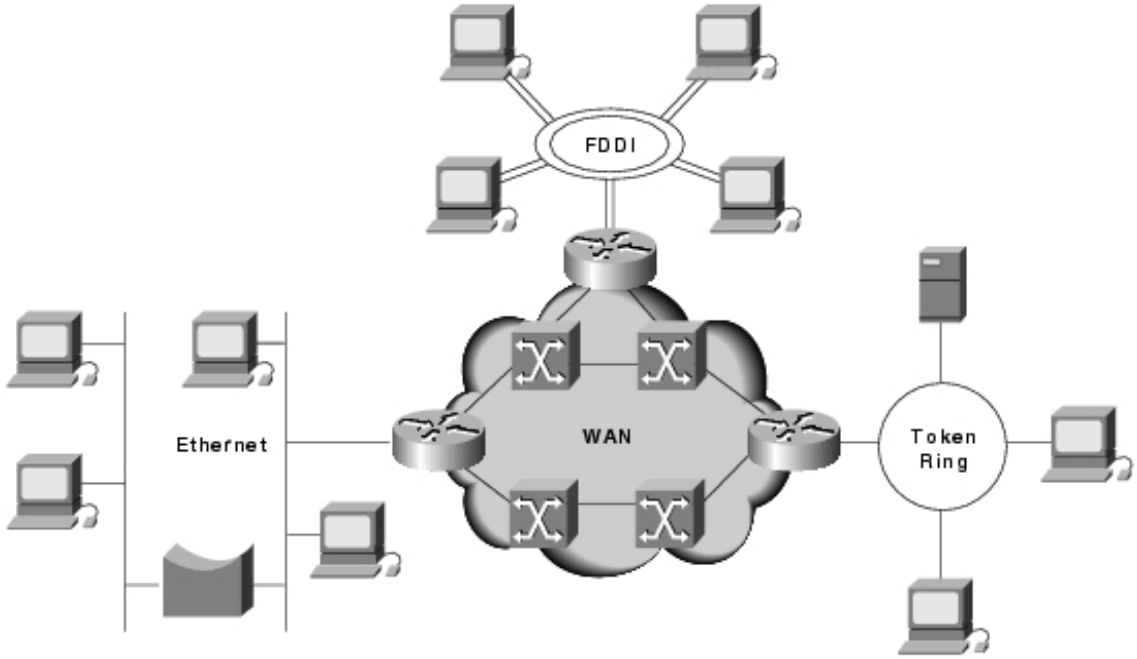
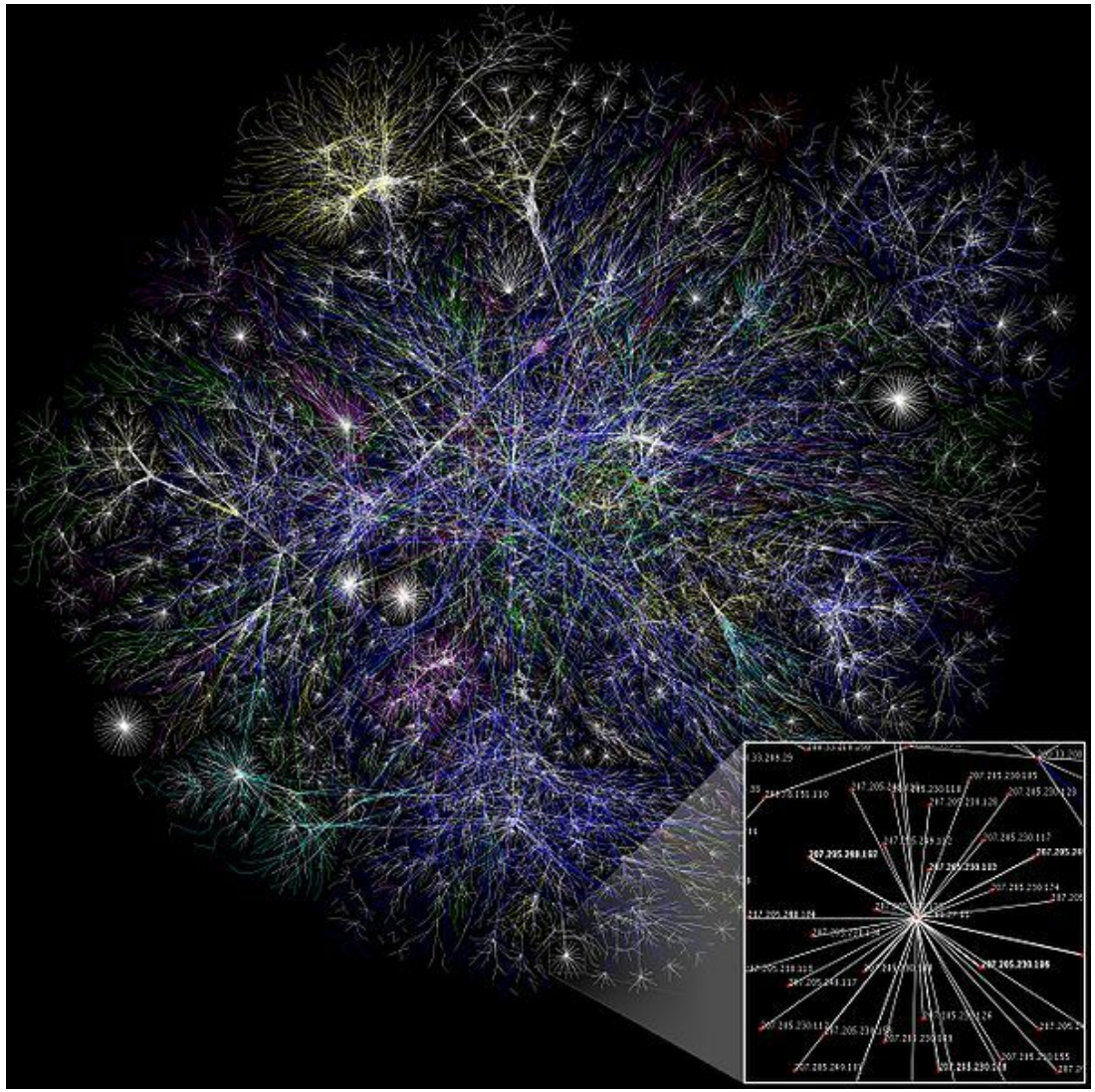
Part A: Technical Review

I. What is the Internet?

- Nobody really owns the Internet.
- An ***Internet*** is a collection of individual networks, connected by intermediate networking devices, that functions as a single large network.
- The Internet Society (a non-profit group) oversees the formation of the policies and protocols that define how we use and interact with the Internet.





Visualization of the Internet

II. Internetworking Challenges

- **Heterogeneity:** Different sites may use different types of media operating at varying speeds, or may even include different types of systems that need to communicate.
- **Reliability:** This is an unpredictable world. So many large internetworks include redundancy to allow for communication even when problems occur.
- **Management:** Network management must provide centralized support and troubleshooting capabilities in an internetwork. Configuration, security, performance, and other issues must be adequately addressed for the internetwork to function smoothly.
- **Flexibility:** Internet must be flexible enough to change with new demands.

III. Open System Interconnection Reference Model

- The OSI reference model is a conceptual model composed of seven layers, each specifying particular network functions.
- The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups.

- A task or group of tasks is then assigned to each of the seven OSI layers. Each layer is reasonably self-contained so that the tasks assigned to each layer can be implemented independently.
- This enables the solutions offered by one layer to be updated without adversely affecting the other layers. The Open System Interconnection (OSI) reference model:
  (1) Layer 7: Application
  (2) Layer 6: Presentation
  (3) Layer 5: Session
  (4) Layer 4: Transport
  (5) Layer 3: Network
  (6) Layer 2: Data link
  (7) Layer 1: Physical

  Note: A handy way to remember the seven layers is the sentence **"All people seem to need data processing."** The beginning letter of each word corresponds to a layer.

IV. Connection-Oriented and Connectionless Network Services

- In general, transport protocols can be characterized as being either connection-oriented or connectionless.

- Connection-oriented services must first establish a connection with the desired service before passing any data.
- A connectionless service can send the data without any need to establish a connection first.
- In general, connection-oriented services provide some level of delivery guarantee, whereas connectionless services do not.
- Connection-oriented service involves three phases: connection establishment, data transfer, and connection termination.
- Connection-oriented services must negotiate a connection, transfer data, and tear down the connection, whereas a connectionless transfer can simply send the data without the added overhead of creating and tearing down a connection.

V. Mapping Addresses between IP and MAC

- When the network layer has determined the destination station's network address, it must forward the information over a physical network using a MAC address (e.g., 00:A2:C8:16:C7:19). (*Problem: How to find a MAC address?*)
- Different protocol suites use different methods to perform this mapping, but the most popular is Address Resolution Protocol (ARP).

- Address Resolution Protocol (ARP) maps network addresses to MAC addresses. The Hello protocol enables network devices to learn the MAC addresses of other network devices. MAC addresses are embedded in the network cards.

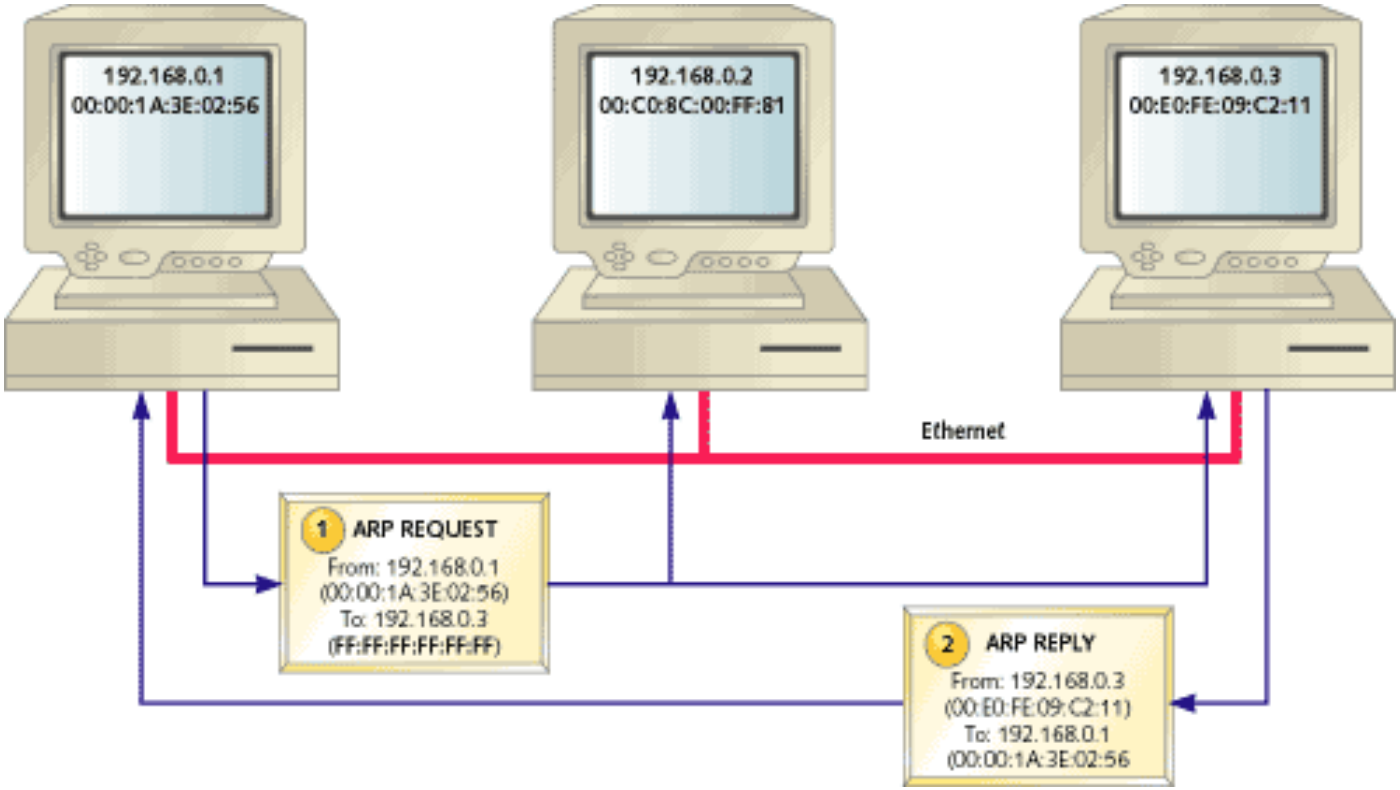
  Hello Protocol:

  (1) The Hello protocol is a network layer protocol that enables network devices to identify one another and indicate that they are still functional.
  (2) When a new end system powers up, for example, it broadcasts hello messages onto the network. Devices on the network then return hello replies.
  (3) Hello messages are also sent at specific intervals to indicate that they are still functional.
  (4) Network devices can learn the MAC addresses of other devices by examining Hello protocol packets.

  Local Network:

  (1) When a network device needs to send data to another device **on the same network,** it knows the destination IP address for the data transfer.
  (2) First, the sending station will check its ARP table to see if it has already discovered this destination station's MAC address.

(3) If it has not, it will send a broadcast on the network with the destination station's IP address contained in the broadcast.
(4) Every station on the network receives the broadcast and compares the embedded IP address to its own.
(5) Only the station with the matching IP address replies to the sending station with a packet containing the MAC address for the station.
(6) The sending station then adds this information to its ARP table for future reference and proceeds to transfer the data.



Remote Network:

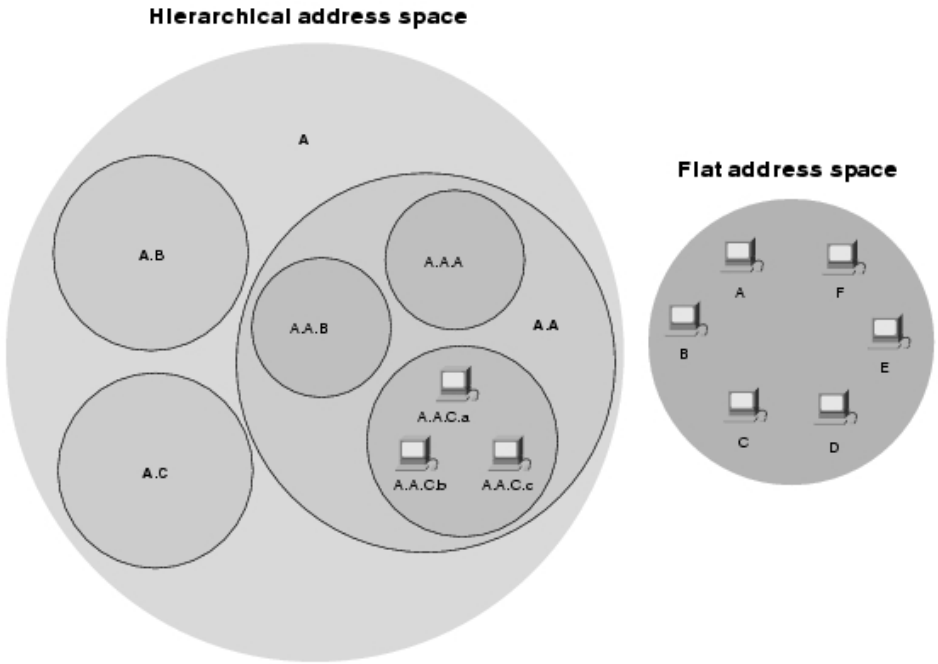
(1) When the destination device lies on a remote network, the default gateway will then forward the information over whatever networks necessary to deliver the packet to the network on which the destination device resides.

(2) When the default gateway of the remote network receives the packets, it then forwards the packets to that device.

(3) The process is the same as that of local network except that the default gateway replaces the sending station's position.

VI. Network Layer Addresses

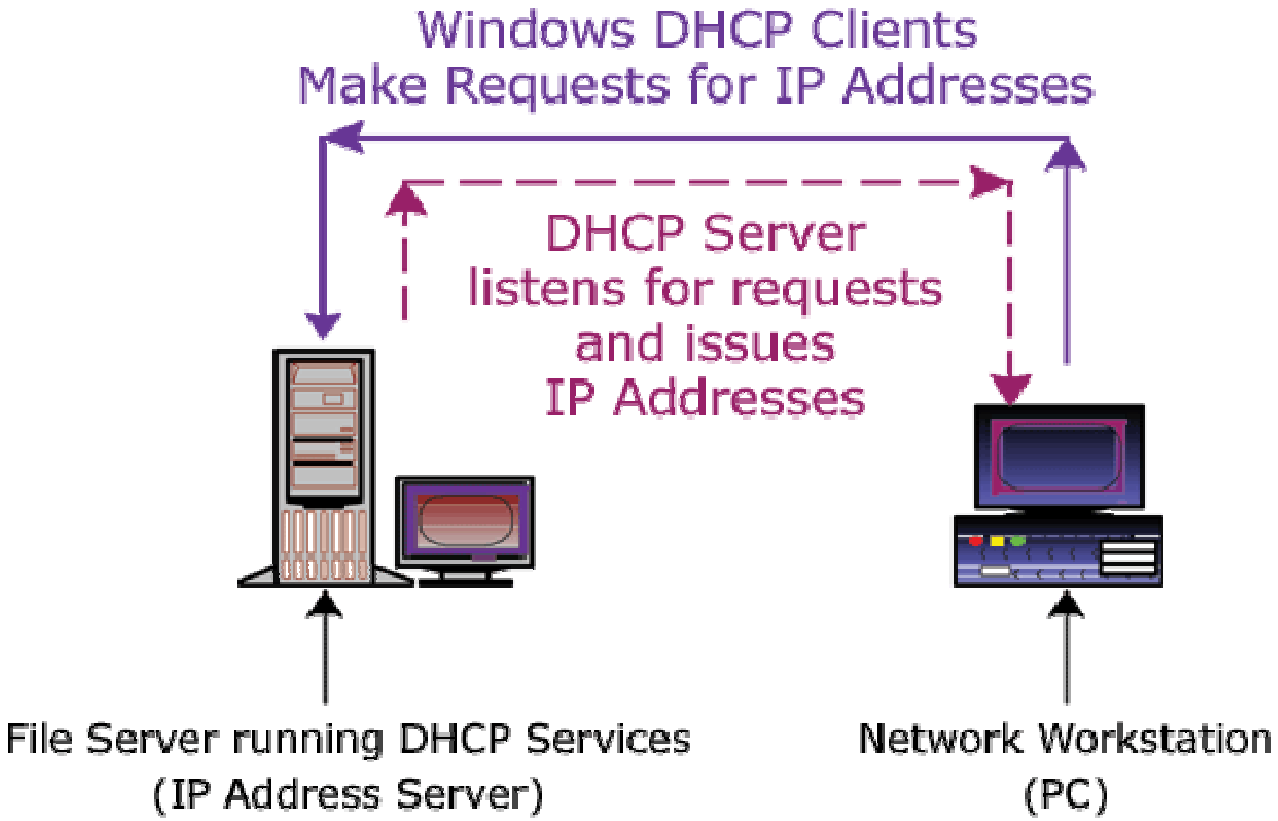
- Network addresses (e.g., IP addresses) usually exist within a hierarchical address space and sometimes are called virtual or logical addresses.
- A hierarchical address space is organized into numerous subgroups, each successively narrowing an address until it points to a single device.
- In contrast, a flat address space is organized into a single group (in a manner similar to Student ID numbers).
- The following figure illustrates the difference between hierarchical and flat address spaces.



(a) Address Assignments

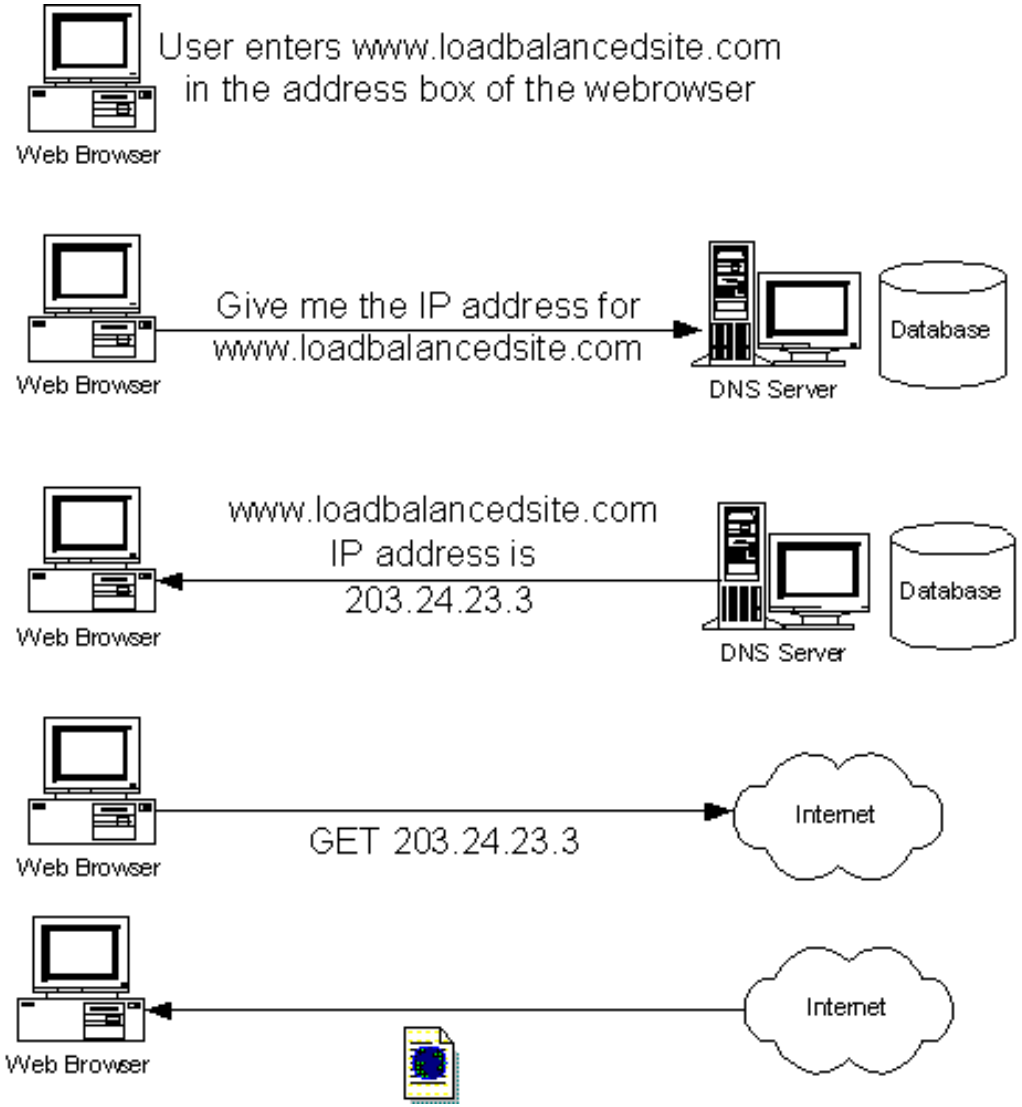
- Addresses are assigned to devices as one of two types: static and dynamic.
- Static addresses are assigned by a network administrator according to a preconceived internetwork addressing plan.
- Dynamic addresses are obtained by devices when they attach to a network, by means of some protocol-specific process.
  - ❖ A device using a dynamic address often has a different address each time that it connects to the network.

❖Some networks use a server to assign addresses. Server-assigned addresses are recycled for reuse as devices disconnect.



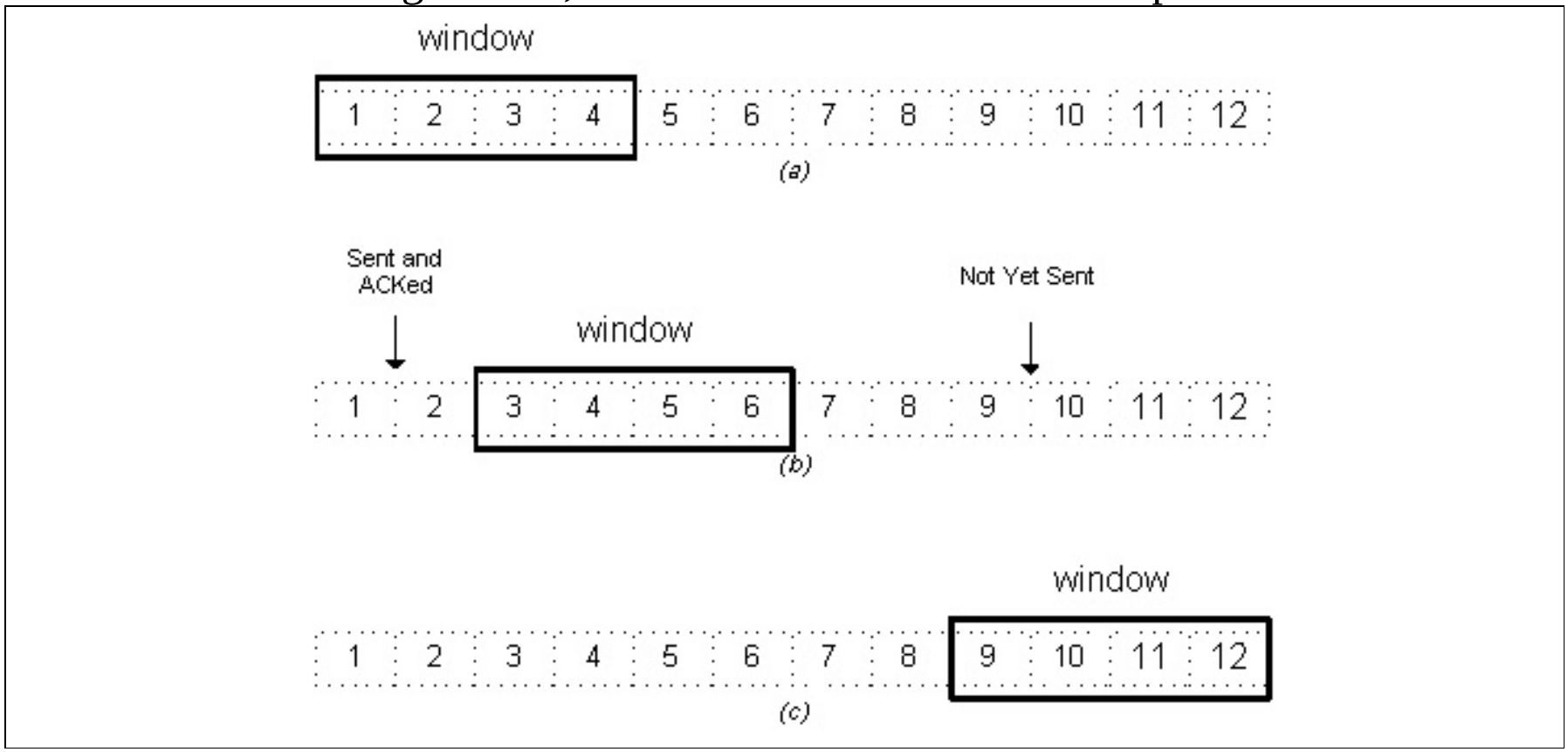
(b) Addresses Versus Names

- Internetwork devices usually have both a name (e.g., domain name) and an address (IP address) associated with them.
- Domain names typically are location-independent and remain associated with a device wherever that device moves.
- IP addresses usually are location-dependent and change when a device is moved (say, from one network to another network).
- Domain names are usually mapped to IP addresses through some protocol. The Internet uses Domain Name System (DNS) to map the name of a device to its IP address. For example, it's easier for you to remember www.cisco.com instead of some IP address.


User enters www.loadbalancedsite.com
in the address box of the webrowser
Web Browser
Give me the IP address for
www.loadbalancedsite.com
Web Browser
DNS Server
Database
www.loadbalancedsite.com
IP address is
203.24.23.3
Web Browser
DNS Server
Database
GET 203.24.23.3
Web Browser
Internet
Web Browser
Internet

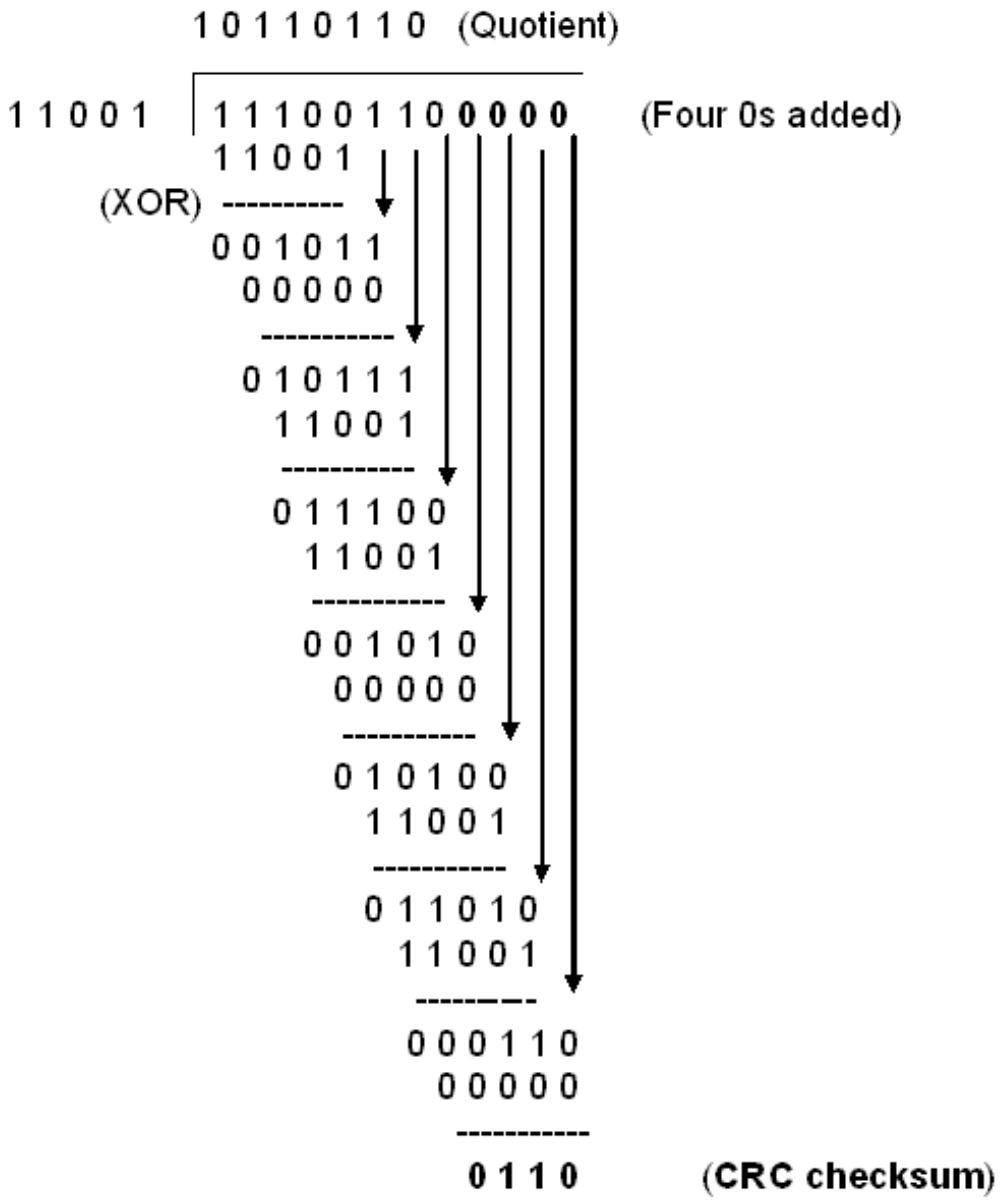
VII. Flow Control Basics

- **Sliding Window** is a flow-control scheme in which the source device requires an acknowledgment from the destination after a certain number of packets have been transmitted.
- If the destination does not receive one or more of the packets for some reason, such as overflowing buffers, the source then retransmits the packets.



VIII. Error-Checking Basics

- One common error-checking scheme is the cyclic redundancy check (CRC), which detects and discards corrupted data.
- First, the source device performs a predetermined set of calculations over the contents of the packet to be sent.
- Then, the source places the calculated value in the packet and sends the packet to the destination.
- The destination performs the same predetermined set of calculations over the contents of the packet and then compares its computed value with that contained in the packet.
- If the values are equal, the packet is considered valid. If the values are unequal, the packet contains errors and is discarded.


1 0 1 1 0 1 1 0 (Quotient)
1 1 0 0 1
1 1 1 0 0 1 1 0 0 0 0 (Four 0s added)
1 1 0 0 1
(XOR)
0 0 1 0 1 1
0 0 0 0 0
0 1 0 1 1 1
1 1 0 0 1
0 1 1 1 0 0
1 1 0 0 1
0 0 1 0 1 0
0 0 0 0 0
0 1 0 1 0 0
1 1 0 0 1
0 1 1 0 1 0
1 1 0 0 1
0 0 0 1 1 0
0 0 0 0 0
0 1 1 0 (CRC checksum)

IX. Multiplexing Basics

- ***Multiplexing*** is a process in which multiple data channels are combined into a single data or physical channel at the source. Conversely, ***de-multiplexing*** is the process of separating multiplexed data channels at the destination.
- The common methods used for multiplexing data are time-division multiplexing (TDM), frequency-division multiplexing (FDM).

X. Standards Organizations

- Some of the best-known standards organizations that contribute to internetworking standards include these:
  (1) **International Organization for Standardization (ISO)**: ISO is an international standards organization responsible for a wide range of standards, including many that are relevant to networking.
  (2) **American National Standards Institute (ANSI)**: ANSI, which is also a member of the ISO, is the coordinating body for voluntary standards groups within the United States.
  (3) **Institute of Electrical and Electronic Engineers (IEEE)**: IEEE is a professional organization that defines networking and other standards (e.g., IEEE 802.3 and IEEE 802.5).

(4) **International Telecommunication Union Telecommunication Standardization Sector (ITU-T)**: Formerly called the Committee for International Telegraph and Telephone (CCITT), ITU-T is now an international organization that develops communication standards.