CEN445 – Network Protocols and Algorithms

Chapter 5 – Network Layer

5.4 Internetworking

Dr. Mostafa Hassan Dahshan
Department of Computer Engineering
College of Computer and Information Sciences
King Saud University
mdahshan@ksu.edu.sa
http://faculty.ksu.edu.sa/mdahshan

Internetworking

- So far assumed homogeneous networks
- Homogenous: same protocols in all layers
- Many different networks exist
  - LAN, MAN, WAN
  - numerous protocols for every layer
- Temporary condition? Unlikely
- Purpose of internetworking: allow different networks to communicate, user access data

How Networks Differ

Item	Some Possibilities
Service offered	Connection oriented versus connectionless
Protocols	IP, IPX, SNA, ATM, MPLS, AppleTalk, etc.
Addressing	Flat (802) versus hierarchical (IP)
Multicasting	Present or absent (also broadcasting)
Packet size	Every network has its own maximum
Quality of service	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, token bucket, RED, 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

How Networks can be Connected

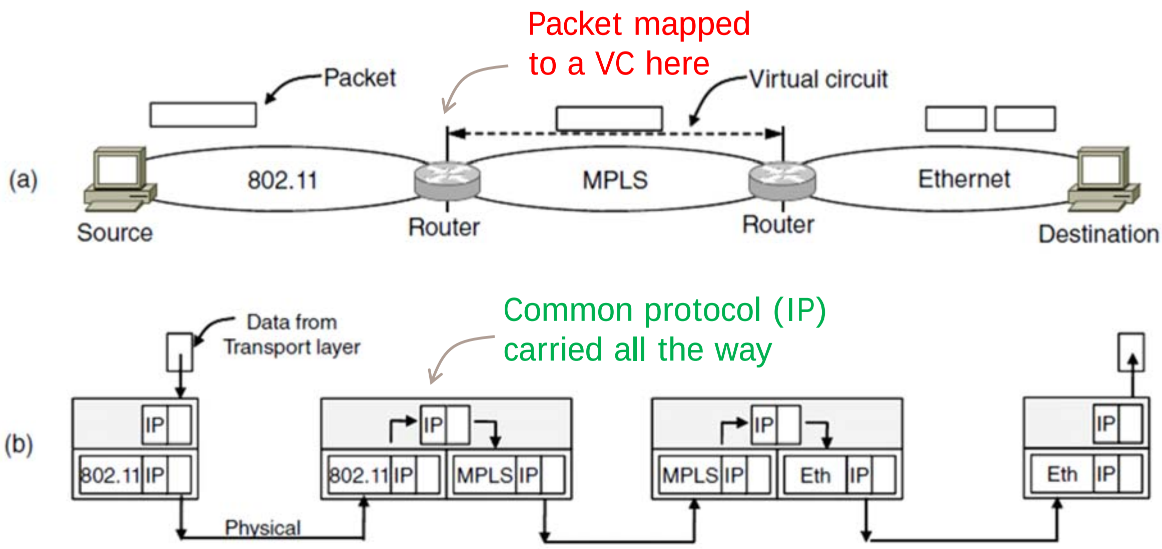
- Devices placed on boundaries
  - convert packet format between networks
  - build common layer on top of diff networks
- Common layer proposed: TCP/IP
- Previously studied: hubs, bridges, switches
- We now focus on network layer

عربي -
中文

English

How Networks can be Connected

Internetworking based on a common network layer – IP



How Networks can be Connected

- An internet of 802.11, MPLS, Ethernet
- Source from 802.11 → Ethernet destination
- Further separated by MPLS network
- Different forms of addressing
- Packet carry network layer address
- Can identify any host across 3 networks

How Networks can be Connected

- From 802.11 to MPLS
  - connectionless to connection-oriented
  - VC must be set up
- From MPLS to Ethernet
  - 802.11 work with large frames than Ethernet
  - may need to be divided into fragments

How Networks can be Connected

- Essential diff between routing/switching
- Routing
  - packet is extracted from frame
  - based on network address decide where to send
- Switching/bridging
  - entire frame transported based on MAC address
- Switches don't have to understand network layer protocol used. Routers do.

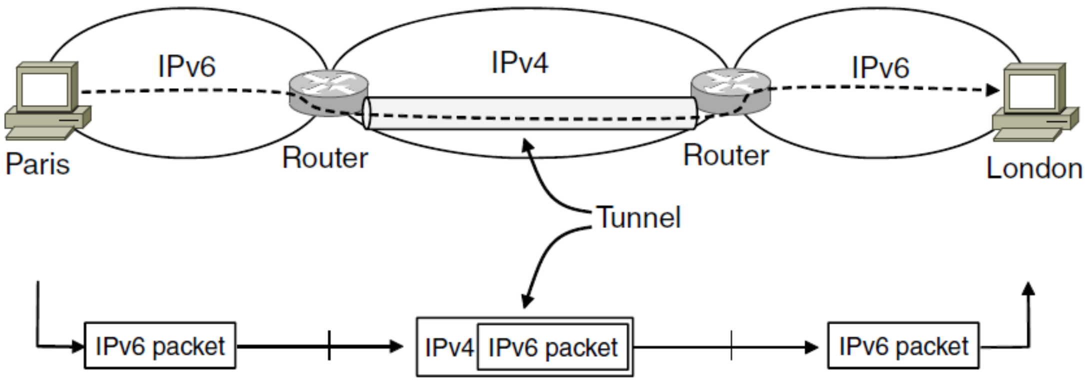
How Networks can be Connected

- Internetworking not as easy as shown
- Different features in LANs are hard to mask
  - max packet size, priority classes
- Bridges connect same link layer networks
- Routers connect different networks
- Works only with common network layer
- IPX, SNA, AppleTalk no longer widely used
- Current problem: IPv4, IPv6

Tunneling

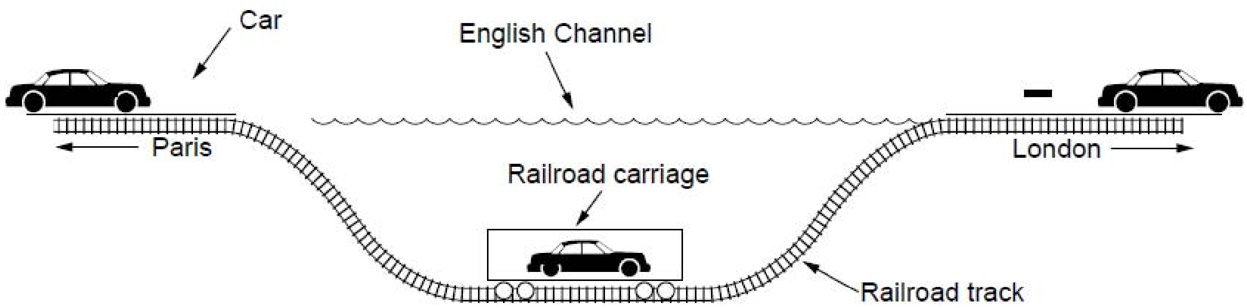
- Source/destination on same network type
- Different network in between
- Used to connect isolated hosts, networks
- Example: IPv6 over IPv4
- Hosts in the middle network unreachable
- Can be turned to advantage: VPN

Tunneling



- IPv4 router encapsulates packet with IPv4 header
- Addressed to multiprotocol router at other side
- Other router unwrap IPv6 packet, send to dest host

Tunneling



- Example: tunneling car from England to France
- Car is carried as a freight

Internetwork Routing

- More complications than in single network
- Networks may use different routing algorithms
  - link-state knows topology, distance vector do not
- Different operators have different metrics for cost
- Operators may want to hide path details
- Require algorithms that scale well using hierarchy
- Thus, routing protocols are classified into
  - interior gateway protocols: e.g. RIP, OSPF
  - exterior gateway protocols: e.g. BGP

Internetwork Routing

- Autonomous System (AS): network(s) controlled by a common admin
- Example: Internet Service Provider (ISP)
- Little info exposed to find routes across net
- Ops freely select routes within their nets
- Routing affected by business arrangement
- Also, non-technical factors: routing policy

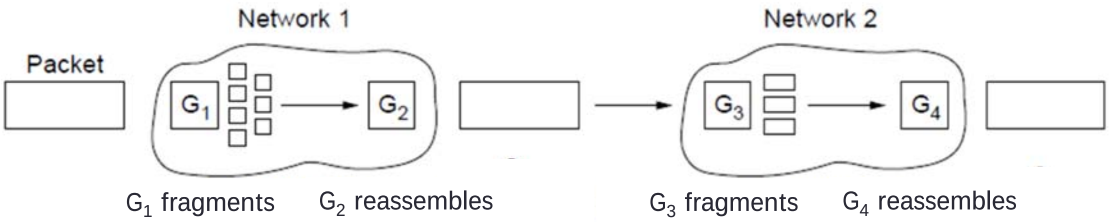
Packet Fragmentation

- Each network has max size limit on packets
  - hardware (e.g. Ethernet frame)
  - operating system (buffer sizes)
  - protocols (no. of bits is packet length field)
  - compliance with some (inter)national standard
  - desire to reduce error-induced retransmissions
  - prevent one packet occupy channel too long
- Common technologies
  - Ethernet: 1500 B; WLAN: 2272 B; IP: 64 KB

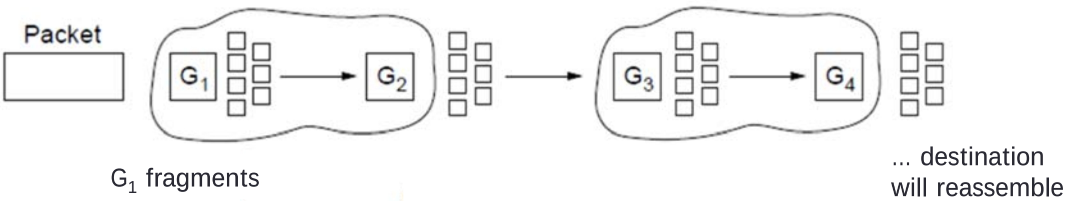
Packet Fragmentation

- Large packets preferred to reduce overhead
- Problem: large packet to travel through a network whose max packet size is too small
- Solution 1: prevent problem
  - set path Maximum Transfer Unit to smallest
  - problem: path may change, MTU also change
- Solution 2: allow fragmentation
  - routers break packets to smaller fragments
  - reverse process is more difficult

Packet Fragmentation



Transparent – packets fragmented / reassembled in each network



Non-transparent – fragments are reassembled at destination

Packet Fragmentation

- Transparent fragmentation
  - exit router must know when all pieces received
    - provide end-of-packet or count field
  - all packets must exit via same router
    - some performance may be lost
  - more work on routers
    - buffer fragments, decide when to throw them

Packet Fragmentation

- Nontransparent fragmentation
  - router do less work, IP model
  - fragments must be numbered
  - packet no. provided in each fragment
  - absolute byte offset, end-of-packet flag

Problems

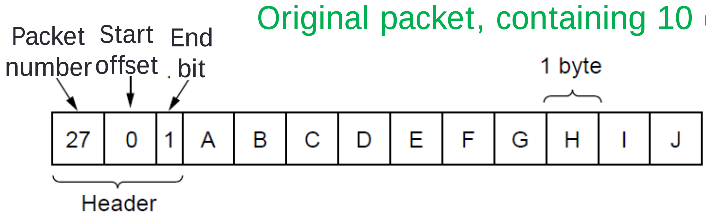
☹ higher overhead due to headers

☹ whole packet is lost if a fragment is lost

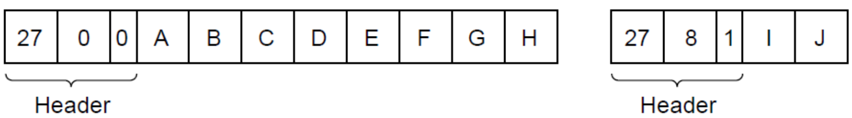
Packet Fragmentation

Example of IP-style fragmentation

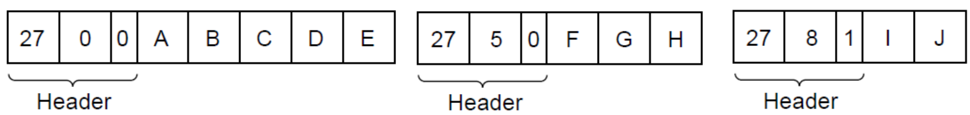
Original packet, containing 10 data bytes



Fragments after passing through a network with maximum packet size of 8 payload bytes plus header.



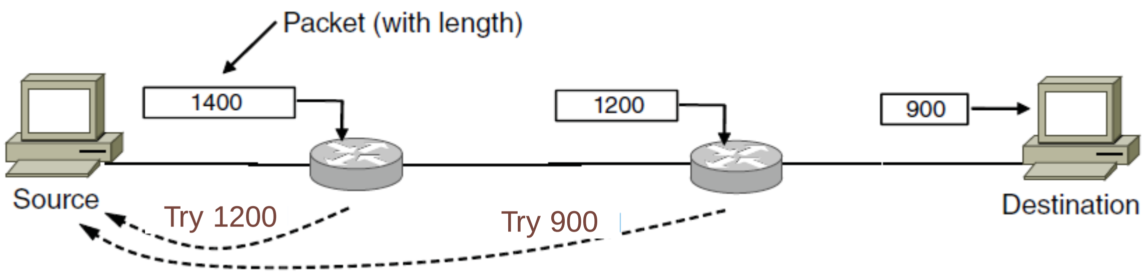
Fragments after passing through a size 5 gateway.



Packet Fragmentation

- Better: back to avoid fragmentation solution
- Path MTU discovery
  - send packet with no-fragmentation allowed
  - if router receives packet too large
    - generate error message, send it to source, drop packet
  - source re-fragment packet to smaller pieces
  - if another router, smaller MTU, repeat process

Packet Fragmentation



- Source knows right MTU
- Higher layer fragmentation still possible
- Disadvantage: added setup delay

External References

- http://searchnetworking.techtarget.com