Internet Protocols

ITS323: Introduction to Data Communications

Sirindhorn International Institute of Technology
Thammasat University

Prepared by Steven Gordon on 17 August 2011

ITS323Y11S1L12, Steve/Courses/ITS323/Lectures/ip.tex, r1941

Contents

LANs and WANs

LANs

- Different types: different topologies, different technologies, different purposes
- Many LANs operate at layers 1 and 2 (Physical and Data Link Layer) using switches and hubs
- Bridges can connect LANs of similar technologies together

WANs

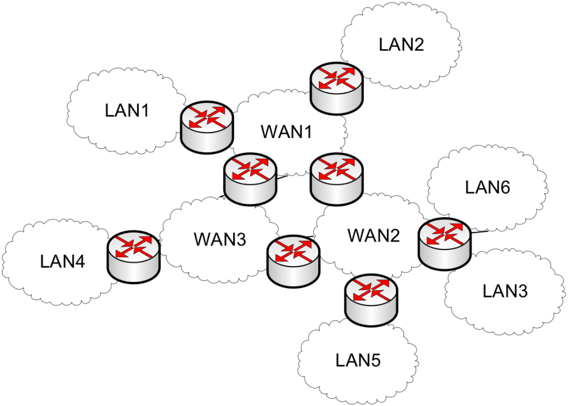
- Can interconnect LANs over a larger distance
- Point-to-point link (e.g. ADSL, PDH) or a network (e.g. ATM, SDH, telephone) using packet or circuit switching
- Device that interconnects the WAN to LAN must support both technologies
- WANs typically operate at Layers 1 and 2

Connect Multiple LANs and WANs

- Organisations have different requirements of their network, and therefore may choose different technologies for their LANs/WANs
- Aim: allow any computer to communicate with any other computer, independent of what LAN/WAN they are connected to
- Internetworking involves connecting the many different types of LANs/WANs together to achieve this aim

Internetworking with Routers

- Internetworking is performed using routers
- Routers connect two or more LANs or WANs together
- Routers are packet switches that operate at network layer



Terminology

- Routers: nodes that connect networks (LANs/WANs) together; operate at network layer
- Subnetworks: individual networks (LANs and WANs)
- Internetworking: connect two or more subnets together using routers
- An internetwork or an internet: the resulting network from internetworking
- The Internet: an internet that uses the Internet Protocol (IP) and used today to connect networks across the globe
- Routing: process of discovering a path from source to destination through a network
- Forwarding: process of sending data along a path through a network
- Packet Switch: a generic device that performs switching in a Packet Switching network. May operate at data link or network layer. A packet switch at network layer is called a router
- Circuit Switch: a generic device that performs circuit switching in a Circuit Switching network
- Ethernet switch: an IEEE 802.3 switch (either Ethernet, Fast Ethernet or Gigabit Ethernet). Operates at data link layer

Requirements of an Internetworking Protocol

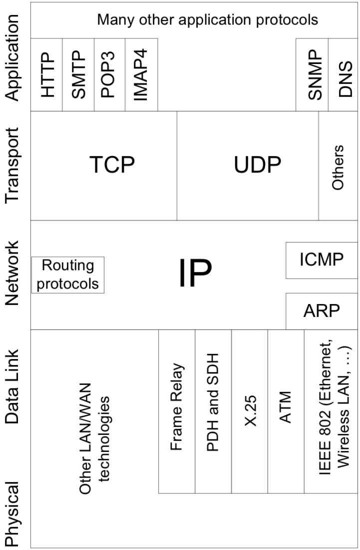
- Provide link between subnetworks
- Provide for routing and delivery of data between processes on different subnets
- Provide service to keep track of use of networks and maintain status information
- Provide above services without requiring changes to the subnets. Accommodate differences between subnets, e.g.
  - Different addressing schemes
  - Different maximum packet size
  - Different timeouts
  - Error recovery
  - Status reporting
  - Routing techniques
  - Security
- The Internet Protocol meets some of these requirements. Others are left to ICMP, TCP and other protocols in the TCP/IP architecture

Contents

The Internet Protocol

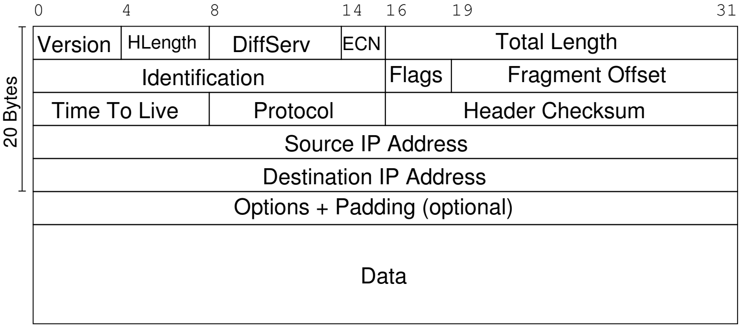
- IP is the internetworking protocol used in the Internet
  - We focus on IP version 4 (IPv4); IPv6 is available but net yet in widespread use
  - Other internetworking protocols: IPX, X.25, CLNP, SCCP
- Initially developed by US Department of Defence; now Internet Standard produced by IETF
- Features of IP:
  - Connectionless, network layer internetworking protocol using datagram packet switching
  - Provides data delivery, addressing, fragmentation and re-assembly
- Features IP does NOT provide:
  - Connection control, error control, flow control (TCP)
  - Status reporting (ICMP)
  - Priority, quality of service (DiffServ, IntServ)
  - Security (IPsec)

IP in the TCP/IP Stack



IP Datagram

- Variable length header and variable length data
- Header: 20 Bytes of required fields; optional fields may bring header size to 60 Bytes
- Data: length must be integer multiple of 8 bits; maximum size of header + data is 65,656 Bytes



IP Datagram Fields

- Version [4 bits]: version number of IP; current value is 4 (IPv4)
- Header Length [4 bits]: length of header, measured in 4 byte words
- DiffServ [6 bits]: Used for quality of service control
- ECN [2 bits]: Used for notifying nodes about congestion
- Total Length [16 bits]: total length of the datagram, including header, measured in bytes
- Identification: sequence number for datagram
- Flags: 2 bits are used for Fragmentation and Re-assembly, the third bit is not used
- Fragment Offset [13 bits]: See Fragmentation and Re-assembly
- Time To Live [8 bits]: datagram lifetime
- Protocol [8 bits]: indicates the next higher layer protocol
- Header Checksum [16 bits]: error-detecting code applied to header only; recomputed at each router
- Source Address [32 bits]: IP address of source host
- Destination Address [32 bits]: IP address of destination host
- Options: variable length fields to include options
- Padding: used to ensure datagram is multiple of 4 bytes in length
- Data: variable length of the data

Connectionless Internetworking with IP

Connection-oriented Internetworking

- Logical connection created between source and destination for data transfer
- All datagrams sent within connection are associated with each other
- Connection setup, data transfer, connection termination

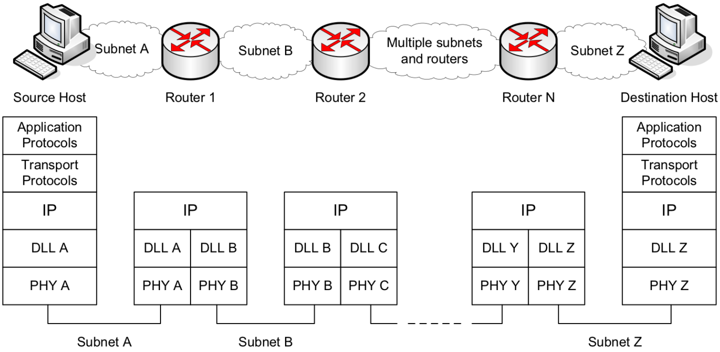
Connectionless Internetworking

- No connection between source and destination
- Datagrams are treated independently
- Advantages:
  - Flexible: can deal with different networks, requires little of subnets
  - Very small overhead if connectionless transport (e.g. UDP) is used

IP Hosts and Routers

- Hosts are the end-devices (stations)
  - Usually only use single network interface at a time
  - Hosts do not forward IP datagrams
  - Either source or destination
- Routers are the datagram packet switches
  - Routers have two or more interfaces (since they connect LANs/WANs together)
  - Routers forward datagrams
  - Routers can act as a source or destination of datagrams (however this is mainly for management purposes)
- IP routing is the process of discovering the best path between source and destination
- IP forwarding is the process of delivering an IP datagram from source to destination

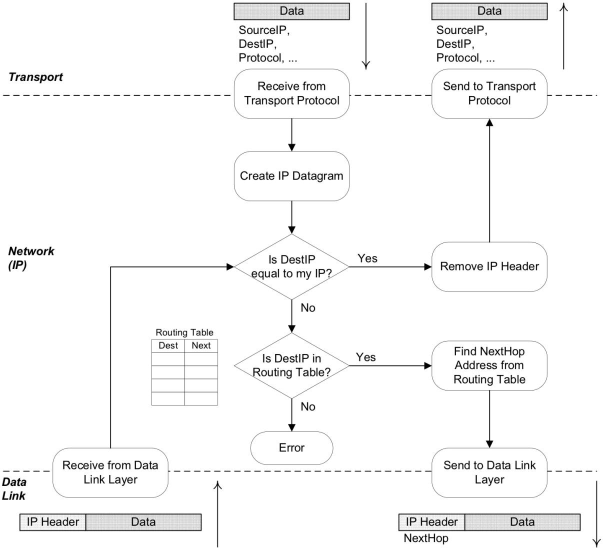
IP Hosts and Routers



IP Routing

- No routing protocol is specified for IP
- Any of the available routing protocols can be used depending on the network topology and requirements of network administrator, e.g. RIP, EIGRP, OSPF, BGP, ...
- Each routing protocol creates and updates a routing table, which stores information to determine the path from source to destination
- IP uses the information in the routing tables to forward datagrams
- In order to make routing tables manageable, three strategies are used in the Internet:
  - Storing Next-Hop Routes
  - Network-specific Routing
  - Default Routes

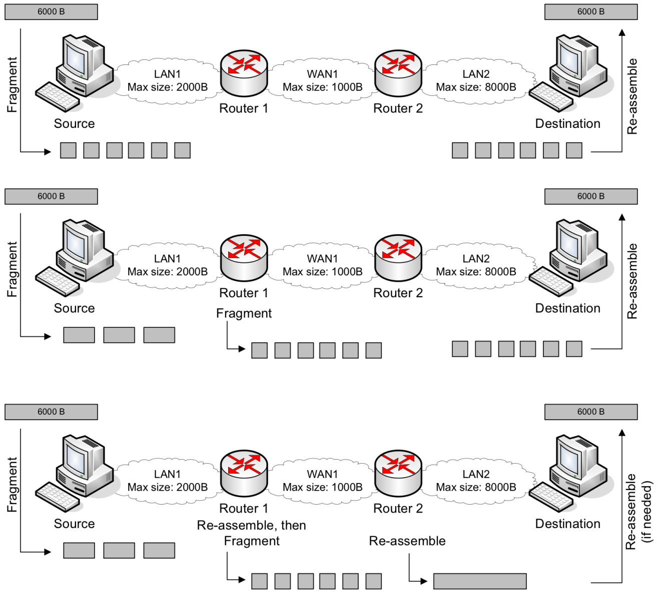
IP Forwawrding



Fragmentation and Re-assembly

- Network layer may divide data from transport layer into multiple blocks (fragmentation)
- Data is re-assembled before being delivered to transport layer at destination
- Why fragmentation and re-assemble?
  - Subnets on path from source to destination may limit maximum size of frame
  - Error control may be more efficient with smaller packets
  - Smaller packets means smaller buffers needed at receivers
- Disadvantages of fragmentation and re-assembly:
  - Smaller packets means header contributes larger overhead
  - More packets means more time processing by routers, receiver

Fragmentation and Re-assembly



Fragmentation and Re-assembly

Three general options in internetworking:

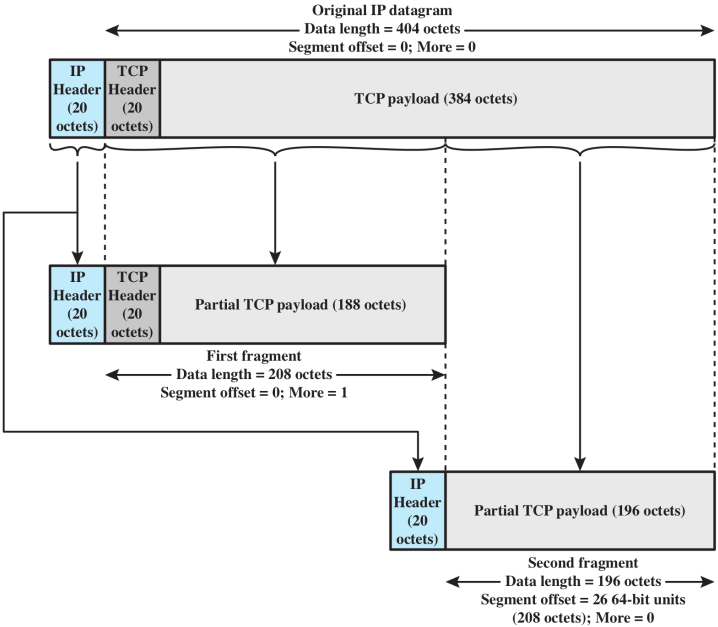
1. Fragment only at source; re-assemble only at destination
2. Fragment at source and routers; re-assemble only at destination
3. Fragment at source and routers; re-assemble at routers and destination

IP uses option 2:

- No need for source to know maximum transmission units along path
- No need for routers to have large buffers for re-assembly
- No need for all fragments to pass through same router

IP uses header fields to indicate if fragmentation has occured and identify fragments

Fragmentation Example



Datagram Lifetime in IP

- With adpative/dynamic routing, it is possible for a routing loop; datagram sent forever
- Datagram marked with lifetime, when lifetime expires datagram is discarded
- IP uses a hop count:
  - Time To Live (TTL) field in header set to number of hops source allows the datagram to traverse (e.g. 64, 255)
  - Each router that processes datagram decrements the TTL field
  - If TTL is 0, datagram is discarded
- Simpler than using actual time, as would require synchronisation between clocks on devices

Contents

IPv4 Addresses

- IPv4 addressess are 32 bits in length
- Split into network portion and host portion: first N bits identify a subnet in the Internet; last H bits identify an IP device (host/router) in that subnet
- All subnets in the Internet have unique network portion
- All IP devices in a subnet have same network portion, but unique host portions
- Where/how to split has changed over time: Classful, Subnet addressing, Classless addressing
- Focus on classless addressing
- Why split? Allows hierarchical addressing, makes routing in Internet scalable

Representing IPv4 Addresses

- Writing and remembering 32 bits is difficult for humans
- IP addresses usually written in dotted decimal notation
- Decimal number represents the bytes of the 32 bit address
- Decimal numbers are separated by dots

```
IP: 11000000111001000001000100111001
```

Classless IP Addressing

- Subnet mask or address mask identifies where the IP address is split between network and host portion
- Mask is 32 bits: a bit 1 indicates the corresponding bit in the IP address is the network portion; a bit 0 indicates the corresponding bit in the IP address is the host portion
- The mask can be given in dotted decimal form or a shortened form, which counts the number of bit 1's from left

```
IP:   10000010000010001001010011000001
Mask: 11111111111111111111110000000000
```

Special Case IP Addresses

Selected IP addressess are used for special purposes; they cannot be used to identify a host

Network Address identifies a subnet in the internet; all bits in host portion are 0

Directed Broadcast Address identifies all hosts on a specific subnet; all bits in host portion are 1

Local Broadcast Address identifies all hosts on the current subnet; all bits are 1

Loopback Address identifies current host; first 8 bits are 01111111; also called localhost

Startup Source Address identifies host if currently it has no address; all bits are 0

Selected addresses reserved for private networks (e.g. not connected to Internet; behind NAT)

- 10.0.0.0—10.255.255.255
- 172.16.0.0—172.31.255.255
- 192.168.0.0—192.168.255.255

IP Addressing Example

View the IP address on your own computer.

IP Addressing Example

My office computer has address 104.209.61.169/18. What is the network address and directed broadcast address for my network? How many IP devices can be attached to my network?

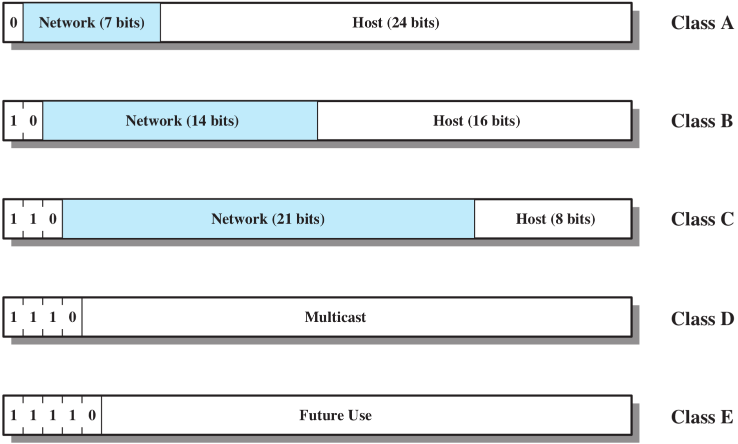
Classful IP Addressing

- Before "classless" addressing was introduced, the split was identified by one of 5 classes of addresses:

Class A	first bit 0; network/host split after 8 bits (1.0.0.0—126.0.0.0)
Class B	first two bits 10; split after 16 bits (128.0.0.0—191.255.0.0)
Class C	first three bits 110; split after 24 bits (192.0.0.0—223.255.255.0)
Class D	first four bits 1110; used only for multicast
Class E	first five bits 11110; reserved for future use

- Subnet mask not needed; first bits of address determine the split
- Problem: only allow 3 different size networks (class A, B or C)

Classful IP Addressing



Obtaining an IP Address

- Internet Assigned Numbers Authority (IANA) manages the assignment of IP addresses
- IANA delegates IP network ranges to regional authorities (e.g. APNIC), delegated further to national registries (e.g. THNIC)
- Organisations obtain network addresses from national/local registries
- Organisations are free to assign addresses as they wish from assigned network address

Other Network Layer Functionality

- ICMP: error reporting, ping
- ARP: map IP addresses to Ethernet addresses
- IPv6
- Multicasting
- Quality of Service
- Mobility
- Security