EECS, University of Ottawa

ELG5374 –Fall 2021

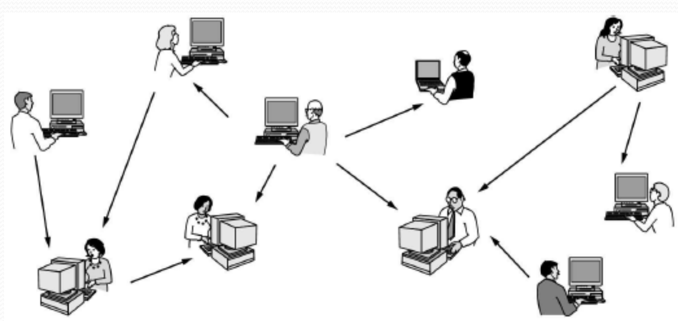
Computer Communication Network

Basics on Computer Networking

Note: some material in the slides has been taken from various other sources 1-1

1

Why we need computer networks?



Application Type	Example
Business-to-consumer	Ordering books on-line
Business-to-business	Car manufacturer ordering tires from supplier
Government-to-consumer	Government distributing tax forms electronically
Consumer-to-consumer	Auctioning second-hand products on-line
Peer-to-peer	File sharing

1-2

2

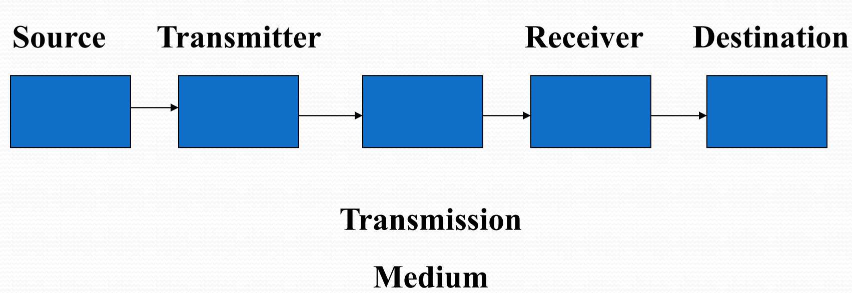
Fundamental Problem of Communication

- Reproduce at one point - either exactly or approximately - a message produced at another point
- Father of Communication Theory: Claude Shannon (MIT Professor)

1-3

3

Communications System Model



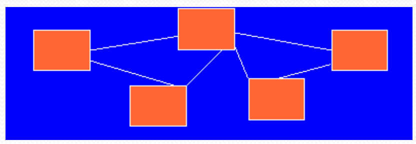
1-4

4

Structure of Transmission System

Two communicating nodes

Two or more nodes (routing issues, ..); ***Computer Network***

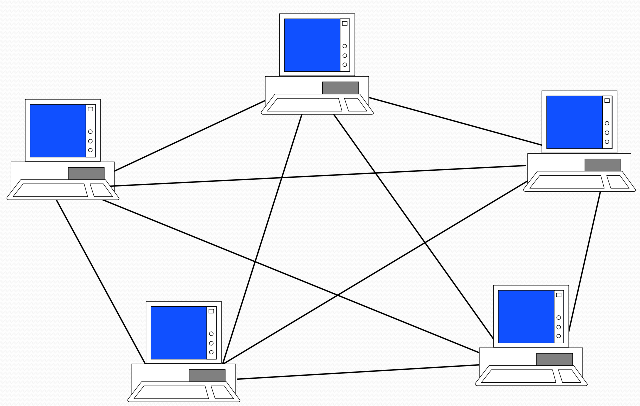


1-5

5

Computer Networks: Why?

Computing & communication devices need to exchange information



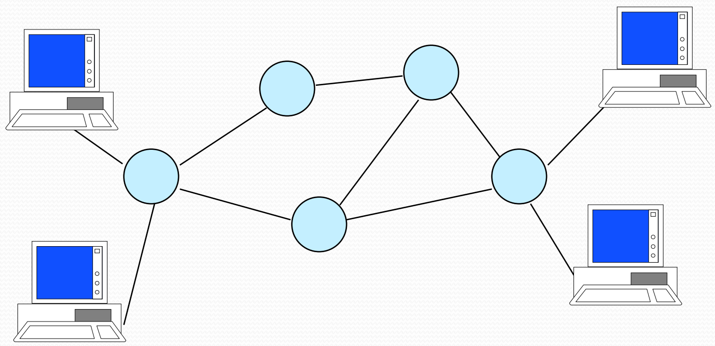
<u># of links required:</u>
unidirectional links:
n (n-1)
bidirectional links:
n (n-1)/2
n: # of devices

1-6

6

Computer Networks

We need switching nodes.



1-7

7

Is "Computer Communications" Important?

- History
  - 1960's "time-sharing" computers
  - 1970's several computers interconnected via wide area networks (WANs)
  - 1980's local area networks (LANs)
  - 1990's Integrated Services Digital Network (ISDN)
  - Late 1990's wireless LANs (WLANs)
  - 2000 Pervasive Computing, Broadband Wireless Access, Optical Networks, Home networks, Personal Access Networks
  - 2004+ Vehicular networks, sensor-nets, PANs, BANs….

1-8

8

Communication Tasks (1)

Transmission system utilization	Addressing
Interfacing	Routing
Signal generation	Recovery
Synchronization	Message formatting
Exchange management	Security
Error detection and correction	Network management
Flow control	

9

9

Communication Tasks (2)

- Transmission System Utilization
  - to make efficient use of transmission facilities
- Interface
  - compatible physical and electrical characteristics

1-10

10

Communication Tasks (3)

- Signal generation
  - generate signals capable of propagating through the transmission medium
- Synchronization
  - receiver should be able to determine when a signal begins to arrive and when it ends

1-11

11

Communication Tasks (4)

- Exchange Management
  - establishment of a connection, communication types, amount of data to be sent at one time
- Error Detection and Correction
  - procedures to make the communication reliable

1-12

12

Communication Tasks (5)

- Flow Control
  - mechanisms required to assure that the source does not overwhelm the destination
- Addressing
  - each computer must be identified

1-13

13

Communication Tasks (6)

- Routing
  - mechanisms to determine the route to use when transferring data from one point to another
- Recovery
  - mechanisms to recover from fatal errors

1-14

14

Communication Tasks (7)

- Message Formatting
  - form of the data to be exchanged or transmitted
- Security
  - Protect the confidentiality of the transferred information
- Network Management
  - Oversee the operation of the network

1-15

15

Types of Communication Networks

Classification according to the way the “information flows” are transported to the users

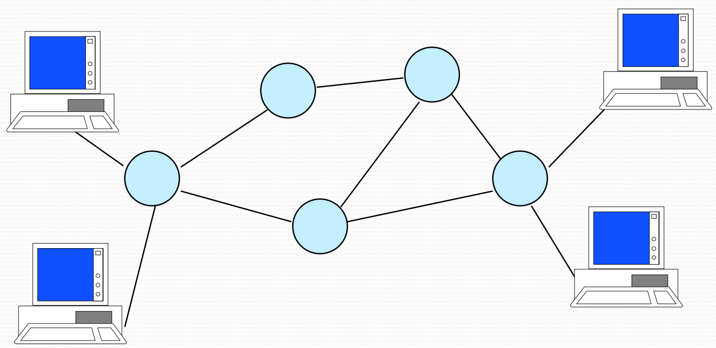
- Switching Networks
- Broadcast Networks

1-16

16

Switching Networks

Data are transferred from source to destination through a series of intermediate nodes

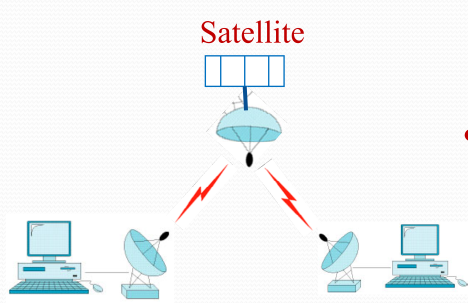


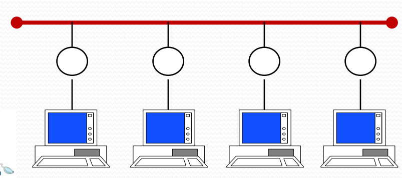
1-17

17

Broadcast Networks

- There are no intermediate switching nodes
- All users are connected on the same medium





1-18

18

Classification According to Coverage Area

- Local Area Networks (0-2 Km; campus)
  - Ethernet (10/100/1000 Mbps), Token ring (4, 16 Mbps), IEEE 802.11(b, g, a, n)
- Metropolitan Area Networks (2-50 km; corporate offices, city)
  - DQDB (Distributed Queue Dual Bus), WiMAX (IEEE 802.16.a/b/e), 4G/LTE
- Wide Area Networks (country, continent)
  - transmission lines, switching elements
- Personal Access Networks (PANs)
  - Bluetooth/IEEE 802.15.3
- Sensor Networks (Sensor-Nets)
  - ZigBee/IEEE 802.15.4
- Body Area Networks (BANs)

1-19

19

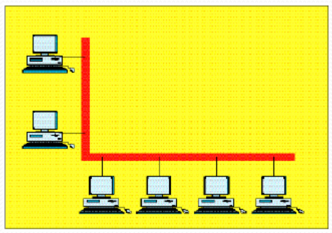
Local Area Networks (LANs)

- It expands over small geographic areas (within a building or close-by buildings)
- It is usually owned by the same organization
- The internal data rates are typically much greater than those of WANs
- Typically, they make use of broadcast rather than switching (Why????)

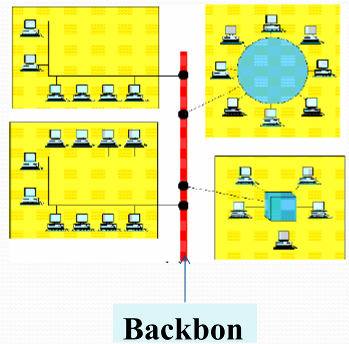
1-20

20

Local Area Networks (LANs)



Single-building LAN



Multi-building LAN

Examples: home network, wireless-wired campus network

1-21

21

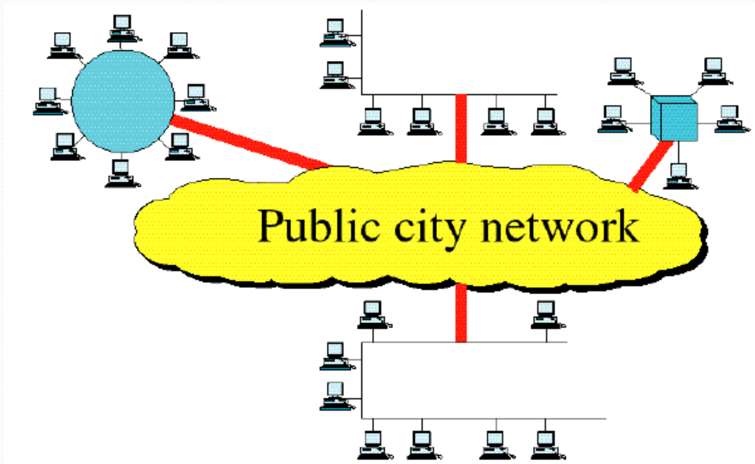
Examples of LANs

- Ethernet (10 Mbps/100 Mbps/1000 Mbps[=1 Gbps])
- Token Ring
- ATM LANs
- IEEE 802.11 Wireless LAN ("1st G....", b, a, g, n)
- HYPERLAN (European Wireless Standard)
- Home RF

1-22

22

Metropolitan Area Networks (MAN)

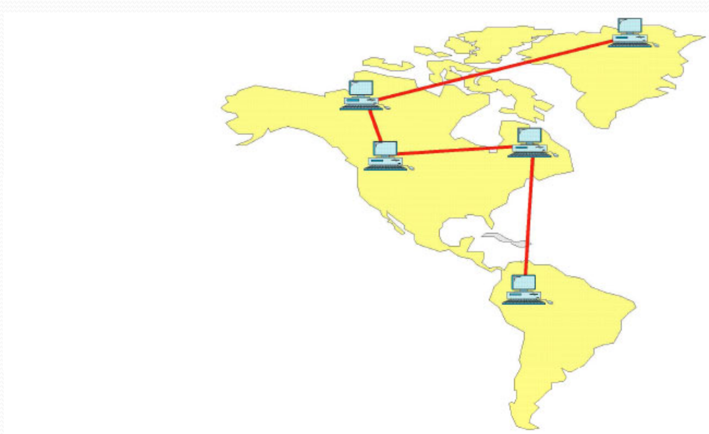


Examples: Ottawa-Carleton Research Institute (OCRI) MAN
National Capital Institute in Telecommunications (NCIT) MAN

1-23

23

Wide Area Networks (WAN)



Example: **Ca**nadian **N**etwork for the **A**dvancement of **R**esearch, **I**ndustry and **E**ducation (**CANARIE**)

1-24

24

Wide Area Networks (WAN)

- Traditionally, WANs have been implemented using one of two technologies
- Circuit Switching
- Packet Switching
  - Datagram
  - Virtual Circuit

1-25

25

Internetworking

- Internetworking: interconnecting **multiple** networks of **<u>different</u>** technologies in a **seamless** manner
- Uses both hardware and software
  - Extra hardware positioned between networks
  - Software on each attached computer
- System of interconnected networks is called an ***Internetwork*** or ***Internet***

1-26

26

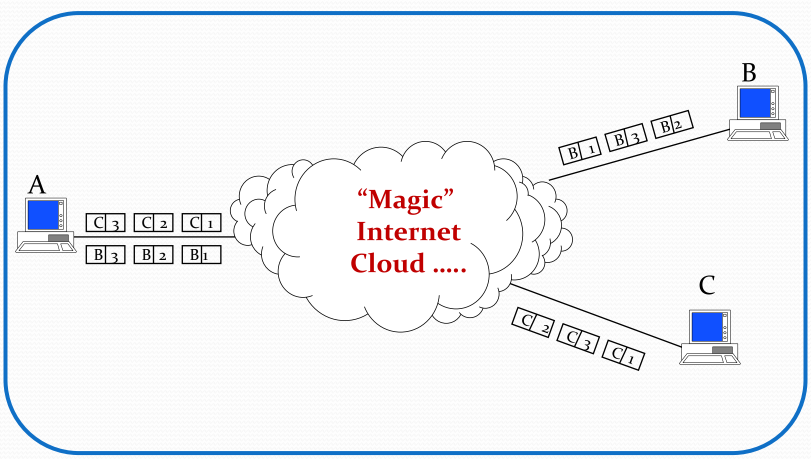
The Internet

- Internet evolved from ARPANET
  - first operational packet network
  - applied to tactical radio & satellite nets as well
  - had a need for interoperability
  - needed to be highly survivable (i.e. tolerate losses of network nodes)
  - lead to standardized TCP/IP protocols

1-27

27

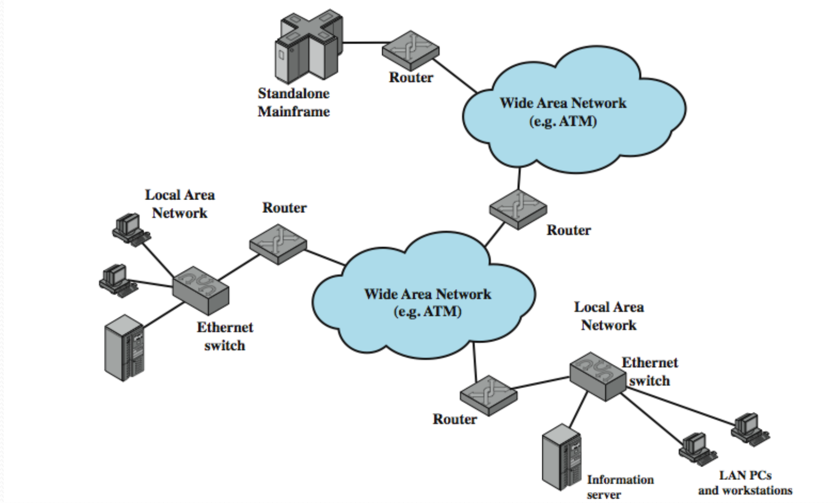
User' s view of Internet



1-28

28

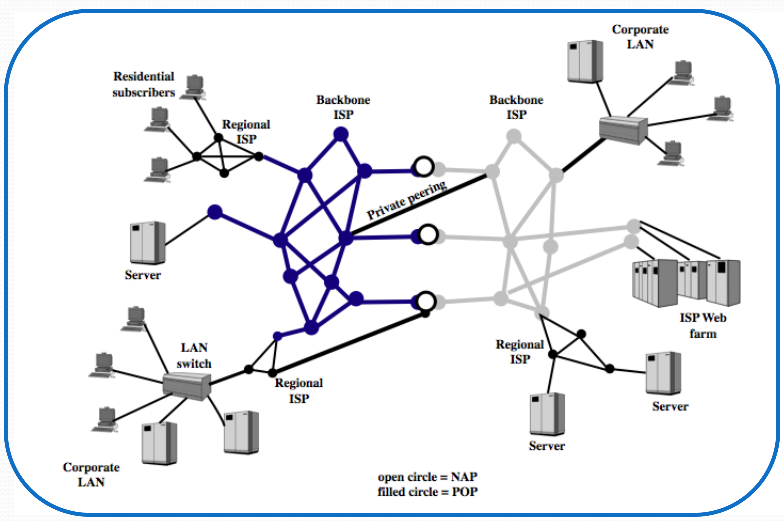
Internet Elements



1-29

29

A "possible" Internet Architecture(1)



1-30

30

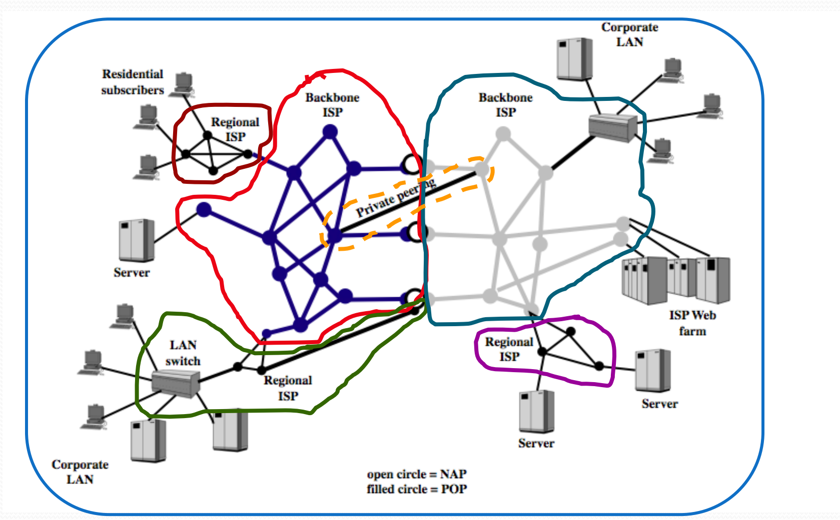
Autonomous System (AS)

- AS is a set of routers and networks managed by a single organization.
- AS consists of a group of routers exchanging information via a common routing protocol.
- Claiming that an AS is "connected", means that (excluding times of failures) there is always a "path" between any pair of nodes.

1-31

31

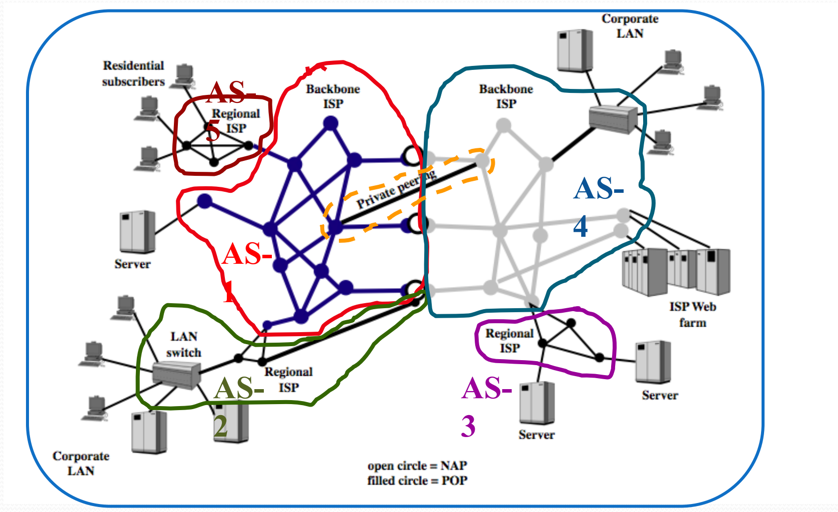
A "possible" Internet Architecture(2)



1-32

32

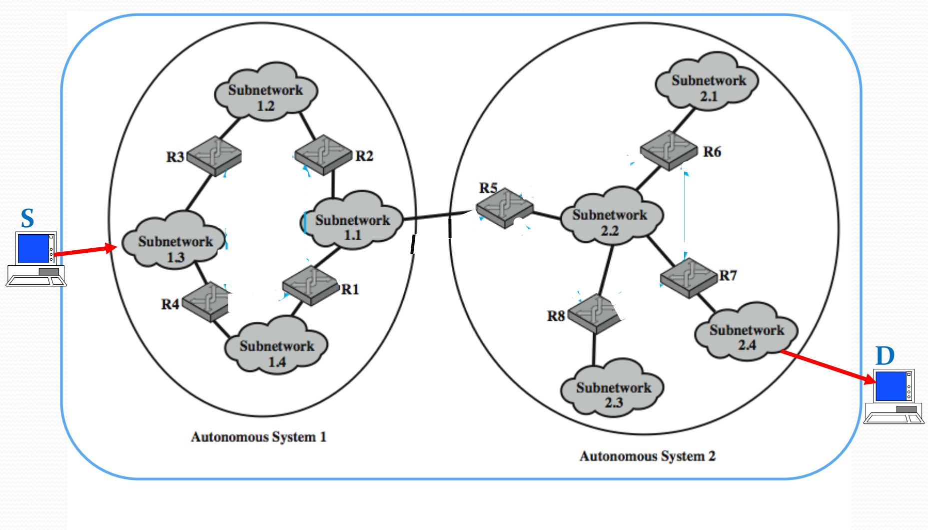
A "possible" Internet Architecture(3)



33

33

Example: 2-AS formed Internet

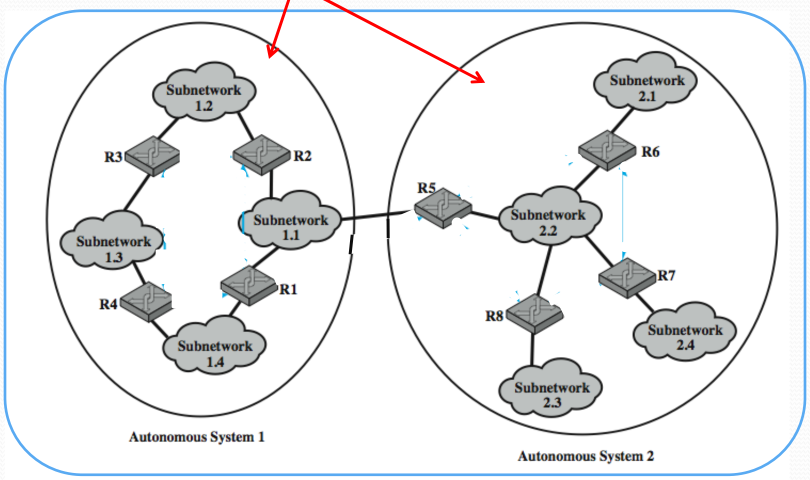


1-34

34

Within an AS domain:

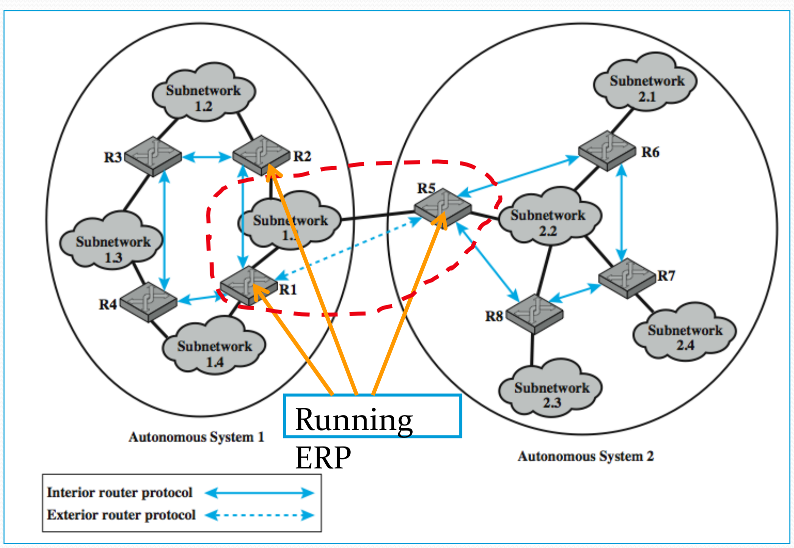
Interior Routing Protocol



1-35

35

Application of ERP



1-36

36

Protocols (1)

- Computer Networks pass useful information between (two or more) entities.
- The information is produced by "applications" (e.g. file transfer, e-mail, video-conferencing etc.)
- In order for the end-systems and networks to pass the information intelligibly, definition of a set of rules governing the exchange of data between two "entities" is needed.
- These rules constitute the protocols.

1-37

37

Protocols (2)

- Protocols
  - set of mutually acceptable conventions between the communicating entities.
  - 3 key elements
    - **syntax:** data formats and signals levels (format, fields, order, ...).
    - **semantics:** control information for coordination and error handling (meaning of things).
    - **timing:** speed matching and sequencing.

1-38

38

Protocol Architecture(1)

- Definition
  - A structured set of modules that implements the communication function
- Objective
  - Provide a flexible, modular structure, developed such that a change in one of the elements within the communications system will require minimal changes in the other elements

Protocol Architecture(2)

- How do we accomplish our objective?
  - By developing a layered architecture
  - the upper layer performs some tasks of its own, exchanges data and requests some service from the lower layer
  - the formatting of the data is independent of the actual implementation, and is not concerned how the lower layer is performing its part

A simple example: A Three -Layer Model (1)

- In general terms, communications involve three agents:
  - **applications** (e.g. file transfers, e-mail, www) more than one application may be running simultaneously on the same computer
  - **computers**
  - **networks**

1-41

41

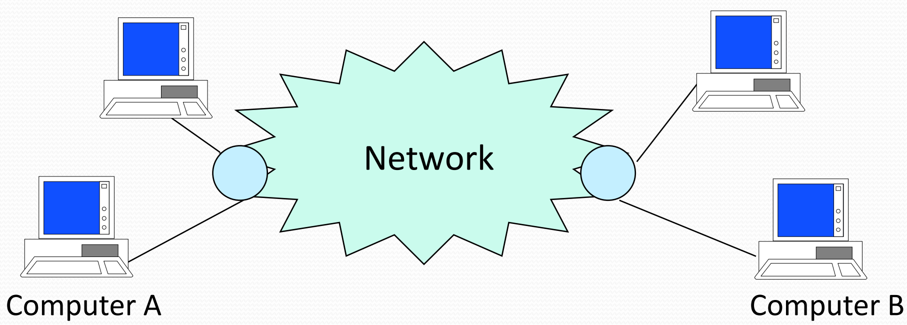
A simple example: A Three -Layer Model (2)

Applications	Application Layer	Contains logic needed to support the various user applications
Computer	Transport Layer	Concerned with the reliable delivery of data
Network	Network Access Layer	Concerned with the exchange of data between computer and network

1-42

42

A simple example: A Three -Layer Model (3)



Unique address, identifying the computer

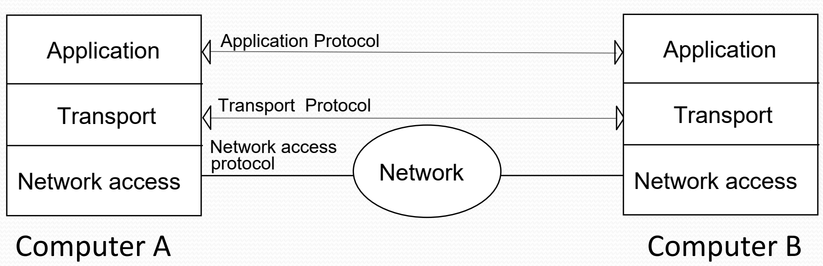
Address, identifying the application:

Service Access Point (SAP)

1-43

43

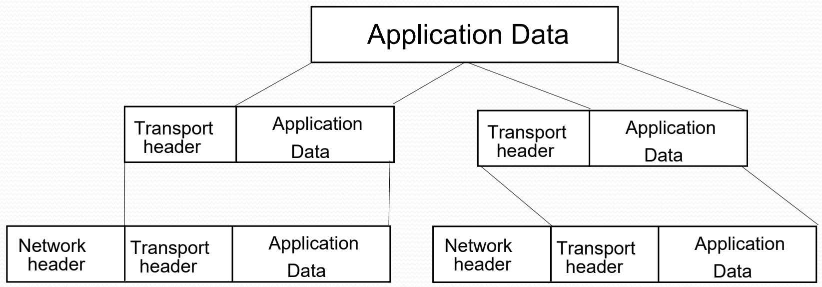
A simple example: A Three -Layer Model (4)



1-44

44

A simple example: A Three -Layer Model (5)

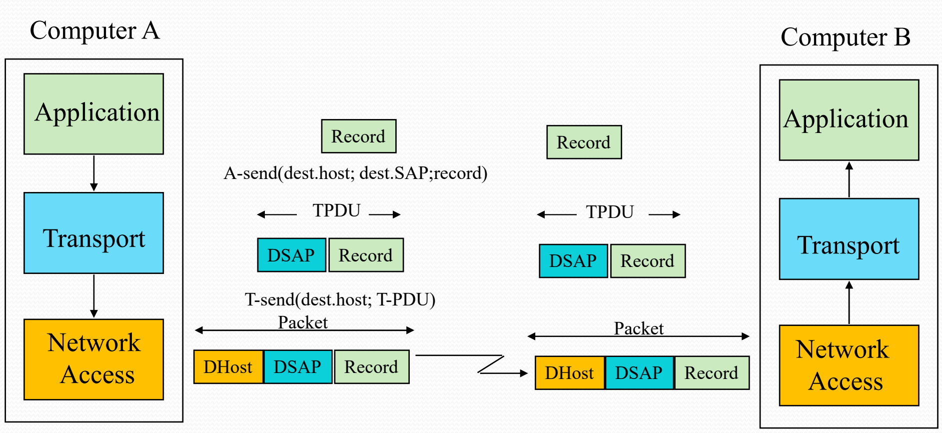


Protocol Data Unit (PDU): Combination of data from the next higher layer and control information

1-45

45

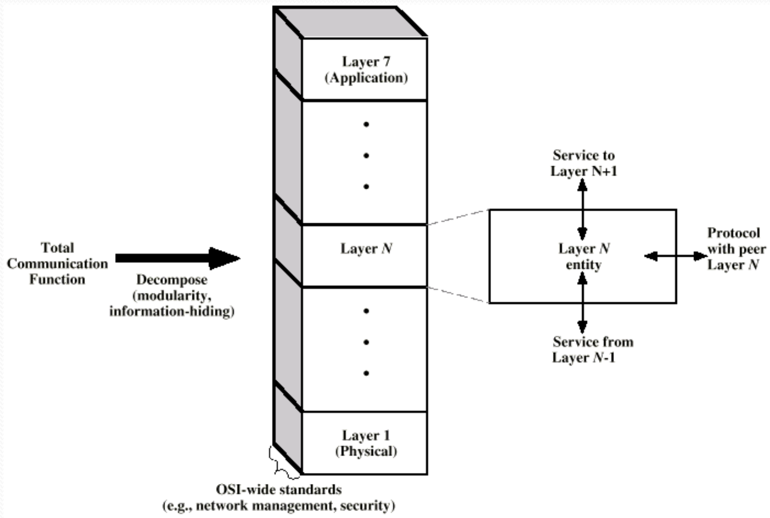
A simple example: A Three -Layer Model (6)



46

46

Standardized Protocol Architectures



1-47

47

Service Primitives and Parameters

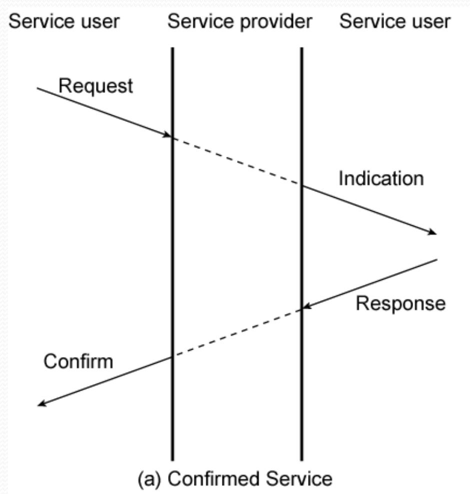
- Define services between adjacent layers using:
  - Primitives to specify the performed function
  - Parameters to pass data and control information

1-48

48

Service Primitives and Parameters

1. Source (N) entity invokes its (N –1) entity with a ***request*** primitive **including needed parameters**, such as the **data to be transmitted and the destination address.**
2. The source (N –1) entity prepares an **(N –1) PDU** to be sent to its peer (N –1) entity.
3. The destination (N –1) entity delivers the data to the appropriate destination (N) entity via an ***indication*** primitive, which includes the data and source address as parameters.
4. If an ack needed, destination (N) entity issues a ***response*** primitive to its (N –1) entity.
5. The (N –1) entity conveys the acknowledgment in an **(N –1) PDU**.
6. The acknowledgment is delivered to the (N) entity as a ***confirm*** primitive.



1-49

49

Generic Protocol Issues

- Error control: making a channel more reliable, and handling lost or out of sequence messages.
- Flow control: avoid flooding a slower peer entity.
- Resource allocation: mediating contention for physical (e.g. buffers) or logical (e.g. data structures) resources
- Fragmentation (Segmentation): dividing chunks of data into smaller pieces, and subsequent reassembly
- Multiplexing: combining several higher layer sessions
- Connection setup: initiating logical communication with peer entity
- Addressing / naming: managing identifiers
- Compression: reducing data rate
- Encryption: provide data security
- Timer management: bookkeeping and error recovery

1-50

50

Relevant Standards Bodies

- ISO: International Organization for Standardization (www.iso.org)
  - An agency of the United Nations.
  - Collaborative standards development for information technology.
  - ISO is not an acronym but a word, derived from the Greek «ίσος» (read as "isos"), meaning equal.
- ITU: International Telecommunications Union (www.itu.int)
  - UN treaty agency that sets telecommunications standards.
  - ITU-T (Telecommunications section)
- ANSI: American National Standards Institute (www.ansi.org)
  - The US national standards body.
  - Coordinates and accredits standards development across the US.
- IEEE; Institute of Electrical & Electronics Engineers (www.ieee.org)
  - US based international professional organization.
  - Among other things, develops standards.
- IETF / IRTF
  - Internet Engineering Task Force (www.ietf.org) / Internet Research Task Force (www.irtf.org)
- EIA: Electronic Industries Alliance (www.eia.org)
  - e.g., standards for wiring and interconnection

51

51

Protocol Architectures

- ISO OSI (Open System Interconnection)
- IBM SNA (System Network Architecture)
- Internet Architecture (TCP/IP Protocol Suite)

1-52

52

Open System Interconnection (OSI) Reference Model

- Developed by the International Organization for Standardization (ISO).
- Has become the standard model for classifying communication functions.
- Has seven layers.
- It is a “theoretical” system delivered too late!
- It has NOT dominated. TCP/IP is the de facto standard.
- Several reasons:
  - TCP/IP appeared earlier
  - Internet “won” the game
  - OSI has a “complex” structure that could result in “heavy processing”

1-53

53

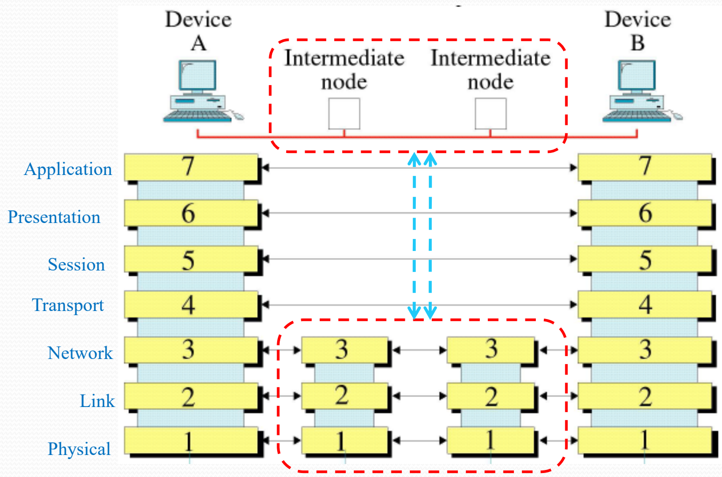
Open System Interconnection (OSI) Reference Model

Application	Access to the users (File transfer, e-mail, r-login, ..
Presentation	Data representation (syntax) (e.g ASCII)
Session	Control structure between applications. Establish/manage connection
Transport	Reliable, transparent transport of data between end-points. End-to-end error recovery and error control
Network	Responsible for establishing, maintaining, terminating connections (routing, addressing, congestion control,….)
Data link	Reliable transfer of information across physical link (sends “frames” of data with proper synchronization., error and flow control)
Physical	How to transmit a signal (access of the transmission medium; Copper, fiber, radio,..). Deals with network hardware, bit encoding)

1-54

54

OSI Reference Model



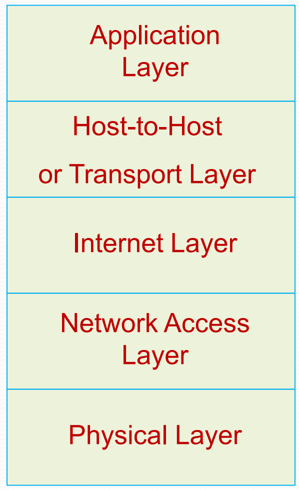
55

TCP/IP Protocol Architecture

- ***No official*** model but a working one.
- Has 5 layers (OSI has 7 layers)
- Funded by DARPA (USA).
- Initially developed as a US military research effort funded by the Department of Defense
- It has dominated.
- It is the “heart” of Internet.

56

TCP/IP Protocol Architecture (2)



1-57

57

Physical Layer

- concerned with physical interface between computer and network
- concerned with issues like:
  - characteristics of transmission medium
  - signal levels
  - data rates
  - other related matters

58

58

Network Access Layer

- exchange of data between an end system and attached network
- concerned with issues like :
  - destination address provision
  - invoking specific services like priority
  - access to & routing data across a network link between two attached systems
- allows layers above to ignore link specifics

59

59

Internet Layer (IP)

- routing functions across multiple networks
- for systems attached to different networks
- using IP protocol
- implemented in end systems and routers
- routers connect two networks and relay data between them

60

60

Host-to-host / Transport Layer

- common layer shared by all applications
- provides reliable delivery of data
- in same order as sent
- commonly uses TCP

61

Application Layer

- Provides support for user applications
- Needs a separate module for each type of application

62

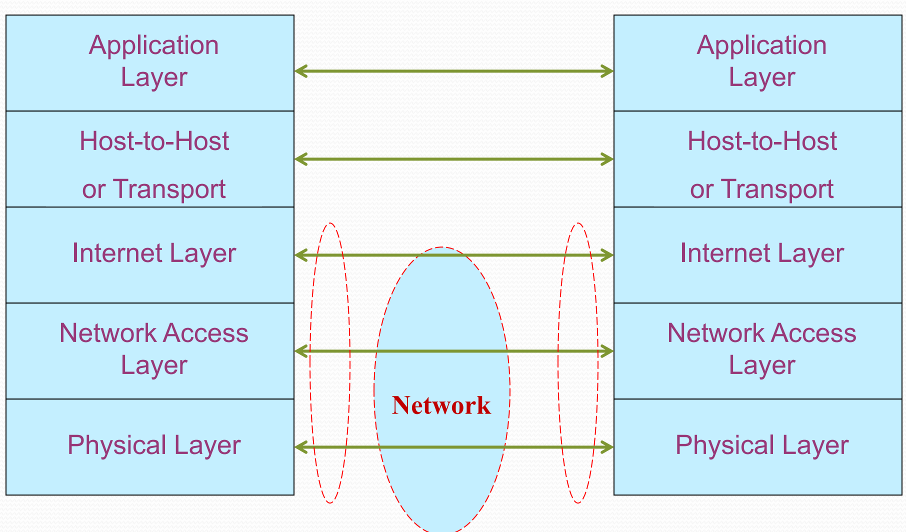
TCP/IP Protocol Architecture

Application Layer	Contains the logic needed to support user applications (ftp, telnet, http etc.) Each application requires different module.
Host-to-Host or Transport	Concerned with the reliability of transmission/reception (error control, sequencing, flow control)
Internet Layer	Provides routing functions across multiple networks. It is implemented in end-systems and routers
Network Access Layer	Concerned with the exchange of data between communicating entities. Depends on network type.
Physical Layer	Covers the physical interface between device (computer and transmission medium or network - medium, signals, data rates..)

1-63

63

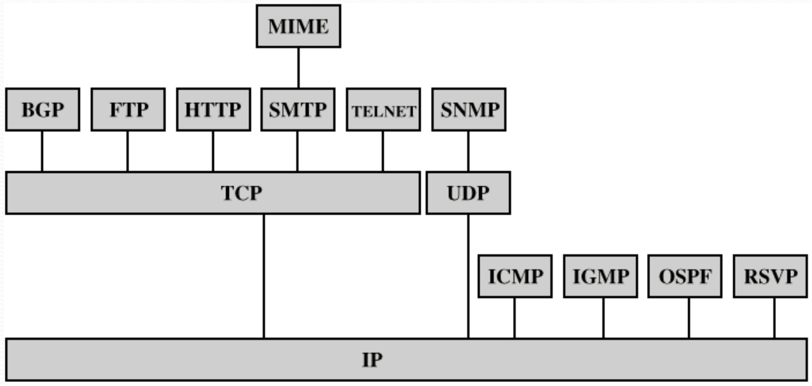
TCP/IP Protocol Architecture



1-64

64

Some TCP/IP Protocols

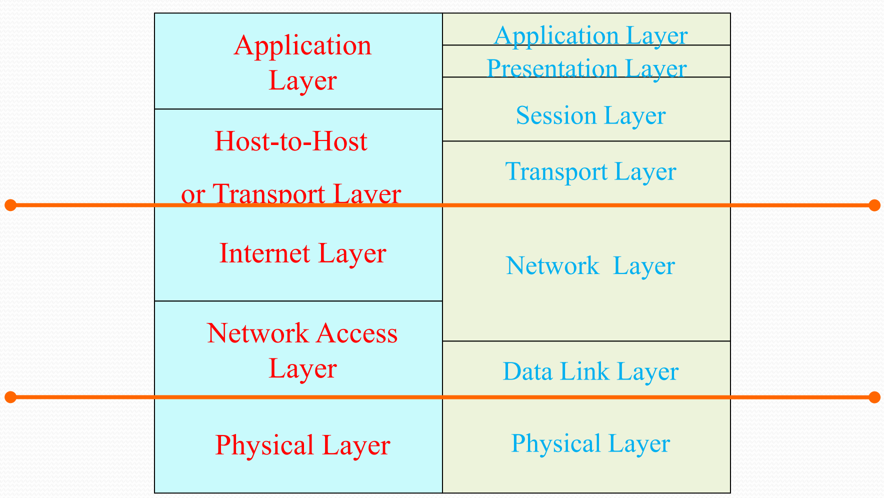


BGP = Border Gateway Protocol
FTP = File Transfer Protocol
HTTP = Hypertext Transfer Protocol
ICMP = Internet Control Message Protocol
IGMP = Internet Group Management Protocol
IP = Internet Protocol
MIME = Multi-Purpose Internet Mail Extension
OSPF = Open Shortest Path First
RSVP = Resource ReSerVation Protocol
SMTP = Simple Mail Transfer Protocol
SNMP = Simple Network Management Protocol
TCP = Transmission Control Protocol
UDP = User Datagram Protocol

1-65

65

TCP/IP versus OSI



1-66

66

OSI Pros and Cons

- Bad timing (too much detailed concept before actual applications)
  - It tries to design the "perfect world", which is either difficult or impractical.
  - Technology and human understanding of how things work (or should work) changes.
- More modular but more processing intensive.
- Provides a good architecture for detailed modeling of processes

1-67

67

IPv4

68

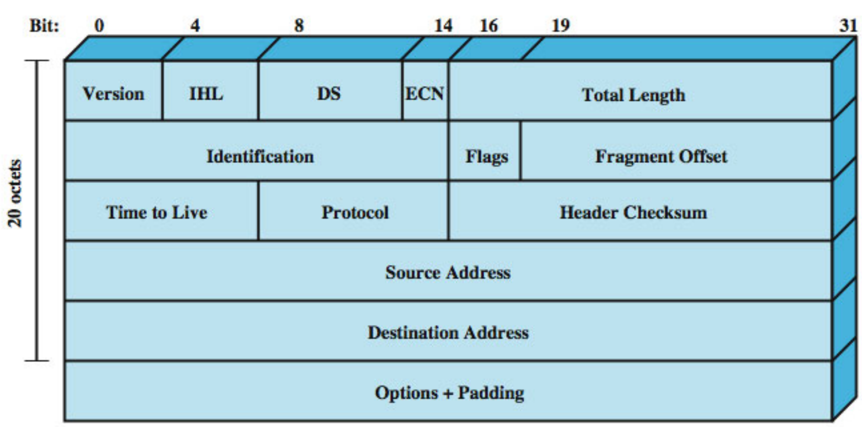
Internet Protocol (IP) v4

- defined in RFC 791
- part of TCP/IP suite
- two parts
  - specification of interface with a higher layer (e.g. TCP)
  - specification of actual protocol format and mechanisms
- is gradually replaced by IPv6

1-69

69

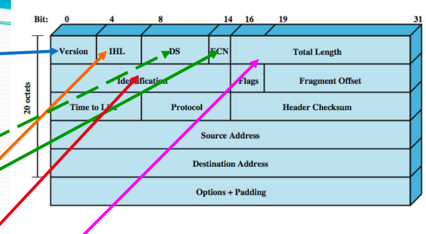
IPv4 Header



1-70

70

Header Fields (1)

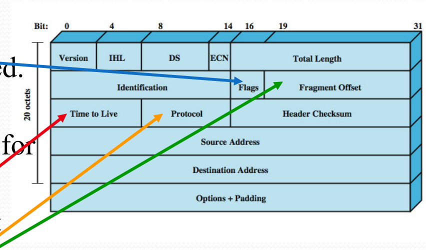


- Version
  - currently IPv4
  - latter IPv6
- Internet Header Length
  - multiple of 32-bit words (including options)
- DS/ECN (was type of service)
- Total length of datagram (in octets)
- Identification
  - sequence number that together with the source address, destination address, and user protocol, identifies a datagram uniquely.

71

71

Header Fields (2)

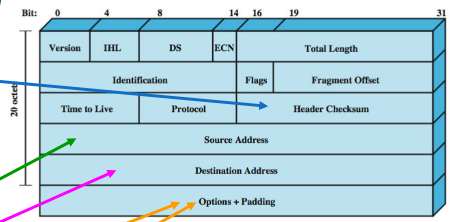


- Flags
  - Only 2 of the bits are currently defined.
  - "More" bit indicates there are more segments of the packet coming (used for fragmentation and reassembly
  - "Don't fragment" bit prohibits packet fragmentation when set.
- Fragmentation offset
  - Indicates where in the original datagram this fragment belongs.
- Time to live
  - Specifies how long a datagram is allowed to remain in the internet.
- Protocol
  - Next higher layer to receive data field at destination (e.g. TCP)

1-72

72

Header Fields (3)



- Header checksum
  - re-verified and recomputed at each router
  - 16 bit ones complement sum of all 16 bit words in header
- Source address
- Destination address
- Options
  - Encodes the options requested by the sending user
- Padding
  - to fill to multiple of 32 bits

1-73

73

IPv6

1-74

74

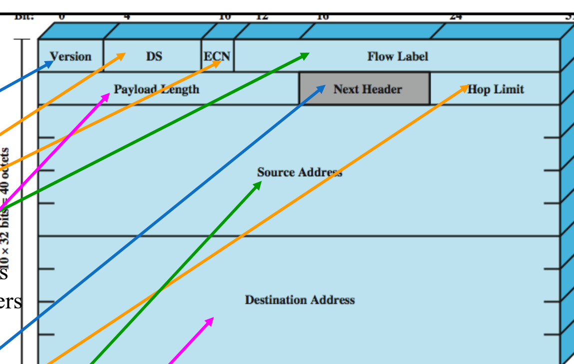
Why Change IP?

- Address space exhaustion
  - two-level addressing (network and host) wastes space
  - network addresses used even if not connected
  - you have to wait for a while, to get more info, in order to understand these two statements
  - growth of networks and the Internet
  - extended use of TCP/IP
  - single address per host
- requirements for new types of service

1-75

75

IPv6 Header



Version (4 bits): IP version number (=6).
DS/ECN (8 bits): As in IPv4.
Flow Label (20 bits): Labels packets that require special handling by routers within a network.

Payload Length (16 bits): Length of remainder of packet following header (extension headers + transport-level PDU).
Next Header (8 bits): Identifies type of header immediately following IPv6 header (either an IPv6 extension header or a higher-layer header (e.g. TCP or UDP).
Hop Limit (8 bits): Remaining number of allowable hops for this packet.
Source Address (128 bits): address of originator of the packet.
Destination Address (128 bits): address of intended recipient of the packet.
IPV6 header:
•longer than the mandatory portion of IPv4 header (40 octets versus 20 octets)
•contains fewer fields (8 versus 12).
•Routers have less processing to do per header (speeds up routing).

1-76

76

END

1-77

77