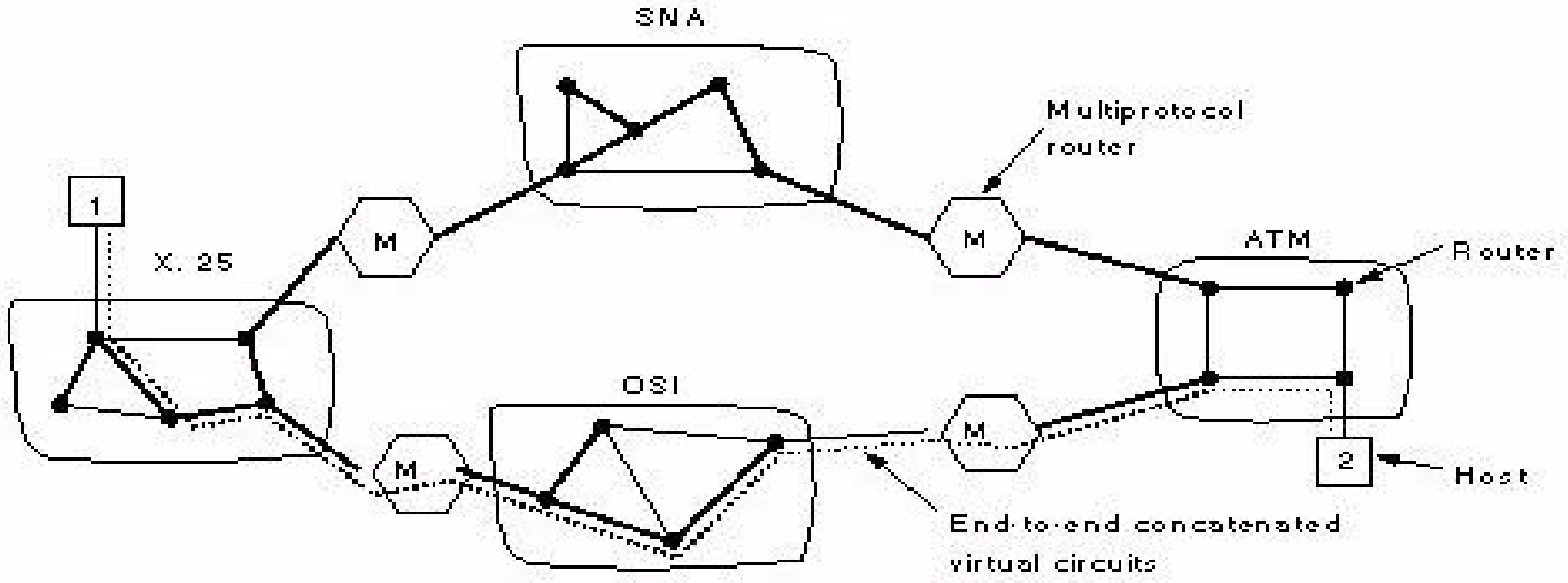
Two half-gateways

Types of Network Differences

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

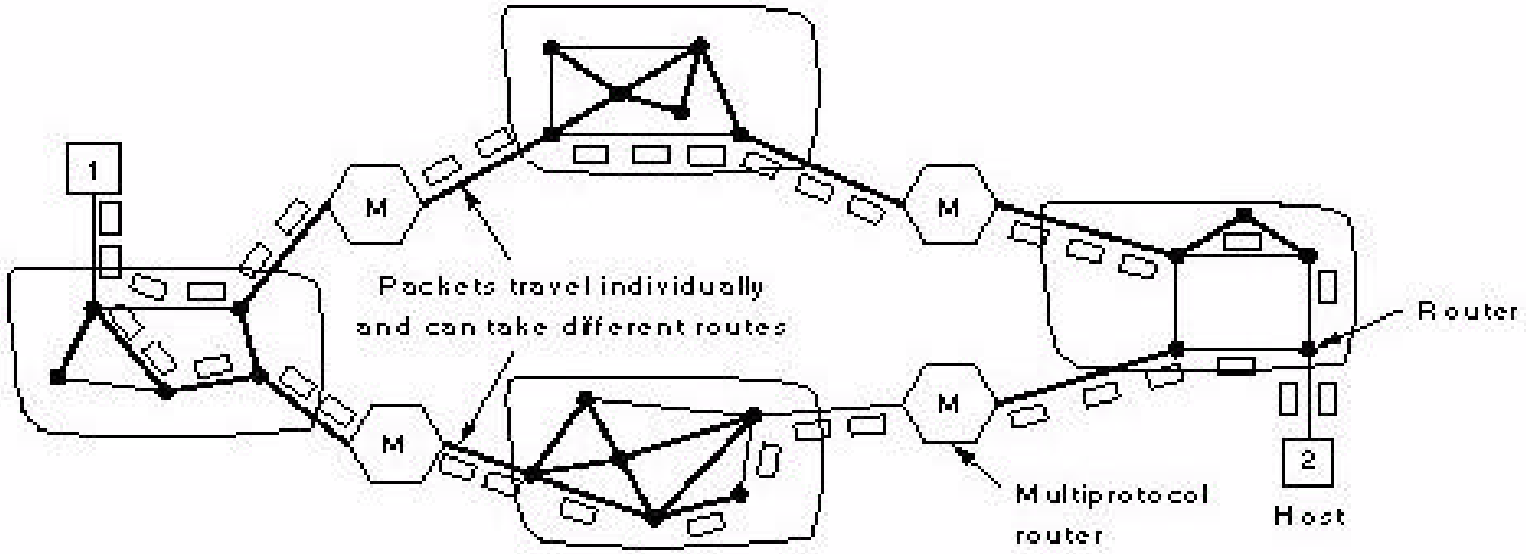
Concatenated Virtual Circuits Internetworking

- **Connection-oriented concatenation of virtual circuit subnets.**
- **A virtual circuit is established across several VC subnets.**
- **As packets cross from one subnet to the next:**
  - **Packets formats and virtual circuit numbers are changed.**



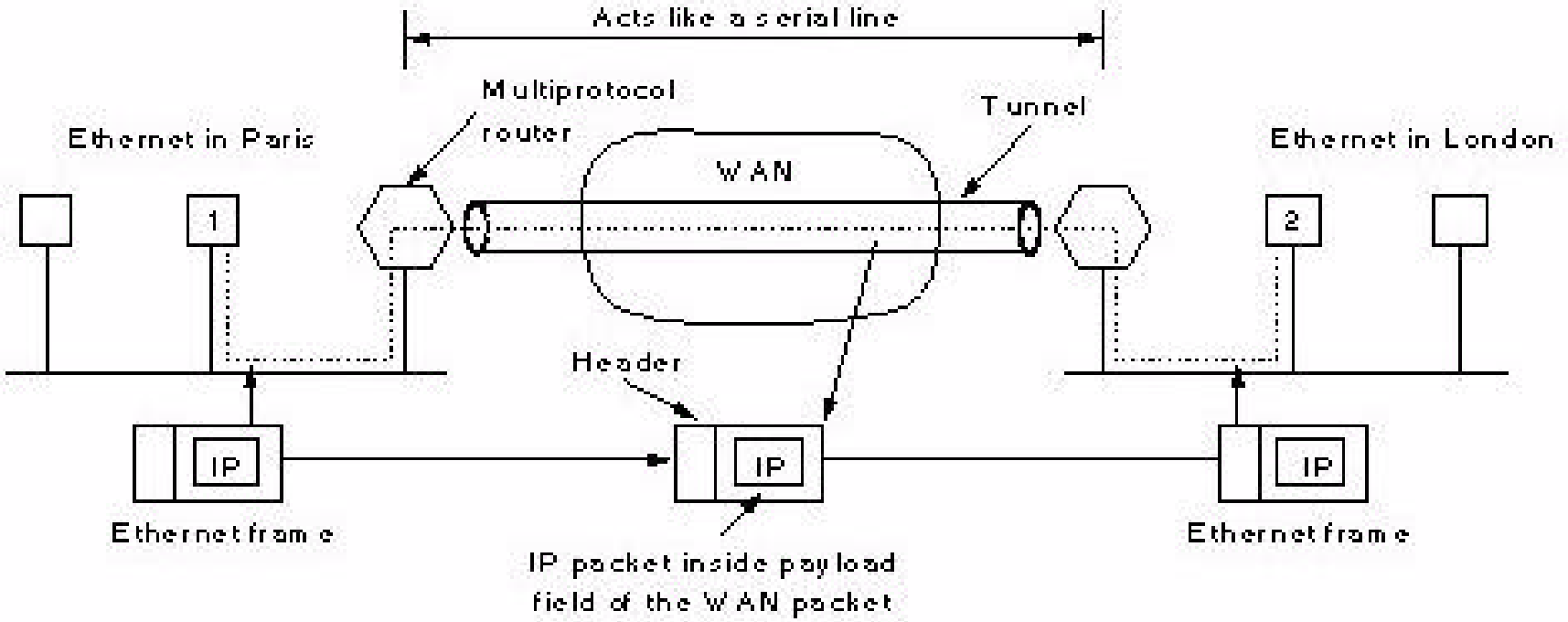
Connectionless Internetworking

- **Internetworked datagram subnets**
- **Multiprotocol router used to:**
  - **Translate between two or more network layer protocols of various subnets.**
  - **Packet format conversion: fields, address, etc.**
- **Possible incompatibilities: Addressing.**



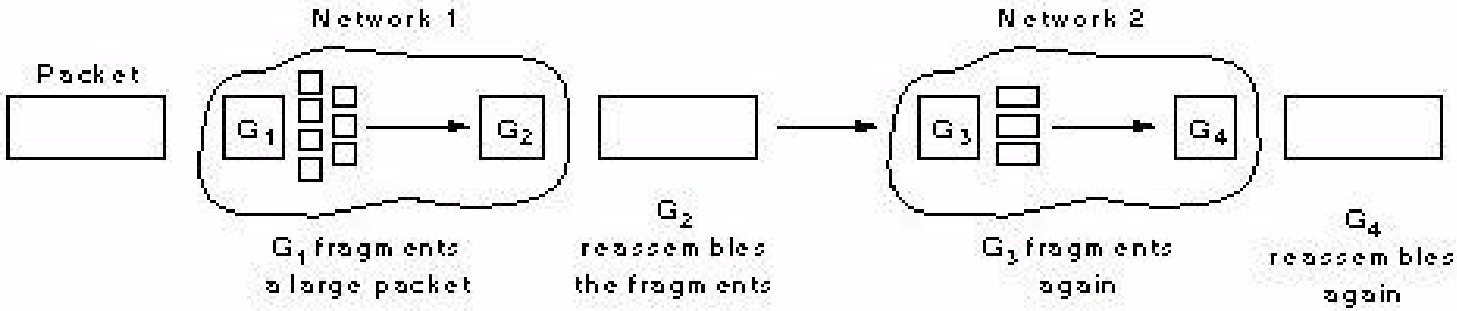
Internetworking Issues: Tunneling

- **Used when the source and destination hosts are on the same type of network with a different type of network in between.**
- **Using multiprotocol routers, packets of the common network type are inserted into the WAN network layer packets.**

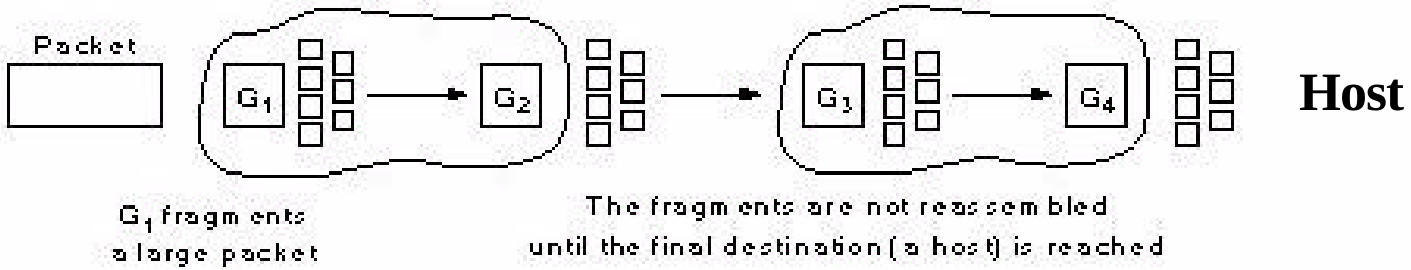


Internetworking Issues: Fragmentation

- When packets from a subnet travel to another subnet with a smaller maximum packet size, packets have to be broken down into fragments and send them as internet packets.

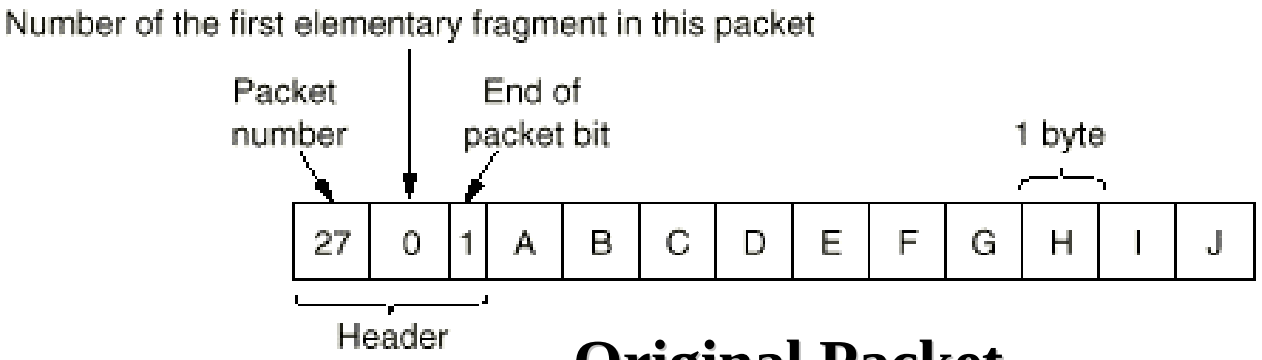


Transparent fragmentation

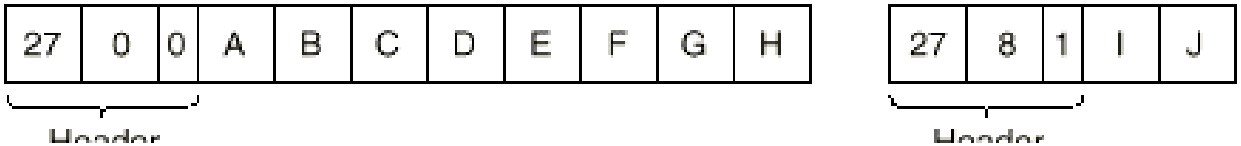


Non-transparent fragmentation

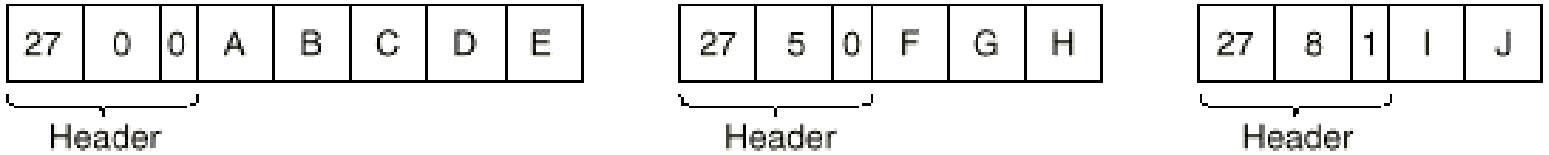
Packet Fragmentation Example



Original Packet



Fragments after passing through a network with max. packet size = 8



Fragments after passing through a network with max. packet size = 5