CS 480: MOBILE NETWORKS

Lecture PowerPoints

NETWORKING AND INTERNETWORKING

Topics Covered

- Circuit switching
- Packet switching
- OSI and TCP/IP models
- Wide area networks
- Local area networks
- Routing protocols
- Error Control

Learning Outcomes

- Understand how the internet works
- Understand TCP/IP and 7 layer model
- Understand the use of internetworking devices

Circuit Switching

- In a circuit-switching network, a dedicated communications path is established between two stations through the nodes of the network.
- That path is a connected sequence of physical links between nodes.
- On each link, a logical channel is dedicated to the connection.
- Data generated by the source station are transmitted along the dedicated path as rapidly as possible.
- At each node, incoming data are routed or switched to the appropriate outgoing channel without delay.
- The most common example of circuit switching is the telephone network.

Packet Switching

- A quite different approach is used in a packet-switching network.
- Data are sent out in a sequence of small chunks, called packets.
- Each packet is passed through the network from node to node along some path leading from source to destination.
- At each node, the entire packet is received, stored briefly, and then transmitted to the next node.
- Packet-switching networks are commonly used for terminal-to-computer and computer-to-computer communications.

Frame Relay

- Packet switching was developed at a time when digital long distance transmission facilities exhibited a relatively high error rate compared to today's facilities.
- There is a considerable amount of overhead built into packet-switching schemes to compensate for errors.
- With modern high-speed telecommunications systems, this overhead is unnecessary and counterproductive.
  - because the rate of errors has been dramatically lower
- Frame relay was developed to take advantage of these high data rates and low error rates.
- Frame relay networks have high data rates
  - The idea is to strip out most of the overhead involved with error control.

Asynchronous Transfer Mode (ATM) (1)

- ATM, sometimes referred to as cell relay, is a culmination of developments in circuit switching and packet switching.
- ATM can be viewed as an evolution from frame relay.
- The obvious difference between frame relay and ATM is
  - that frame relay uses variable-length packets, called frames, and ATM uses fixed-length packets, called cells.
- As with frame relay, ATM provides little overhead for error control,
  - depending on the reliability of the transmission system and on higher layers of logic in end systems to catch and correct errors.
- By using a fixed packet length, the processing overhead is reduced even further for ATM compared to frame relay

Asynchronous Transfer Mode (2)

- ATM can also be viewed as an evolution from circuit switching.
- With circuit switching, only fixed-data-rate circuits are available to the end system.
- ATM allows the definition of multiple virtual channels with data rates that are dynamically defined at the time the virtual channel is created.
- By using small, fixed-size cells, ATM is so efficient that it can offer a constant-data-rate channel even though it is using a packet-switching technique.
- Thus ATM extends circuit switching to allow multiple channels with the data rate on each channel dynamically set on demand.

Wide Area Networks (WANs) (1)

- WANs generally cover a large geographical area, require the crossing of public right-of-ways, and rely at least in part on circuits provided by a common carrier.
- Typically, a WAN consists of a number of interconnected switching nodes.
- A transmission from any device is routed through these internal nodes to the specified destination device.
- These nodes (including the boundary nodes) are not concerned with the content of the data;
  - their purpose is to provide a switching facility that will move the data from node to node until they reach their destination.

Wide Area Networks (WANs) (2)

- Traditionally, WANs have been implemented using one of two technologies: circuit switching and packet switching.
- More recently, frame relay and ATM networks have assumed major roles.

Local Area Networks (LANs) (1)

- As with WANs, a LAN is a communications network that interconnects a variety of devices and provides a means for information exchange among those devices.
- There are several distinctions between LANs and WANs:
  - The scope of the LAN is small, typically a single building or a cluster of buildings. This difference in geographic scope leads to different technical solutions.
  - The LAN is usually owned by the same organization that owns the attached devices.
  - For WANs, this is less often the case, or at least a significant fraction of the network assets is not owned.
  - The internal data rates of LANs are typically much greater than those of WANs.

Local Area Networks (LANs) (2)

- LANs come in a number of different configurations.
- Common ones are switched LANs and wireless LANs
- Most common switched LAN is a switched Ethernet LAN,
  - which may consist of a single switch with a number of attached devices, or a number of interconnected switches.
- Two other prominent examples are ATM LANs,
  - which use an ATM network in a local area, and Fibre Channel.
- Wireless LANs use a variety of wireless transmission technologies and organizations.

The TCP/IP Protocol Architecture

- The TCP/IP protocol architecture is a result of protocol research and development conducted on the experimental packet-switched network, ARPANET.
- This research was funded by the Defense Advanced Research Projects Agency (DARPA), and is generally referred to as the TCP/IP protocol suite.
- This protocol suite consists of a large collection of protocols that have been issued as Internet standards by the Internet Activities Board (IAB)

The TCP/IP Layers (1)

- In general, communications involve three agents:
  - applications, computers, and networks.
- Examples of applications include file transfer and electronic mail.
- We are interested in distributed applications that involve exchange of data between two computer systems
- These applications, and others, execute on computers that can often support multiple simultaneous applications
- Computers are connected to networks, and the data to be exchanged are transferred by the network from one computer to another.

The TCP/IP Layers (2)

- Thus, the transfer of data from one application to another involves first getting the data from the computer in which the application resides and then getting the data to the intended application within the computer.
- With these concepts in mind, we can organize the communication task into 5 relatively independent layers
  - Physical layer
  - Network access layer
  - Internet layer
  - Host-to-host, or transport layer
  - Application layer

Physical Layer

- This layer covers the physical interface between a data transmission device (e.g., workstation, computer) and a transmission medium or network.
- This layer is concerned with specifying characteristics of the transmission medium, the nature of the signals, the data rate, and related matters.

Network Access Layer

- This layer is concerned with exchange of data between an end system (server, workstation, etc.) and the network to which it is attached.
- The sending computer must provide the network with the address of the destination computer, so that the network may route the data to the appropriate destination.
  - The sending computer may wish to invoke certain services, such as priority, that might be provided by the network.
- The specific software used at this layer depends on the type of network to be used;
  - different standards have been developed for circuit switching, packet switching (e.g., frame relay), LANs (e.g., Ethernet)
- The layers above the network access layer, need not be concerned about the specifics of the network to be used.

Internet Layer

- The network access layer is concerned with access to and routing data across a network for two end systems attached to the same network.
- In those cases where two devices are attached to different networks, procedures are needed to allow data to traverse multiple interconnected networks.
- This is the function of the internet layer.
- The Internet Protocol (IP) is used at this layer to provide the routing function across multiple networks.
- This protocol is implemented in end systems and routers

Transport Layer

- Regardless of the nature of the applications that are exchanging data, there is usually a requirement that data be exchanged reliably.
  - i.e., that all of the data arrive at the destination application and that the data arrive in the same order in which they were sent.
- The mechanisms for providing reliability are essentially independent of the nature of the applications.
- Thus all those mechanisms are collected in a common layer shared by all applications;
- This is called the host-to-host layer, or transport layer.
- The Transmission Control Protocol (TCP) is the most commonly used protocol to provide this functionality.

Application Layer

- Finally, the application layer contains the logic needed to support the various user applications.
- For each different type of application, such as file transfer, a separate module is needed that is peculiar to that application.

TCP and UDP (1)

- For most applications running as part of the TCP/IP protocol architecture, the transport layer protocol is TCP.
- TCP provides a reliable connection for the transfer of data between applications.
- A connection is simply a temporary logical association between two entities in different systems.
- A logical connection refers to a given pair of port values.
- For the duration of the connection each entity keeps track of TCP segments coming and going to the other entity, in order to regulate the flow of segments and to recover from lost or damaged segments.
- Figure 1(a) shows the header format for TCP, which is a minimum of 20 octets, or 160 bits.

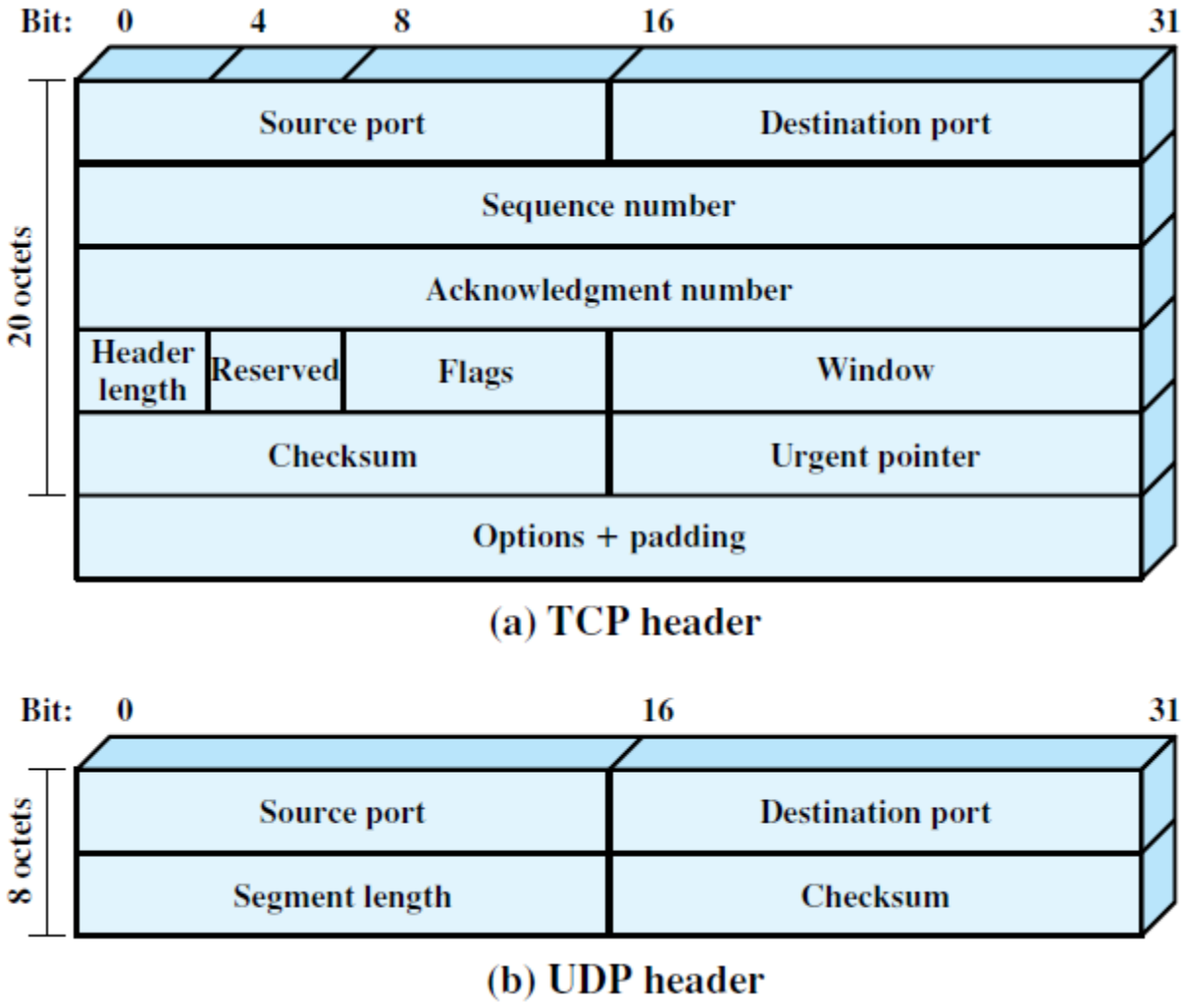


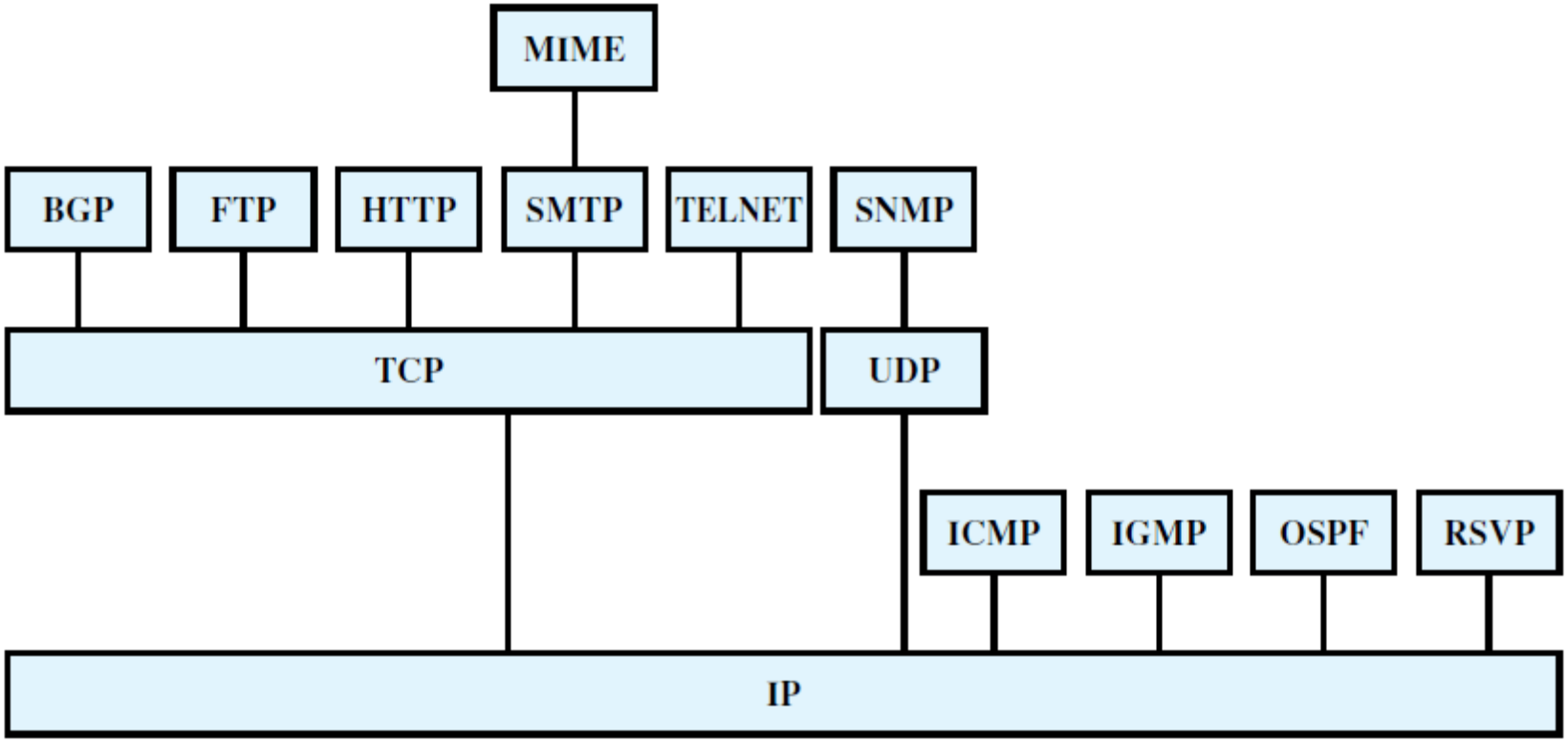
Figure 1: TCP and UDP Headers

TCP and UDP (2)

- The User Datagram Protocol (UDP) is another transport-level protocol that is in common use as part of the TCP/IP protocol suite:
- UDP does not guarantee delivery, preservation of sequence, or protection against duplication.
- Some transaction-oriented applications use UDP;
  - one example is SNMP, the standard network management protocol for TCP/IP networks.
- Because it is connectionless, UDP has very little to do.
- Essentially, it adds a port addressing capability to IP.
- This is best seen by examining the UDP header, shown in Figure 1 (b).

TCP/IP Applications

- A number of applications have been standardized to operate on top of TCP.
- The three most common are
  - The Simple Mail Transfer Protocol (SMTP)
  - The File Transfer Protocol (FTP)
  - TELNET
- Figure 2 shows some protocols in the TCP/IP protocol suite



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 = Multipurpose 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

Figure 2: Some Protocols in the TCP/IP Protocol Suite

THE OSI Model (1)

- The Open Systems Interconnection (OSI) reference model was developed by the International Organization for Standardization (ISO)
  - as a model for a computer protocol architecture and as a framework for developing protocol standards.

The OSI model consists of seven layers:

- Application
- Presentation
- Session
- Transport
- Network
- Data link
- Physical

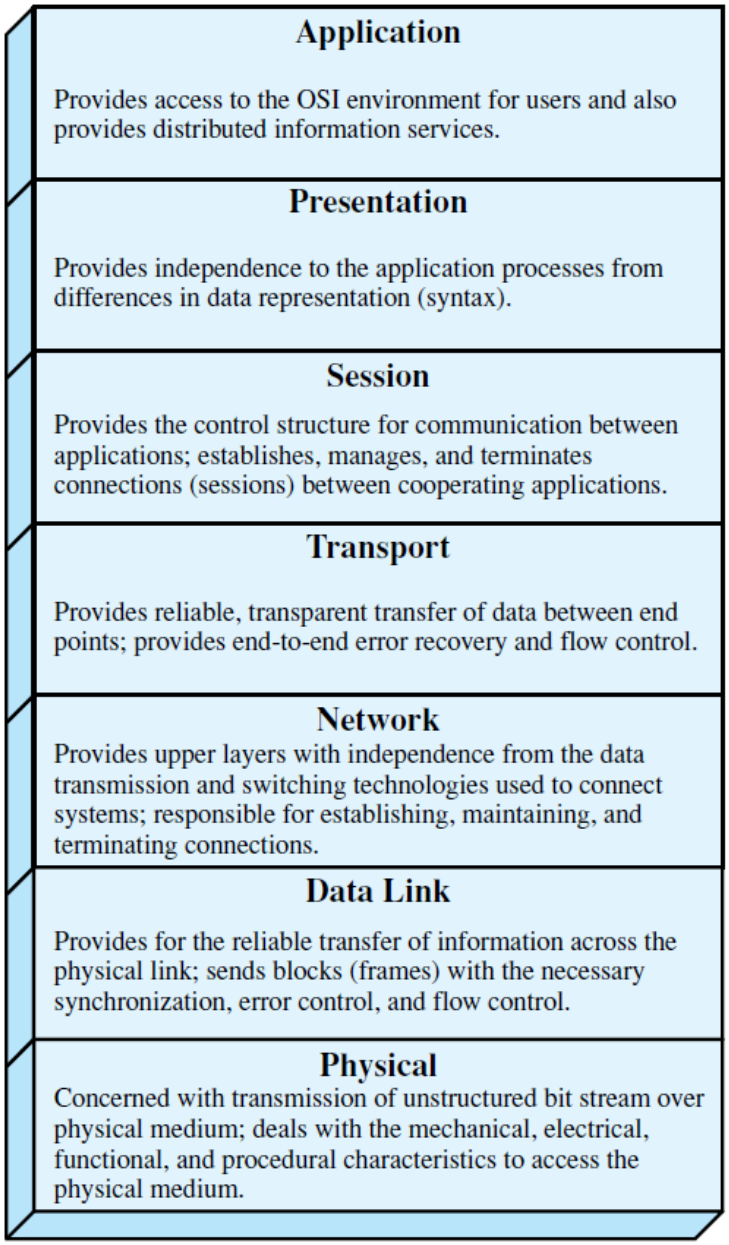


Figure 3: The OSI Layers

THE OSI Model (2)

- Figure 3 illustrates the OSI model and provides a brief definition of the functions performed at each layer.
- The designers of OSI assumed that this model and the protocols developed within this model would come to dominate computer communications,
  - eventually replacing proprietary protocol implementations and rival multivendor models such as TCP/IP.
- But this has not happened.
- Although many useful protocols have been developed in the context of OSI, the overall seven-layer model has not flourished.
- Instead, the TCP/IP architecture has come to dominate.

THE OSI Model (3)

- There are a number of reasons for this outcome.
- The key TCP/IP protocols were mature and well tested at a time when similar OSI protocols were in the development stage.
- TCP/IP achieved the need for interoperability across networks
- The OSI model is unnecessarily complex, with seven layers to accomplish what TCP/IP does with fewer layers.
- Figure 4 illustrates the layers of the TCP/IP and OSI architectures, showing roughly the correspondence in functionality between the two.

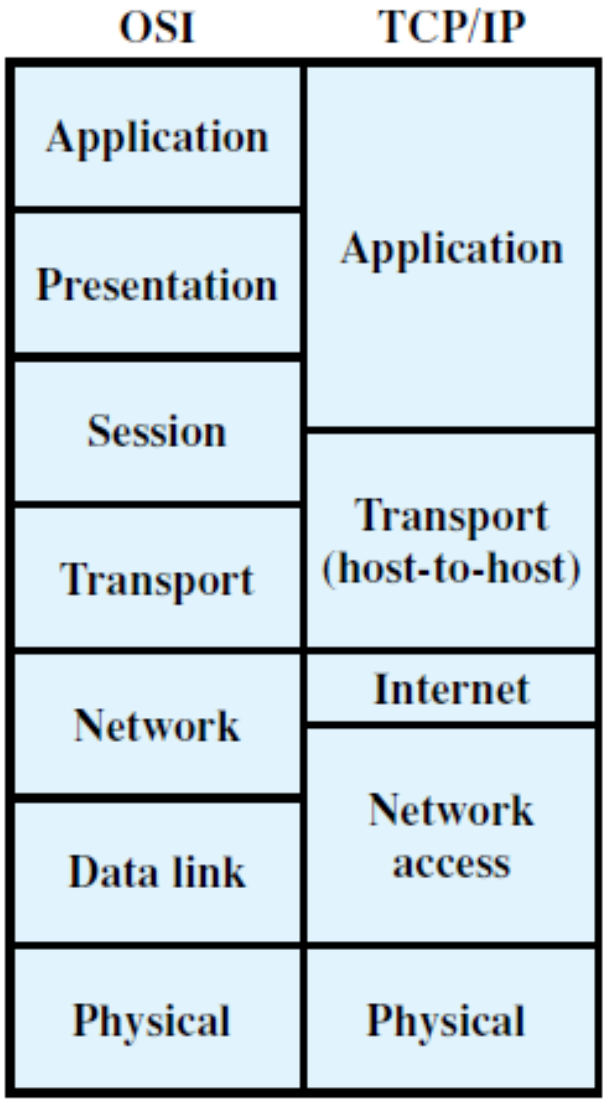


Figure 4: A Comparison of the OSI and TCP/IP Protocol Architectures

Routing Protocols

- Introduction to Routing Protocols
- Autonomous Systems
- Approaches to Routing
- Border Gateway Protocol
- Open Shortest Path First (OSPF) Protocol

Introduction to Routing Protocols (1)

- Routers in an internet receive and forward packets
  - through the interconnected set of networks.
- A router makes routing decision based on knowledge of the topology and traffic/delay conditions of the internet.
- In a simple internet, a fixed routing scheme is possible.
- In more complex internets, a degree of dynamic cooperation is needed among the routers.
  - The router must avoid portions of the network that have failed and should avoid portions of the network that are congested.

Introduction to Routing Protocols (2)

- To make dynamic routing decisions, routers exchange routing information using a chosen routing protocol
- Information is needed about the status of the internet,
  - in terms of which networks can be reached by which routes, and the delay characteristics of various routes.
- In considering the routing function, it is important to distinguish two concepts:
  - Routing information: Information about the topology and delays of the internet
  - Routing algorithm: The algorithm used to make a routing decision for a particular datagram, based on current routing information

Autonomous Systems

- To discuss routing protocols, we need to introduce the concept of an autonomous system.
- An autonomous system (AS) exhibits the following characteristics:
  1. An AS is a set of routers and networks managed by a single organization.
  2. An AS consists of a group of routers exchanging information via a common routing protocol.
  3. Except in times of failure, an AS is connected (in a graph-theoretic sense); that is, there is a path between any pair of nodes.

Interior Router Protocol (IRP)

- IRP is a shared routing protocol that passes routing information between routers within an AS.
- The protocol used within the AS does not need to be implemented outside of the system.
- This flexibility allows IRPs to be custom tailored to specific applications and requirements.

Exterior Router Protocol (ERP)

- An internet may be constructed of more than one AS.
  - For example, all of the LANs at a site, such as an office complex or campus, could be linked by routers to form an AS.
- The system might be linked through a WAN to other ASs
- The situation is illustrated in Figure 5.
- In this case, the routing algorithms and information in routing tables used by routers in different ASs may differ.
- Routers in one AS need little information regarding networks outside the system that can be reached
- ERP is a protocol used to pass routing information between routers in different ASs

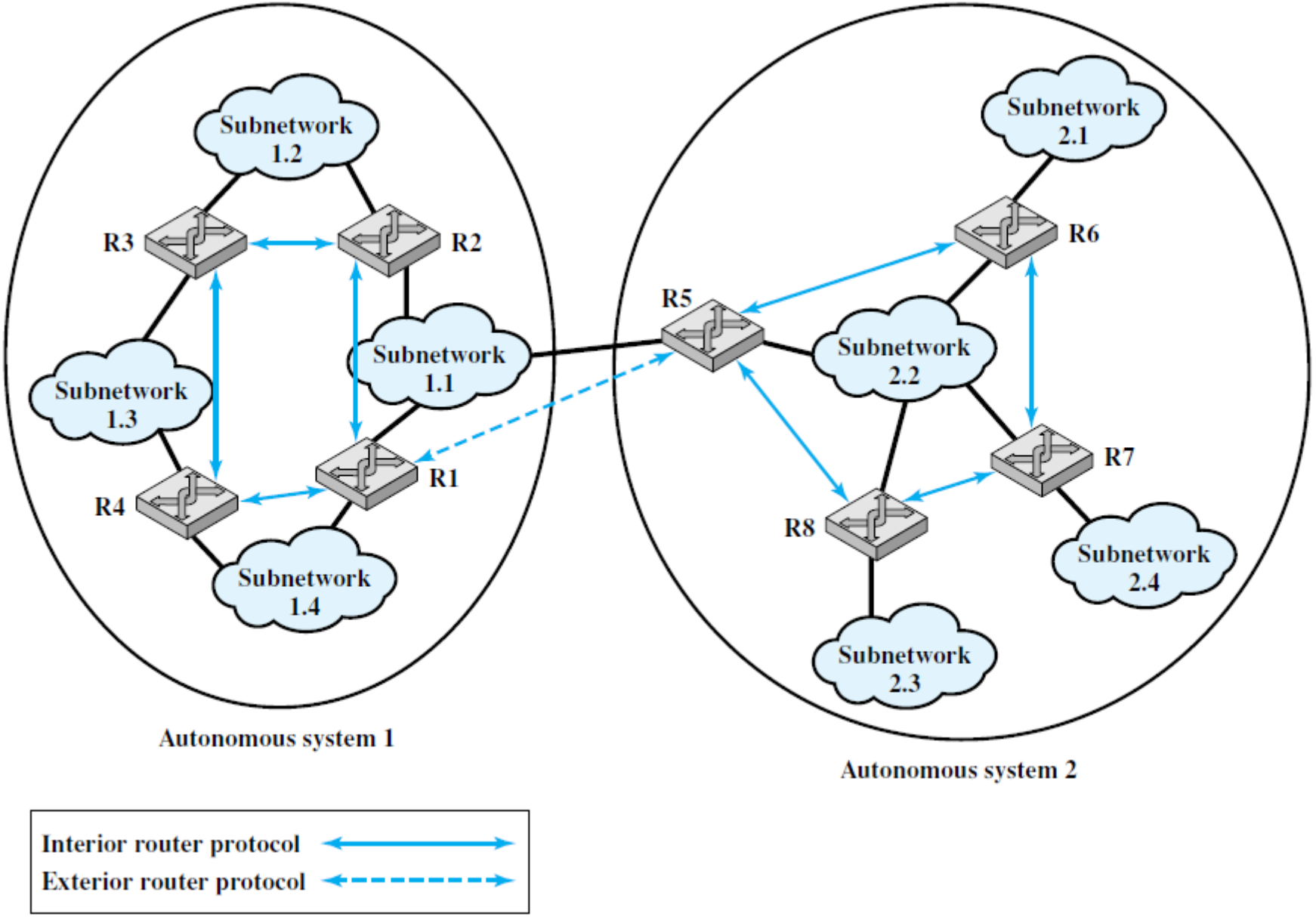


Figure 5: Application of Exterior and Interior Routing Protocols

Approaches to Routing

- Internet routing protocols employ one of three approaches to gathering and using routing information:
  - distance-vector routing
  - link-state routing
  - path-vector routing.

Distance-vector routing (1)

- Distance-vector routing requires that each node exchange information with its neighboring nodes.
- Two nodes are said to be neighbors if they are both directly connected to the same network.
- For this purpose, each node maintains a vector of link costs for each directly attached network and distance and next-hop vectors for each destination.
- The relatively simple Routing Information Protocol (RIP) uses this approach.

Distance-vector routing (2)

- Distance-vector routing requires the transmission of a considerable amount of information by each router.
- Each router sends a distance vector to all its neighbors
  - and that vector contains the estimated path cost to all networks in the configuration.
- When there is a significant change in a link cost or when a link is unavailable,
  - it may take a considerable amount of time for this information to propagate through the internet.

Link-state routing (1)

- Link-state routing is designed to overcome the drawbacks of distance-vector routing.
- When a router is initialized, it determines the link cost on each of its network interfaces.
- The router then advertises this set of link costs to all other routers in the internet topology, not just neighboring routers.
- From then on, the router monitors its link costs.
- Whenever there is a significant change
  - the router again advertises its set of link costs to all other routers in the configuration.

Link-state routing (2)

- Because each router receives the link costs of all routers in the configuration,
  - each router can construct the topology of the entire configuration and then calculate the shortest path to each destination network.
- Having done this, the router can construct its routing table, listing the first hop to each destination.
- The router can use any routing algorithm to determine the shortest paths.
- The Open Shortest Path First (OSPF) protocol is an example of a routing protocol that uses link-state routing.

Path-vector routing

- Path-vector routing simply provide information about which networks can be reached by a given router and the ASs that must be crossed to get there.
- The approach differs from a distance-vector algorithm in two respects:
  - First, the path-vector approach does not include a distance or cost estimate.
  - Second, each block of routing information lists all of the ASs visited in order to reach the destination network by this route.
- Because a path vector lists the ASs that a datagram must traverse if it follows this route, the path information enables a router to perform policy routing.

Border Gateway Protocol

- The Border Gateway Protocol (BGP) was developed for use in internets that employ the TCP/IP suite.
- BGP has become the preferred exterior router protocol for the Internet.
- BGP was designed to allow routers, called gateways in different ASs to cooperate in the exchange of routing information.
- The protocol operates in terms of messages, which are sent over TCP connections.

Open Shortest Path First (OSPF) Protocol

- The OSPF protocol (RFC 2328) is now widely used as the interior router protocol in TCP/IP networks.
- OSPF computes a route through the internet that incurs the least cost based on a user-configurable metric of cost.
- The user can configure the cost to express a function of delay, data rate, dollar cost, or other factors.
- OSPF is able to equalize loads over multiple equal-cost paths.
- Each router maintains a database that reflects the known topology of the autonomous system of which it is a part.

Error Control (1)

- Error control techniques are needed to guard against loss or damage of data and control information.
- Typically, error control is implemented as two separate functions:
  - error detection and
  - retransmission.
- To achieve error detection, the sender inserts an error-detecting code in the transmitted PDU, which is a function of the other bits in the PDU.
- The receiver checks the value of the code on the incoming PDU.
- If an error is detected, the receiver discards the PDU.

Error Control (2)

- Upon failing to receive an acknowledgment to the PDU in a reasonable time, the sender retransmits the PDU.
- Some protocols also employ an error correction code, which enables the receiver not only to detect errors but, in some cases, to correct them.
- As with flow control, error control is a function that must be performed at various layers of protocol.
- The network access protocol should include error control
  - to assure that data are successfully exchanged between station and network.
- However, a packet of data may be lost inside the network, and the transport protocol should be able to recover from this loss.