Unit-IV

6.1 Introduction: The following are the elements in a wireless network

- **Wireless hosts**: A wireless host might be a laptop, palmtop, smartphone, or desktop computer. The hosts themselves may or may not be mobile.
- **Wireless links**: A host connects to a base station (defined below) or to another wireless host through a wireless communication link. Different wireless link technologies have different transmission rates and can transmit over different distances.
- **Base station**: A base station is responsible for sending and receiving data (e.g. Packets) to and from a wireless host that is associated with that base station. A base station will often be responsible for coordinating the transmission of multiple wireless hosts with which it is associated. When we say a wireless host is "associated" with a base station, we mean that (1) the host is within the wireless communication distance of the base station, and (2) the host uses that base station to relay data between it (the host) and the larger network. Cell towers in cellular networks and access points in 802.11 wireless LANs are examples of base stations. Hosts associated with a base station are often referred to as operating in infrastructure mode,
- **Network infrastructure**: This is the larger network with which a wireless host may wish to communicate

We can classify wireless networks according to two criteria: (i) whether a packet in the wireless network crosses exactly one wireless hop or multiple wireless hops, and (ii) whether there is infrastructure such as a base station in the network:

- **Single-hop, infrastructure-based**: These networks have a base station that is connected to a larger wired network (e.g., the Internet). Furthermore, all communication is between this base station and a wireless host over a single wireless hop. The 802.11 networks you use in the classroom, café, or library; and the 3G cellular data networks that we will learn about shortly all fall in this category.
- **Single-hop, infrastructure-less**: In these networks, there is no base station that is connected to a wireless network. One of the nodes in this single-hop network may coordinate the transmissions of the other nodes. Bluetooth networks and 802.11 networks in ad hoc mode are single-hop, infrastructure-less networks.
- **Multi-hop, infrastructure-based:** In these networks, a base station is present that is wired to the larger network. However, some wireless nodes may have to relay their communication through other wireless nodes in order to communicate via the base station. Some wireless sensor networks and so-called wireless mesh networks fall in this category.
- **Multi-hop, infrastructure-less**: There is no base station in these networks, and nodes may have to relay messages among several other nodes in order to reach a destination. Nodes may also be mobile, with connectivity changing among nodes—a class of

networks known as mobile ad hoc networks (MANETs). If the mobile nodes are vehicles, the network is a vehicular ad hoc network (VANET).

6.2 Wireless Links and Network Characteristics: Important differences between a wired link and a wireless link are as follows:

- **Decreasing signal strength**: Electromagnetic radiation attenuates as it passes through matter (e.g., a radio signal passing through a wall). Even in free space, the signal will disperse, resulting in decreased signal strength (sometimes referred to as path loss) as the distance between sender and receiver increases.
- **Interference from other sources:** Radio sources transmitting in the same frequency band will interfere with each other. For example, 2.4 GHz wireless phones and 802.11b wireless LANs transmit in the same frequency band. Thus, the 802.11b wireless LAN user talking on a 2.4 GHz wireless phone can expect that neither the network nor the phone will perform particularly well. In addition to interference from transmitting sources, electromagnetic noise within the environment (e.g., a nearby motor, a microwave) can result in interference.
- **Multipath propagation:** Multipath propagation occurs when portions of the electromagnetic wave reflect off objects and the ground, taking paths of different lengths between a sender and receiver. This results in the blurring of the received signal at the receiver. Moving objects between the sender and receiver can cause multipath propagation to change over time

The signal-to-noise ratio (SNR) is a relative measure of the strength of the received signal (i.e., the information being transmitted) and this noise. The SNR is typically measured in units of decibels (dB), The bit error rate (BER) is the probability that a transmitted bit is received in error at the receiver. BER versus the SNR for three different modulation techniques for encoding information for transmission on an idealized wireless channel is shown in 6.3. 6.3 illustrate several physical-layer characteristics that are important in understanding higher-layer wireless communication protocols:

- For a given modulation scheme, the higher the SNR, the lower the BER. Since a sender can increase the SNR by increasing its transmission power, a sender can decrease the probability that a frame is received in error by increasing its transmission power. There are also disadvantages associated with increasing the transmission power: More energy must be expended by the sender (an important concern for battery-powered mobile users), and the sender's transmissions are more likely to interfere with the transmissions of another sender
- For a given SNR, a modulation technique with a higher bit transmission rate (whether in error or not) will have a higher BER
- Dynamic selection of the physical-layer modulation technique can be used to adapt the modulation technique to channel conditions. The SNR (and hence the BER) may change as a result of mobility or due to changes in the environment. Adaptive modulation and coding are used in cellular data systems and in the 802.11 WiFi and 3G cellular data networks

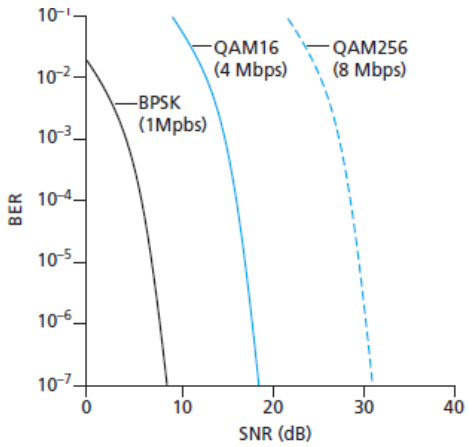


Figure 6.3 ♦ Bit error rate, transmission rate, and SNR

A higher and time-varying bit error rate is not the only difference between a wired and wireless link. Recall that in the case of wired broadcast links, all nodes receive the transmissions from all other nodes. In the case of wireless links, the situation is not as simple, as shown in Figure 6.4. Suppose that Station A is transmitting to Station B. Suppose also that Station C is transmitting to Station B. With the so called **hidden terminal problem**, physical obstructions in the environment (for example, a mountain or a building) may prevent A and C from earing each other's transmissions, even though A's and C's transmissions are indeed interfering at the destination, B. This is shown in Figure 6.4(a). A second scenario that results in undetectable collisions at the receiver results from the **fading** of a signal's strength as it propagates through the wireless medium. Figure 6.4(b) illustrates the case where A and C are placed such that their signals are not strong enough to detect each other's transmissions, yet their signals are strong enough to interfere with each other at station B.

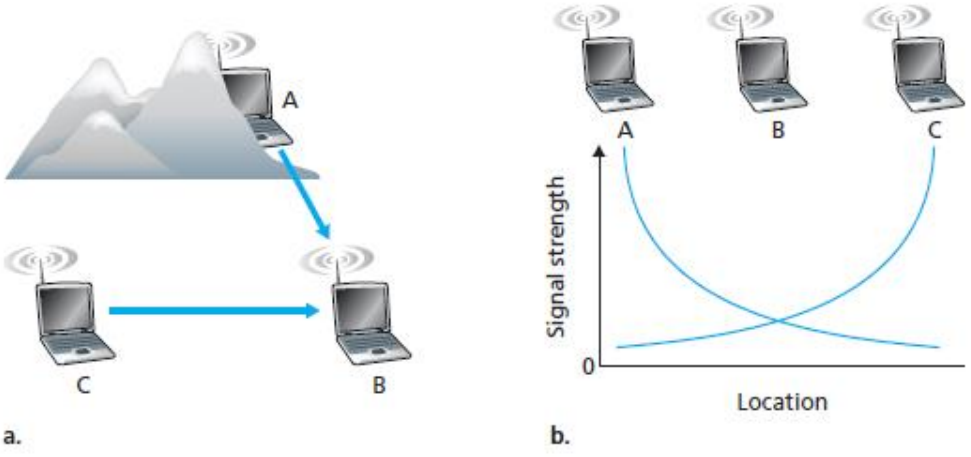


Figure 6.4 ♦ Hidden terminal problem caused by obstacle (a) and fading (b)

6.2.1 CDMA: Code division multiple access (CDMA) belongs to the family of channel partitioning protocols. It is prevalent in wireless LAN and cellular technologies.

- used in several wireless broadcast channels (cellular, satellite, etc) standards
- unique "code" assigned to each user; i.e., code set partitioning
- all users share same frequency, but each user has own chipping sequence (i "chipping

” sequence (i e code) to encode data .e., code) to encode data

- encoded signal = (original data) X (chipping sequence)
- decoding :inner product of encoded signal and chipping sequence
- allows multiple users to allows multiple users to coexist and transmit “coexist ” and transmit simultaneously with minimal interference (if codes are “orthogonal”)

Let di be the value of the data bit for the i^{th} bit slot. Each bit slot is further subdivided into M mini-slots. For the m^{th} mini-slot of the bit-transmission time of di, the output of the CDMA encoder, Zi,m, is the value of di multiplied by the mth bit in the assigned CDMA code, cm:

$$Z_{i,m} = d_i \cdot c_m \qquad (6.1)$$

the receiver would receive the encoded bits, Zi,m, and recover the original data bit, di, by computing:

$$d_i = \frac{1}{M}\sum_{m=1}^{M} Z_{i,m} \cdot c_m \qquad (6.2)$$

In the presence of multiple senders, sender s computes its encoded transmissions, $Z^s_{i,m}$, in exactly the same manner as in Equation 6.1. The value received at a receiver during the mth mini-slot of the ith bit slot, however, is now the sum of the transmitted bits from all N senders during that mini-slot:

$$Z^*_{i,m} = \sum_{s=1}^{N} Z^s_{i,m}$$

Amazingly, if the senders’ codes are chosen carefully, each receiver can recover the data sent by a given sender out of the aggregate signal simply by using the sender’s code in exactly the same manner as in Equation 6.2

$$d_i = \frac{1}{M}\sum_{m=1}^{M} Z^*_{i,m} \cdot c_m \qquad (6.3)$$

CDMA Encode/Decode

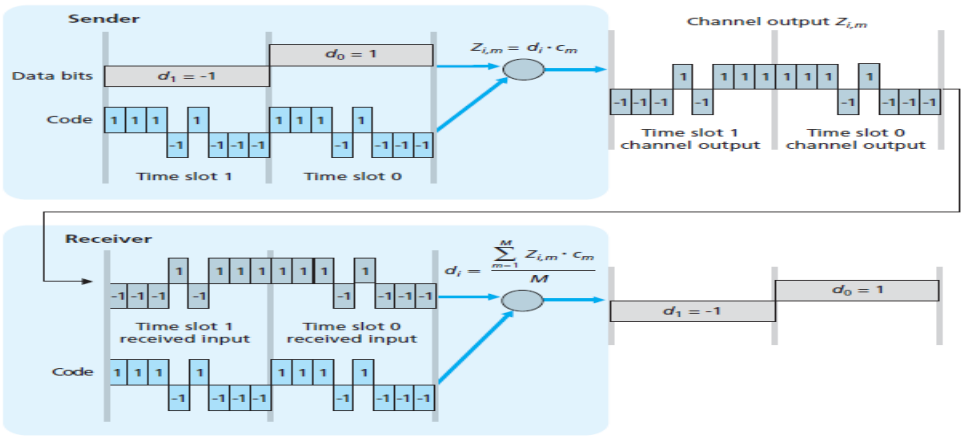


Figure 6.5 ♦ A simple CDMA example: sender encoding, receiver decoding

CDMA: two-sender interference

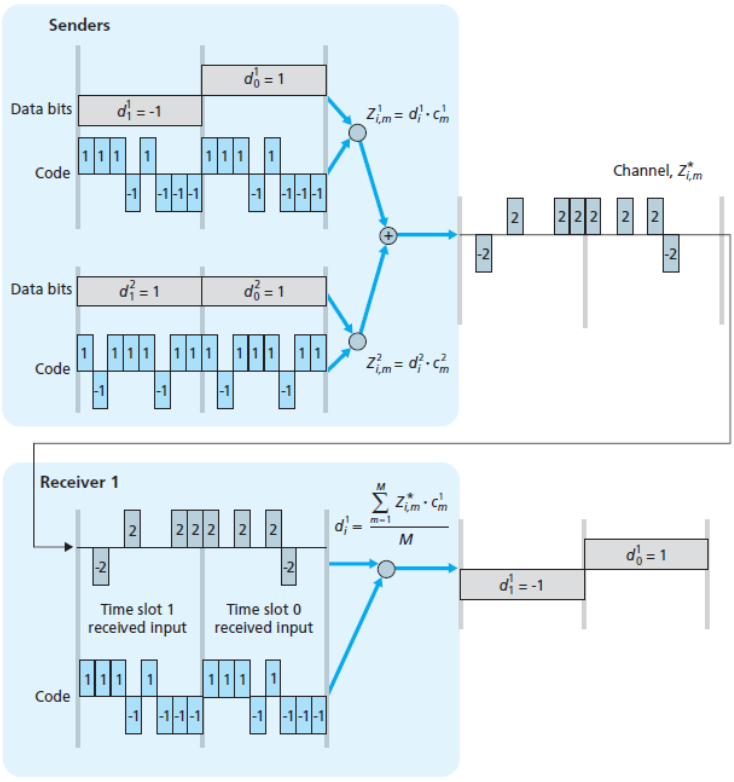


Figure 6.6 ♦ A two-sender CDMA example

6.3 WiFi: 802.11 Wireless LANs: Wireless LANs are now one of the most important access network technologies in the Internet today. Although wireless LAN, also known as WiFi. There are several 802.11 standards for wireless LAN technology, including 802.11b, 802.11a, and 802.11g.

The three 802.11 standards share many characteristics:

- They all use the same medium access protocol, CSMA/CA,
- All three use the same frame structure for their link-layer frames as well.
- All three standards have the ability to reduce their transmission rate in order to reach out over greater distances.

- And all three standards allow for both “infrastructure mode” and “ad hoc mode,”

Table 6.1, the three standards have some major differences at the physical layer.

Standard	Frequency Range (United States)	Data Rate
802.11b	2.4–2.485 GHz	up to 11 Mbps
802.11a	5.1–5.8 GHz	up to 54 Mbps
802.11g	2.4–2.485 GHz	up to 54 Mbps

Table 6.1 ♦ Summary of IEEE 802.11 standards

6.3.1 The 802.11 Architecture: Figure 6.7 illustrates the principal components of the 802.11 wireless LAN architecture. The fundamental building block of the 802.11 architecture is the basic service set (BSS). A BSS contains one or more wireless stations and a central base station, known as an access point (AP) in 802.11 parlance. Figure 6.7 shows the AP in each of two BSSs connecting to an interconnection device (such as a switch or router), which in turn leads to the Internet. As with Ethernet devices, each 802.11 wireless station has a 6-byte MAC address that is stored in the firmware of the station’s adapter.

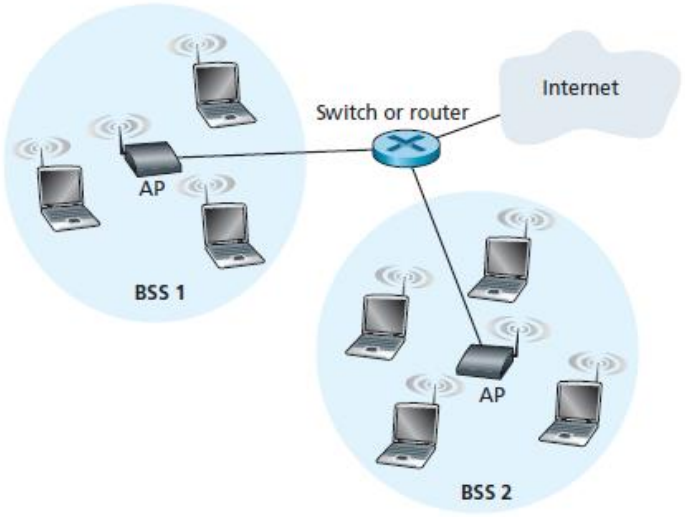


Figure 6.7 ♦ IEEE 802.11 LAN architecture

Figure 6.8 shows that IEEE 802.11 stations can also group themselves together to form an ad hoc network—a network with no central control and with no connections to the “outside world.” Here, the network is formed “on the fly,” by mobile devices that have found themselves in proximity to each other, that have a need to communicate, and that find no pre existing network infrastructure in their location.

Figure 6.8 ♦ An IEEE 802.11 ad hoc network

Channels and Association

In 802.11, each wireless station needs to associate with an AP before it can send or receive network-layer data. When a network administrator installs an AP, the administrator assigns Service Set Identifier (SSID) to the access point. The administrator must also assign a channel number to the AP. To understand channel numbers, recall that 802.11 operate in the frequency range of 2.4 GHz to 2.485 GHz. Within this 85 MHz band, 802.11 define 11 partially overlapping channels. Any two channels are non-overlapping if and only if they are separated by four or more channels. In particular, the set of channels 1, 6, and 11 is the only set of three non overlapping channels.

Wi-Fi Jungle: A Wi-Fi jungle is any physical location where a wireless station receives a sufficiently strong signal from two or more APs. Suppose there are five APs in the Wi-Fi jungle. To gain Internet access, your wireless station needs to join exactly one of the subnets and hence needs to associate with exactly one of the APs.

Associating means the wireless station creates a virtual wire between itself and the AP. Specifically, only the associated AP will send data frames (that is, frames containing data, such as a datagram) to your wireless station, and your wireless station will send data frames into the Internet only through the associated AP.

Beacon frames: The 802.11 standard requires that an AP periodically send beacon frames, each of which includes the AP's SSID and MAC address. Your wireless station, knowing that APs are sending out beacon frames, scans the 11 channels, seeking beacon frames from any APs that may be out there. Having the available APs from the beacon frames, you (or your wireless host) select one of the APs for association.

How to Select the AP: Typically, the host chooses the AP whose beacon frame is received with the highest signal strength. While high signal strength is good, signal strength is not the only AP characteristic that will determine the performance a host receives. In particular, it's possible that the selected AP may have a strong signal, but may be overloaded with other affiliated hosts (that will need to share the wireless bandwidth at that AP), while an unloaded AP is not selected due to a slightly weaker signal.

Passive and Active Scanning: The process of scanning channels and listening for beacon frames is known as passive scanning (see Figure 6.9a). A wireless host can also perform active scanning, by broadcasting a probe frame that will be received by all APs within the wireless host's range, as shown in Figure 6.9b. APs respond to the probe request frame with a

probe response frame. The wireless host can then choose the AP with which to associate from among the responding APs.

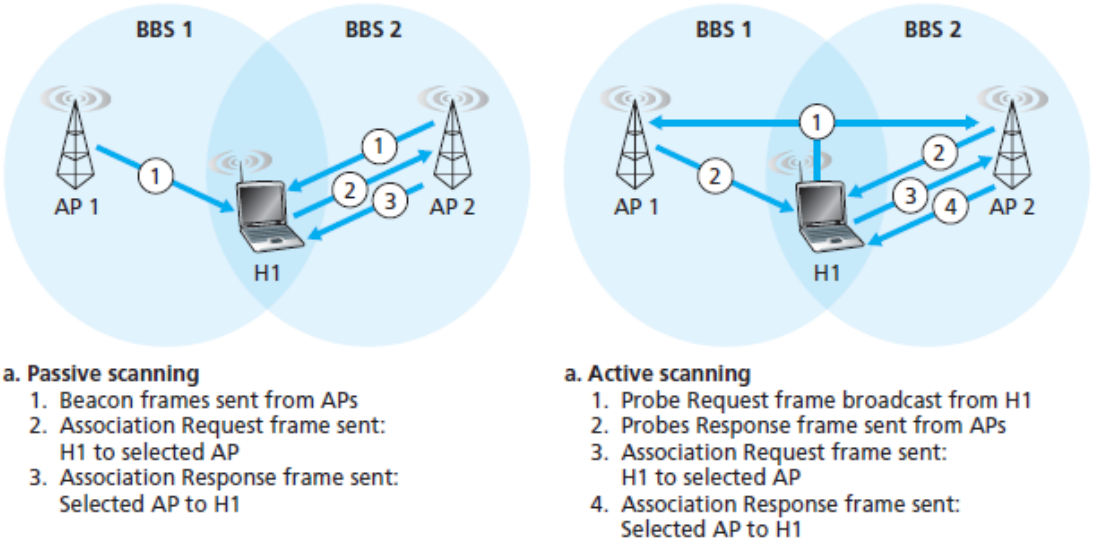


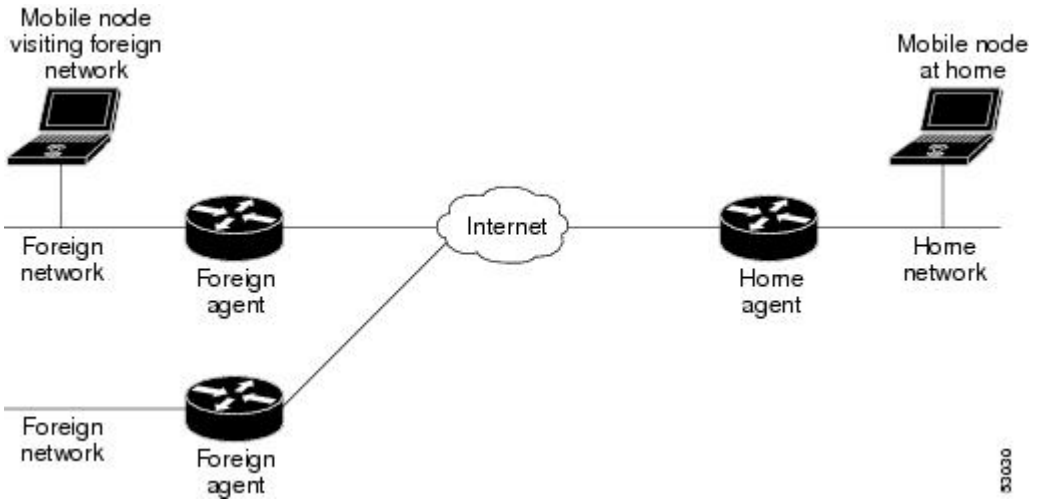
Figure 6.9 ♦ Active and passive scanning for access points

6.6 Mobile IP: Mobile IP is an open standard, defined by the Internet Engineering Task Force (IETF) RFC 2002, that allows users to keep the same IP address, stay connected, and maintain ongoing applications while roaming between IP networks. Because the mobility functions of Mobile IP are performed at the network layer rather than the physical layer, the mobile device can span different types of wireless and wire line networks while maintaining connections and ongoing applications. Remote login, remote printing, and file transfers are some examples of applications.

Components of a Mobile IP Network: Mobile IP has the following three components, as shown in Figure 1:

- Mobile Node
- Home Agent
- Foreign Agent

Figure 1 Mobile IP Components and Relationships



- The Mobile Node is a device such as a cell phone, personal digital assistant, or laptop whose software enables network roaming capabilities.

- **The Home Agent** is a router on the home network serving as the anchor point for communication with the Mobile Node; it tunnels packets from a device on the Internet, called a Correspondent Node, to the roaming Mobile Node. (A tunnel is established between the Home Agent and a reachable point for the Mobile Node in the foreign network.)

- **The Foreign Agent** is a router that may function as the point of attachment for the Mobile Node when it roams to a foreign network, delivering packets from the Home Agent to the Mobile Node.

- **The care-of address** is the termination point of the tunnel toward the Mobile Node when it is on a foreign network. The Home Agent maintains an association between the home IP address of the Mobile Node and its care-of address, which is the current location of the Mobile Node on the foreign or visited network

How Mobile IP Works: The Mobile IP process has three main phases,

- **Agent Discovery**: A Mobile Node discovers its Foreign and Home Agents during agent discovery.

- **Registration:** The Mobile Node registers its current location with the Foreign Agent and Home Agent during registration.

- **Tunnelling**: A reciprocal tunnel is set up by the Home Agent to the care-of address (current location of the Mobile Node on the foreign network) to route packets to the Mobile Node as it roams.

Agent Discovery: It is the discovery of a new foreign agent, with a new network address, that allows the network layer in a mobile node to learn that it has moved into a new foreign network. This process is known as agent discovery. Agent discovery can be accomplished in one of two ways:

- via agent advertisement or
- via agent solicitation.

With **agent advertisement**, a foreign or home agent advertises its services using an extension to the existing router discovery protocol .The agent periodically broadcasts an ICMP message with a type field of 9 (router discovery) on all links to which it is connected. Among the more important fields in the extension are the following:

- **Home agent bit (H).** Indicates that the agent is a home agent for the network in which it resides.
- **Foreign agent bit (F).** Indicates that the agent is a foreign agent for the network in which it resides.
- **Registration required bit (R).** Indicates that a mobile user in this network must register with a foreign agent. In particular, a mobile user cannot obtain a care of address in the foreign network (for example, using DHCP) and assume the functionality of the foreign agent for itself, without registering with the foreign agent.
- **M, G encapsulation bits**. Indicate whether a form of encapsulation other than IP-in-IP encapsulation will be used.
- **Care-of addresses (COA) fields.** A list of one or more care-of addresses provided by the foreign agent. In our example below, the COA will be associated with the foreign agent, who will receive datagrams sent to the COA and then forward them to the appropriate mobile node. The mobile user will select one of these addresses as its COA when registering with its home agent.

Figure 6.27 illustrates some of the key fields in the agent advertisement message

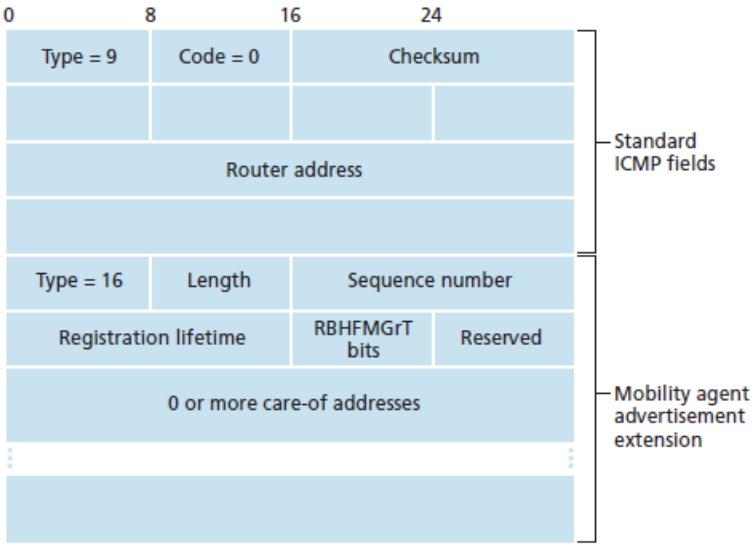


Figure 6.27 ♦ ICMP router discovery message with mobility agent advertisement extension

With **agent solicitation**, a mobile node wanting to learn about agents without waiting to receive an agent advertisement can broadcast an agent solicitation message, which is simply an ICMP message with type value 10. An agent receiving the solicitation wills unicast an agent advertisement directly to the mobile node, which can then proceed as if it had received an unsolicited advertisement.

Registration with the Home Agent: Once a mobile IP node has received a COA, that address must be registered with the home agent. This can be done either via the foreign agent (who then registers the COA with the home agent) or directly by the mobile IP node itself. We consider the former case below. Four steps are involved.

1. Following the receipt of a foreign agent advertisement, a mobile node sends a mobile IP registration message to the foreign agent. The registration message is carried within a UDP datagram and sent to port 434. The registration message carries a COA advertised by the foreign agent, the address of the home agent (HA), the permanent address of the mobile node (MA), the requested lifetime of the registration, and a 64-bit registration identification.
2. The foreign agent receives the registration message and records the mobile node's permanent IP address. The foreign agent now knows that it should be looking for datagrams containing an encapsulated datagram whose destination address matches the permanent address of the mobile node. The foreign agent then sends a mobile IP registration message (again, within a UDP datagram) to port 434 of the home agent. The message contains the COA, HA, MA, encapsulation format requested, requested registration lifetime, and registration identification.
3. The home agent receives the registration request and checks for authenticity and correctness. The home agent binds the mobile node's permanent IP address with the COA; in the future, datagrams arriving at the home agent and addressed to the mobile node will now be encapsulated and tunnelled to the COA. The home agent sends a mobile IP registration reply containing the HA, MA, actual registration lifetime, and the registration identification of the request that is being satisfied with this reply.
4. The foreign agent receives the registration reply and then forwards it to the mobile node.

At this point, registration is complete, and the mobile node can receive datagrams sent to its permanent address. Figure 6.28 illustrates these steps.

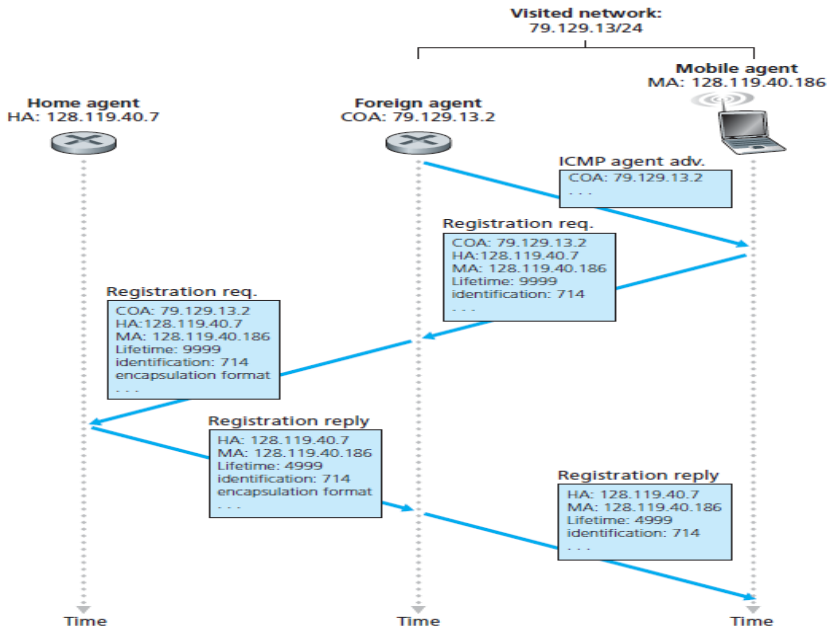


Figure 6.28 ♦ Agent advertisement and mobile IP registration

8.1 Cryptography: Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word kryptos, which means hidden**.**

8.1.1 Introduction to Cryptography:

- **Plaintext**: This is the original intelligible message or data that is fed into the algorithm as input.
- **Encryption algorithm**: The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key**: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.
- **Cipher text**: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts. The cipher text is an apparently random stream of data and, as it stands, is unintelligible.
- **Decryption algorithm**: This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext
- **Cryptanalysis**: The art of breaking ciphers, known as cryptanalysis, and the art of devising them (cryptography) are collectively known as **Cryptology**
- **Cryptology** - the field of both cryptography and cryptanalysis

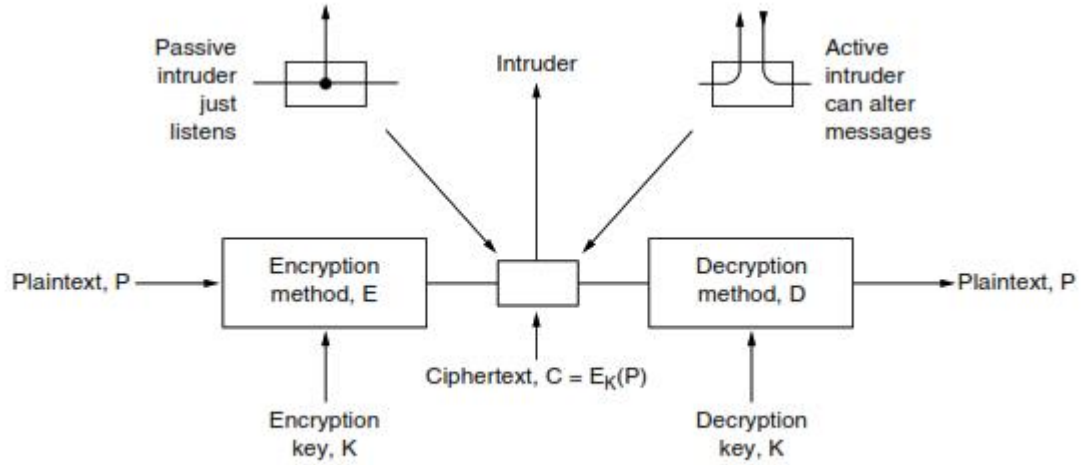


Figure 8-2. The encryption model (for a symmetric-key cipher).

We will use $C = E_K(P)$ to mean that the encryption of the plaintext P using key K gives the ciphertext C. Similarly, $P = D_K(C)$ represents the decryption of C to get the plaintext again. It then follows that

$$D_K(E_K(P)) = P$$

Kerckhoff's principle: The idea that the cryptanalyst knows the algorithms and that the secrecy lies exclusively in the keys is called Kerckhoff's principle,

Kerckhoff's principle: All algorithms must be public; only the keys are secret

The cryptanalysis problem has three principal variations:

Ciphertext-Only: During ciphertext-only attacks, the attacker has access only to a number of encrypted messages. He has no idea what the plaintext data or the secret key may be. The goal is to recover as much plaintext messages as possible or (preferably) to guess the secret key. After discovering the encryption key, it will be possible to break all the other messages which have been encrypted by this key.

Known-Plaintext Attack: During known-plaintext attacks, the attacker has an access to the ciphertext and its corresponding plaintext. His goal is to guess the secret key (or a number of secret keys) or to develop an algorithm which would allow him to decrypt any further messages.

Chosen-Plaintext Attack: During the chosen-plaintext attack, a cryptanalyst can choose arbitrary plaintext data to be encrypted and then he receives the corresponding ciphertext. He tries to acquire the secret encryption key or alternatively to create an algorithm which would allow him to decrypt any ciphertext messages encrypted using this key (but without actually knowing the secret key).

8.1.2 Substitution Ciphers : In a substitution cipher, each letter or group of letters is replaced by another letter or group of letters to disguise it

Caesar cipher: The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet.

Example: Replaces each letter by 3rd letter on

meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB

Monoalphabetic cipher: Monoalphabetic cipher which also substitutes one letter of the alphabet with another letter of the alphabet. However, rather than substituting according to a regular pattern (for example, substitution with an offset of k for all letters), any letter can be substituted for any other letter, as long as each letter has a unique substitute letter, and vice versa. The substitution rule in Figure 8.3 shows one possible rule for encoding plaintext.

Plaintext letter:	a b c d e f g h i j k l m n o p q r s t u v w x y z
Ciphertext letter:	m n b v c x z a s d f g h j k l p o i u y t r e w q

Figure 8.3 ♦ A monoalphabetic cipher

A monoalphabetic cipher would also appear to be better than the Caesar cipher in that there are 26! (on the order of 1026) possible pairings of letters rather than 25 possible pairings. A brute-force approach of trying all 1026 possible pairings would require far too much work to be a feasible way of breaking the encryption algorithm and decoding the message.
Another approach is to guess a probable word or phrase. For example, consider the following ciphertext from an accounting firm (blocked into groups of five characters):

CTBMN BYCTC BTJDS QXBNS GST JC BTSWX CTQTZ CQVUJ
QJSGS T JQZZ MNQJS VLNSX VSZ JU JDSTS JQUUS JUBX J
DSKSU JSNTK BGAQJ ZBGYQ T LCTZ BNYBN QJSW

A likely word in a message from an accounting firm is financial. Using our knowledge that financial has a repeated letter (i), with four other letters between their occurrences, we look for repeated letters in the ciphertext at this spacing. We find 12 hits, at positions 6, 15, 27, 31, 42, 48, 56, 66, 70, 71, 76, and 82. However, only two of these, 31 and 42, have the next letter (corresponding to n in the plaintext) repeated in the proper place. Of these two, only 31 also has the a correctly positioned, so we know that financial begins at position 30

8.1.3 Transposition Ciphers: Substitution ciphers preserve the order of the plaintext symbols but disguise them. Transposition ciphers, in contrast, reorder the letters but do not disguise them. Figure 8-3 depicts a common transposition cipher, the columnar transposition. The cipher is keyed by a word or phrase not containing any repeated letters. In this example, MEGABUCK is the key. The purpose of the key is to order the columns, with column 1 being under the key letter closest to the start of the alphabet, and so on. The plaintext is written horizontally, in rows, padded to fill the matrix if need be. The ciphertext is read out by columns, starting with the column whose key letter is the lowest

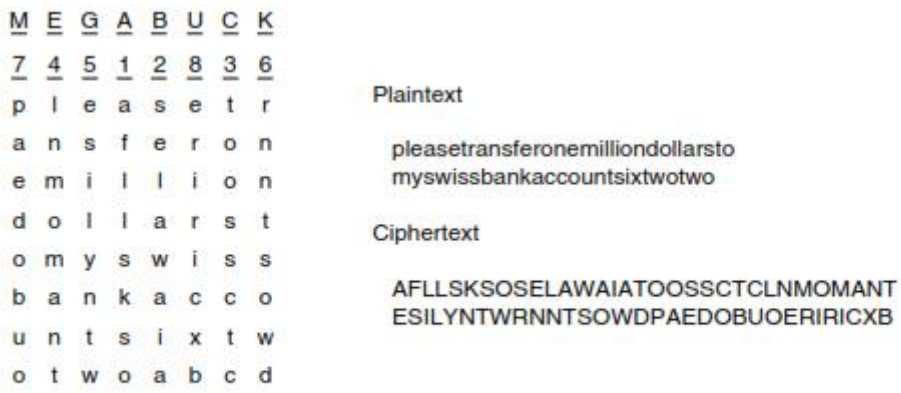


Figure 8-3. A transposition cipher.

8.1.4 One-Time Pads: One-time pad cipher is a type of Vignere cipher which includes the following features −

- It is an unbreakable cipher.
- The key is exactly same as the length of message which is encrypted.
- The key is made up of random symbols.
- As the name suggests, key is used one time only and never used again for any other message to be encrypted.

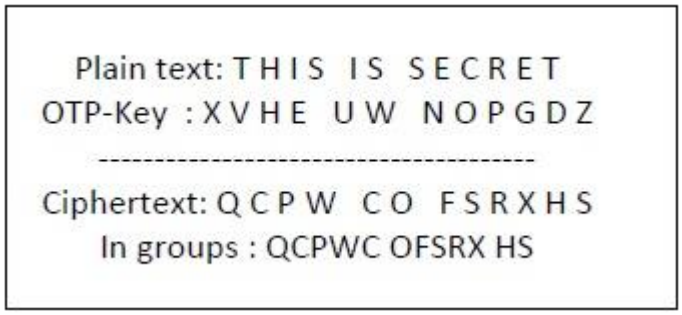
Due to this, encrypted message will be vulnerable to attack for a cryptanalyst. The key used for a one-time pad cipher is called **pad**, as it is printed on pads of paper.

Why is it Unbreakable?

The key is unbreakable owing to the following features −

- The key is as long as the given message.
- The key is truly random and specially auto-generated.
- Key and plain text calculated as modulo 10/26/2.
- Each key should be used once and destroyed by both sender and receiver.
- There should be two copies of key: one with the sender and other with the receiver.

Encryption: To encrypt a letter, a user needs to write a key underneath the plaintext. The plaintext letter is placed on the top and the key letter on the left. The cross section achieved between two letters is the plain text. It is described in the example below –



Decryption: To decrypt a letter, user takes the key letter on the left and finds cipher text letter in that row. The plain text letter is placed at the top of the column where the user can find the cipher text letter.

Quantum Cryptography: Quantum cryptography is based on the fact that light comes in little packets called photons, which have some peculiar properties. Furthermore, light can be polarized by being passed through a polarizing filter, a fact well known to both sunglasses wearers and photographers. If a beam of light (i.e., a stream of photons) is passed through a polarizing filter, all the photons emerging from it will be polarized in the direction of the filter's axis (e.g., vertically). If the beam is now passed through a second polarizing filter, the intensity of the light emerging from the second filter is proportional to the square of the cosine of the angle between the axes. If the two axes are perpendicular, no photons get through. The absolute orientation of the two filters does not matter; only the angle between their axes counts.

8.2 SYMMETRIC-KEY ALGORITHMS: The first class of encryption algorithms are called symmetric-key algorithms because they use the same key for encryption and decryption. Transpositions and substitutions can be implemented with simple electrical circuits. Figure 8- 6(a) shows a device, known as a P-box (P stands for permutation), used to effect a transposition on an 8-bit input. If the 8 bits are designated from top to bottom as 01234567, the output of this particular P-box is 36071245. By appropriate internal wiring, a P-box can be made to perform any transposition and do it at practically the speed of light since no computation is involved, just signal propagation.

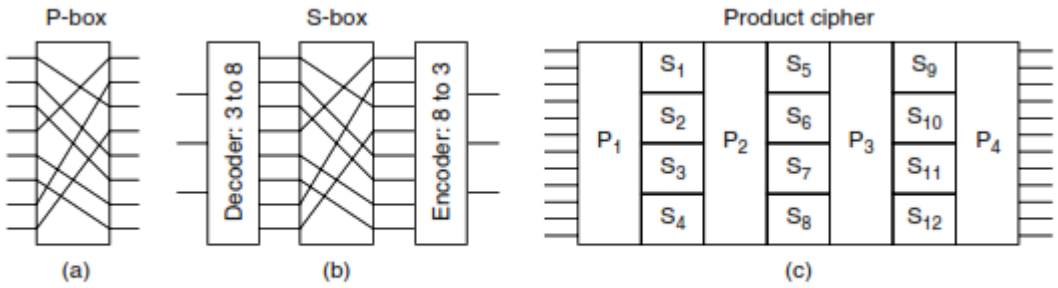


Figure 8-6. Basic elements of product ciphers. (a) P-box. (b) S-box. (c) Product.

Substitutions are performed by S-boxes, as shown in Fig. 8-6(b). In this example, a 3-bit plaintext is entered and a 3-bit ciphertext is output. The 3-bit input selects one of the eight lines exiting from the first stage and sets it to 1; all the other lines are 0. The second stage is a P-box. The third stage encodes the selected input line in binary again. With the wiring shown, if the eight octal numbers 01234567 were input one after another, the output sequence would be 24506713. In other words, 0 has been replaced by 2, 1 has been replaced by 4, etc. Again, by appropriate wiring of the P-box inside the S-box, any substitution can be accomplished.
The real power of these basic elements only becomes apparent when we cascade a whole series of boxes to form a product cipher, as shown in Fig. 8-6(c). In this example, 12 input lines are transposed (i.e., permuted) by the first stage (P1). In the second stage, the input is

broken up into four groups of 3 bits, each of which is substituted independently of the others (S1 to S4)

8.2.1 DES—The Data Encryption Standard: The most widely used encryption scheme is based on the Data Encryption Standard (DES) adopted in 1977 by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), The algorithm itself is referred to as the Data Encryption Algorithm (DEA).

The overall scheme for DES encryption is illustrated in Figure below. As with any encryption scheme, there are two inputs to the encryption function: the plaintext to be encrypted and the key. In this case, the plaintext must be 64 bits in length and the key is 56 bits in length.

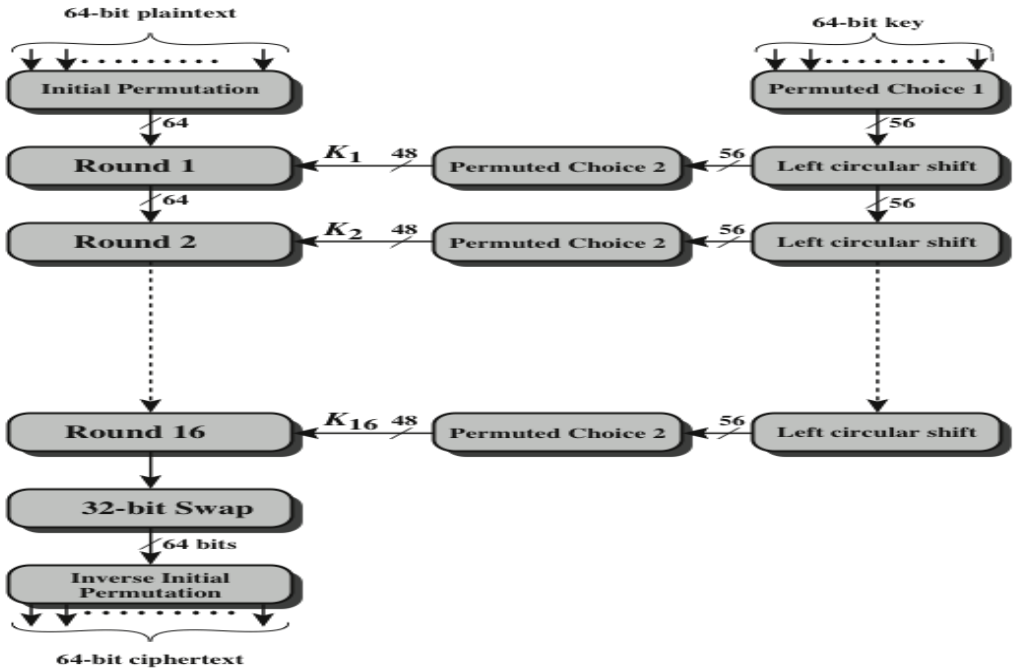
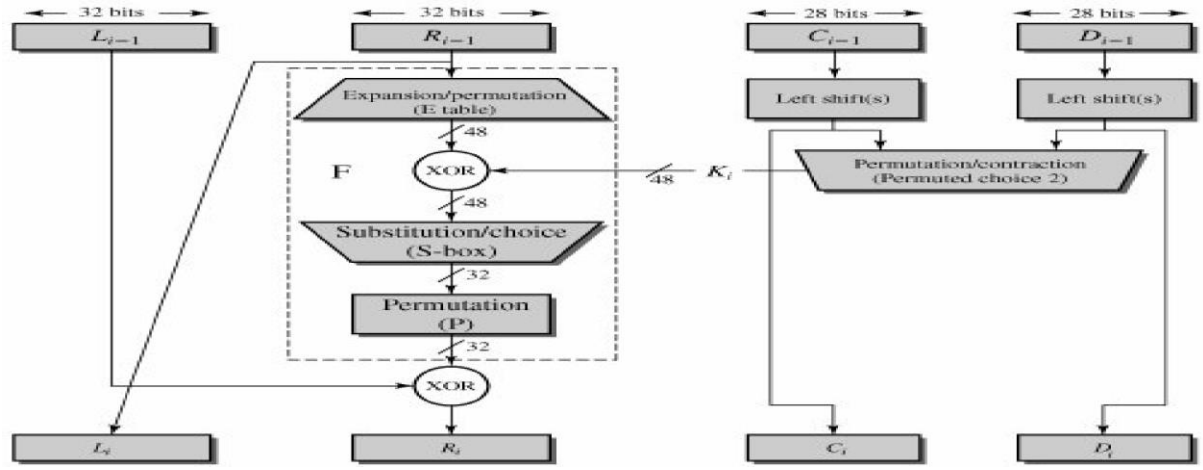


Figure 3.5 General Depiction of DES Encryption Algorithm

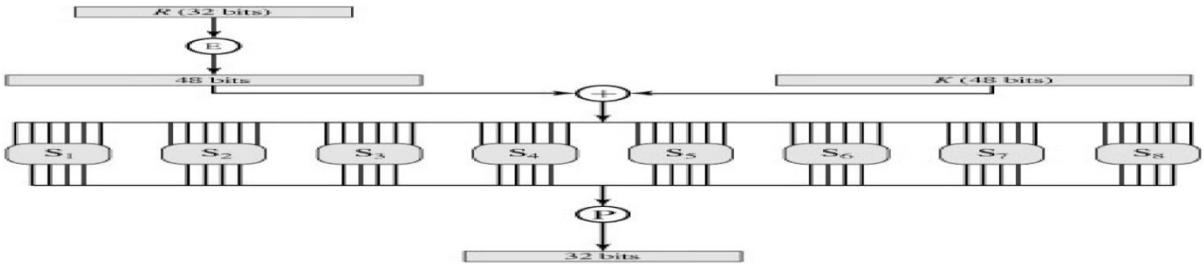
The processing of the plaintext proceeds in three phases. First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input. This is followed by a phase consisting of 16 rounds of the same function, which involves both permutation and substitution functions. The output of the last (sixteenth) round consists of 64 bits that are a function of the input plaintext and the key. The left and right halves of the output are swapped to produce the preoutput. Finally, the preoutput is passed through a permutation (IP^{-1}) that is the inverse of the initial permutation function, to produce the 64-bit cipher text.

The right-hand portion of Figure shows the way in which the 56-bit key is used. Initially, the key is passed through a permutation function. Then, for each of the 16 rounds, a subkey (Ki) is produced by the combination of a left circular shift and a permutation. The permutation function is the same for each round, but a different subkey is produced because of the repeated shifts of the key bits.

Details of Single Round:



The round key Ki is 48 bits. The R input is 32 bits. This R input is first expanded to 48 bits by using a table that defines a permutation plus an expansion that involves duplication of 16 of the R bits (Table 3.2c). The resulting 48 bits are XORed with Ki. This 48-bit result passes through a substitution function that produces a 32-bit output, which is permuted as defined by Table 3.2d. The role of the S-boxes in the function F is illustrated in Figure below



The substitution consists of a set of eight S-boxes, each of which accepts 6 bits as input and produces 4 bits as output. The first and last bits of the input to box Si form a 2-bit binary number to select one of four substitutions defined by the four rows in the table for Si. The middle four bits select one of the sixteen columns. The decimal value in the cell selected by the row and column is then converted to its 4-bit representation to produce the output.

Triple DES: As early as 1979, IBM realized that the DES key length was too short and devised a way to effectively increase it, using triple encryption (Tuchman, 1979). The method chosen, which has since been incorporated in International Standard 8732, is illustrated in Fig. 8-8. Here, two keys and three stages are used. In the first stage, the plaintext is encrypted using DES in the usual way with K1. In the second stage, DES is run in decryption mode, using K2 as the key. Finally, another DES encryption is done with K1. This design immediately gives rise to two questions. First, why are only two keys used, instead of three? Second, why is EDE (Encrypt Decrypt Encrypt) used, instead of EEE (Encrypt Encrypt Encrypt)? The reason that two keys are used is that even the most paranoid of cryptographers believe that 112 bits is adequate for routine commercial applications for the time being. (And among cryptographers, paranoia is considered a feature, not a bug.) Going to 168 bits would

just add the unnecessary overhead of managing and transporting another key for little real gain.

Figure 8-8. (a) Triple encryption using DES. (b) Decryption.

8.2.2 AES—The Advanced Encryption Standard: The Rijndael proposal for AES defined a cipher in which the block length and the key length can be independently specified to be 128,192, or 256 bits. The AES specification uses the same three key size alternatives but limits the block length to 128 bits**.**

Rijndael was designed to have the following characteristics:

- Resistance against all known attacks
- Speed and code compactness on a wide range of platforms
- Design simplicity

Figure 5.1 shows the overall structure of AES. The input to the encryption and decryption algorithms is a single 128-bit block. This block is depicted as a square matrix of bytes. This block is copied into the State array, which is modified at each stage of encryption or decryption. After the final stage, State is copied to an output matrix. Similarly, the 128-bit key is depicted as a square matrix of bytes. This key is then expanded into an array of key schedule words; each word is four bytes and the total key schedule is 44 words for the 128-bit key.

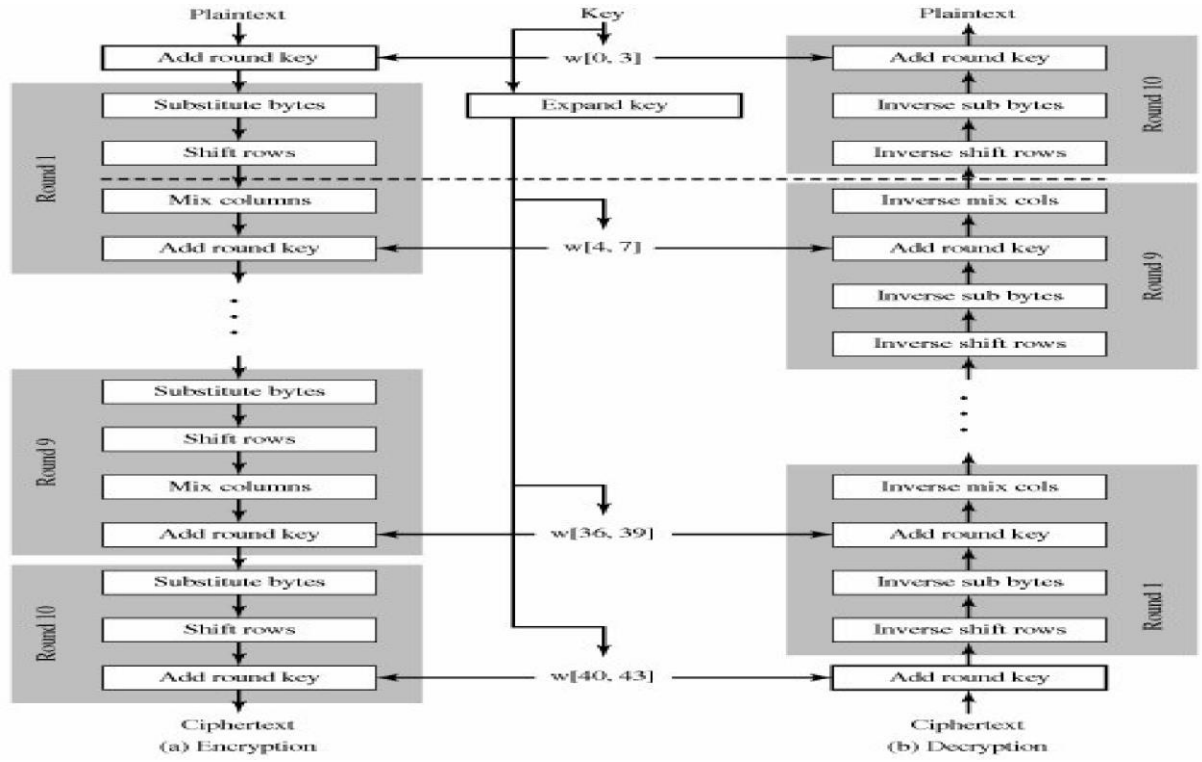
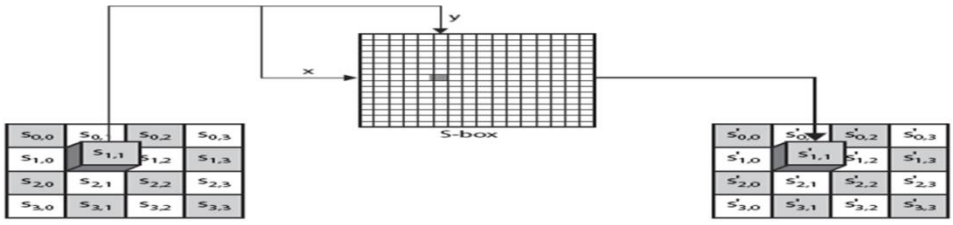


Figure 5.1. AES Encryption and Decryption

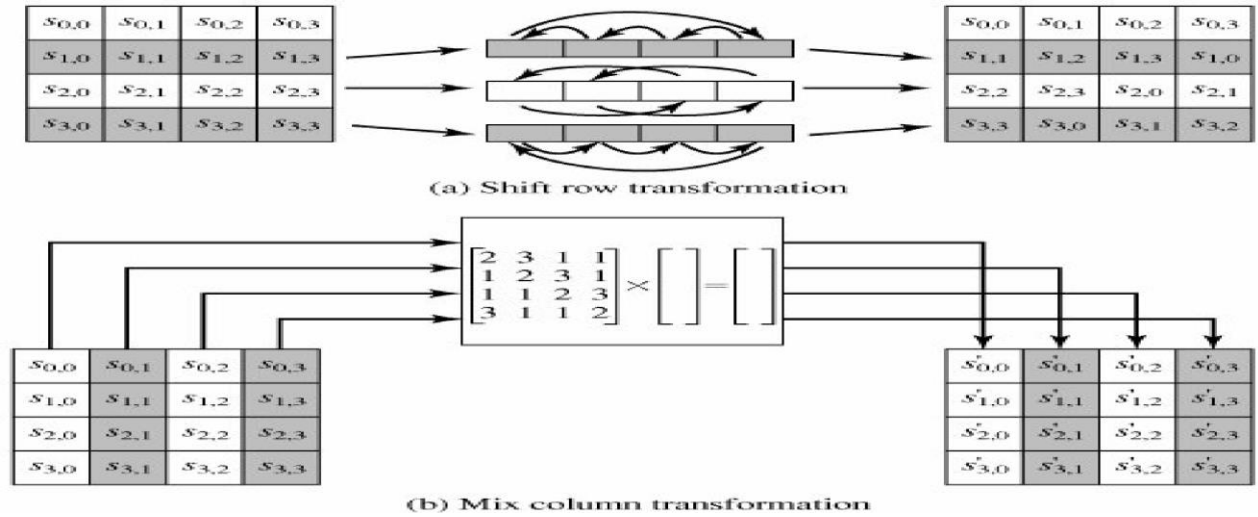
Four different stages are used, one of permutation and three of substitution:

- Substitute bytes: Uses an S-box to perform a byte-by-byte substitution of the block
- ShiftRows: A simple permutation
- MixColumns: A substitution that makes use of arithmetic over GF(28)
- AddRoundKey: A simple bitwise XOR of the current block with a portion of the expanded key

Substitute Bytes Transformation: The forward substitute byte transformation, called SubBytes, is a simple table lookup (Figure 5.4a). AES defines a 16 x 16 matrix of byte values, called an S-box (Table 5.4a), that contains a permutation of all possible 256 8-bit values. Each individual byte State is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value. These row and column values serve as indexes into the S-box to select a unique 8-bit output value.



ShiftRows Transformation: The forward shift row transformation, called ShiftRows, is depicted in Figure 5.5a. The first row of State is not altered. For the second row, a 1-byte circular left shift is performed. For the third row, a 2-byte circular left shift is performed. For the fourth row, a 3-byte circular left shift is performed. The inverse shift row transformation, called InvShiftRows, performs the circular shifts in the opposite direction for each of the last three rows, with a one-byte circular right shift for the second row, and so on.



MixColumns Transformation: The forward mix column transformation, called Mix Columns, operates on each column individually. Each byte of a column is mapped into a new

value that is a function of all four bytes in that column. The transformation can be defined by the following matrix multiplication on State (Figure 5.5b)

AddRoundKey Transformation: In the forward add round key transformation, called Add Round Key, the 128 bits of State are bitwise XORed with the 128 bits of the round key. The operation is viewed as a column wise operation between the 4 bytes of a State column and one word of the round key; it can also be viewed as a byte-level operation

8.3 PUBLIC-KEY ALGORITHMS: Suppose Alice wants to communicate with Bob. As shown in Figure 8.6, rather than Bob and Alice sharing a single secret key (as in the case of symmetric key systems), Bob (the recipient of Alice's messages) instead has two keys—a public key that is available to everyone in the world (including Trudy the intruder) and a private key that is known only to Bob. We will use the notation KB+ and KB– to refer to Bob's public and private keys, respectively. In order to communicate with Bob, Alice first fetches Bob's public
key. Alice then encrypts her message, m, to Bob using Bob's public key and a known (for example, standardized) encryption algorithm; that is, Alice computes KB+ (m). Bob receives Alice's encrypted message and uses his private key and a known (for example, standardized) decryption algorithm to decrypt Alice's encrypted message. That is, Bob computes KB–(KB +(m)).

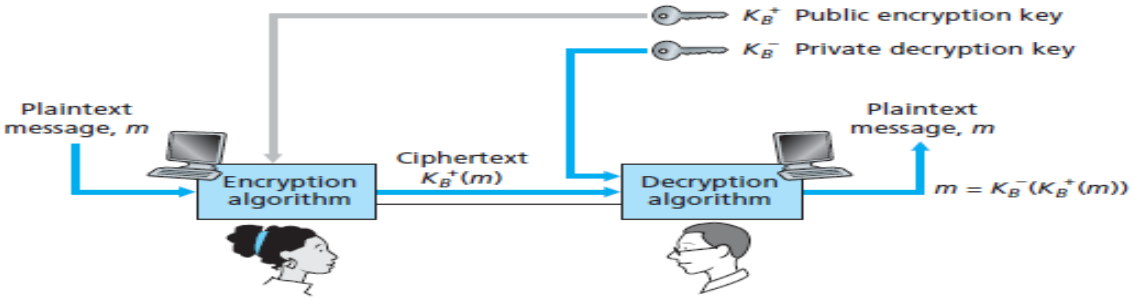


Figure 8.6 ◆ Public key cryptography

8.3.1 RSA: One of the first successful algorithms for public key cryptography was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978. The Rivest-Shamir-Adleman (RSA) scheme is the most widely accepted and implemented general-purpose approach to public-key encryption.

The **RSA** scheme is a cipher in which the plaintext and cipher text are integers between 0 and *n* - 1 for some *n*. A typical size for *n* is 1024 bits, or 309 decimal digits. That is, *n* is less than 2^{1024}.

Description of the Algorithm

RSA makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to $\log_2 (n) + 1$.

Encryption and decryption for some plaintext block M and cipher text block C are:

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of PU = {e, n} and a private key of PR = {d,n}.

For this algorithm to be satisfactory for public-key encryption, the following requirements must be met.

1. It is possible to find values of e, d, and n such that $M^{ed} \bmod n = M$ for all M <n.
2. It is relatively easy to calculate $M^e \bmod n$ and Cd mod n for all values of M <n.
3. It is infeasible to determine d given e and n.

By the first requirement, there is a need to find a relationship of the form $M^{ed} \bmod n = M$

The preceding relationship holds if e and d are multiplicative inverses modulo (n), where (n) is the Euler totient function. For any prime numbers p, q, (pq) = (p - 1)(q - 1). The relationship between e and d can be expressed as edmod (n) = 1

This is equivalent to saying

$$ed \equiv 1 \; mod \; (n)$$

$$d \equiv e{-}1 mod \; (n)$$

That is, e and d are multiplicative inverses mod f(n). Note that, according to the rules of modular arithmetic, this is true only if d (and therefore e) is relatively prime to (n). Equivalently, gcd(φ(n), d) = 1.

The ingredients of the RSA scheme are the following:

p, q, two prime numbers (private, chosen)

n = pq (public, calculated)

e, with gcd($\phi(n)$, e) = 1; 1 <e <$\phi(n)$ (public, chosen)

$d \equiv e{-}1 mod \; (n)$ (private, calculated)

The private key consists of {d, n} and the public key consists of {e, n}. Suppose that user A has published its public key and that user B wishes to send the message M to A. Then B calculates $C = M^e \bmod n$ and transmits C. On receipt of this cipher text user A decrypts by calculating $M = C^d \bmod n$.

Key Generation	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p - 1)(q - 1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Example:

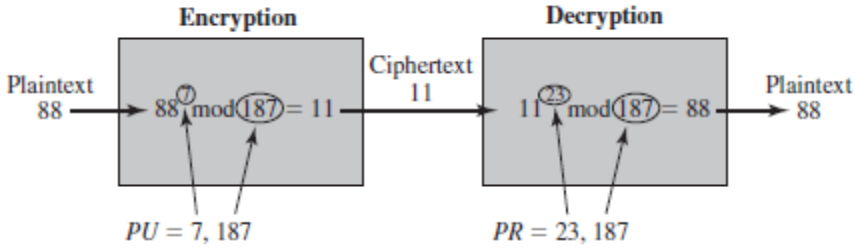
The keys were generated as follows.
1. Select two prime numbers, p = 17 and q = 11.
2. Calculate n = pq= 17 * 11 = 187.
3. Calculate (n) = (p - 1)(q - 1) = 16 * 10 = 160.
4. Select e such that e is relatively prime to (n)= 160 and less than $\phi(n)$; choose e = 7.
5. Determine d such that $de \equiv 1\ (mod\ 160)$ and d < 160. The correct value is d = 23, because 23 * 7 = 161 = (1 * 160) + 1; d can be calculated using the extended Euclid's algorithm.

The resulting keys are public key PU = {7, 187} and private key PR = {23, 187}.
Assume M = 88,

For encryption,
Calculate C = 88^7 mod 187. Exploiting the properties of modular arithmetic, this can be done as follows.

88^7 mod 187 = [(88^4 mod 187) (88^2 mod 187) (88^1 mod 187)] mod 187
88^1 mod 187 = 88
88^2 mod 187 = 7744 mod 187 = 77
88^4 mod 187 = 59,969,536 mod 187 = 132
88^7 mod 187 = (88 77 132) mod 187 = 894,432 mod 187 = 11

For decryption,
Calculate M = 11^{23} mod 187:
11^{23} mod 187 = [(11^1 mod 187) (11^2 mod 187) (11^4 mod 187) (11^8 mod 187)(11^8 mod 187)] mod 187
11^1 mod 187 = 11
11^2 mod 187 = 121
11^4 mod 187 = 14,641 mod 187 = 55
11^8 mod 187 = 214,358,881 mod 187 = 33
11^{23} mod 187 = (11 *121* 55* 33 *33) mod 187 = 79,720,245 mod 187 = 88



Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

8.9 Operational Security:

In a computer network, when traffic entering/leaving a network is security-checked, logged, dropped, or forwarded, it is done by operational devices known as firewalls, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs).

8.9.1 Firewalls:

A firewall is a combination of hardware and software that isolates an organization's internal network from the Internet at large, allowing some packets to pass and blocking others. A firewall allows a network administrator to control access between the outside world and resources within the administered network by managing the traffic flow to and from these resources. A firewall has three goals:

All traffic from outside to inside, and vice versa, passes through the firewall. Figure 8.33 shows a firewall, sitting squarely at the boundary between the administered network and the rest of the Internet.

Only authorized traffic, as defined by the local security policy, will be allowed to pass. With all traffic entering and leaving the institutional network passing through the firewall, the firewall can restrict access to authorized traffic

The firewall itself is immune to penetration. The firewall itself is a device connected to the network. If not designed or installed properly, it can be compromised, in which case it provides only a false sense of security

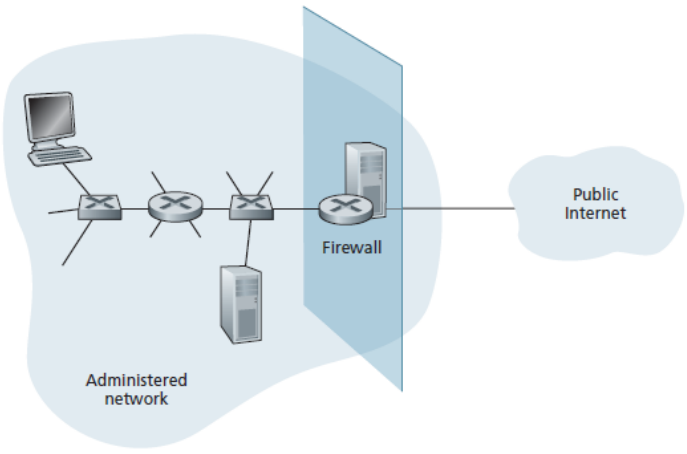


Figure 8.33 ♦ Firewall placement between the administered network and the outside world

Firewalls can be classified in three categories:

- traditional packet filters,
- stateful filters, and
- application gateways

Traditional Packet Filters: As shown in Figure 8.33, an organization typically has a gateway router connecting its internal network to its ISP (and hence to the larger public Internet). All traffic leaving and entering the internal network passes through this router, and it is at this router where packet filtering occurs. A packet filter examines each datagram in isolation, determining whether the datagram should be allowed to pass or should be dropped based on administrator-specific rules. Filtering decisions are typically based on:

- IP source or destination address
- Protocol type in IP datagram field: TCP, UDP, ICMP, OSPF, and so on
- TCP or UDP source and destination port
- TCP flag bits: SYN, ACK, and so on
- ICMP message type
- Different rules for datagrams leaving and entering the network
- Different rules for the different router interfaces

A network administrator configures the firewall based on the policy of the organization. The policy may take user productivity and bandwidth usage into account as well as the security concerns of an organization. Table 8.5 lists a number of possible polices an organization may have, and how they would be addressed with a packet filter

Policy	Firewall Setting
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for organization's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets—except DNS packets.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP ping packets going to a "broadcast" address (eg 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

Table 8.5 ♦ Policies and corresponding filtering rules for an organization's network 130.27/16 with Web server at 130.207.244.203

- A filtering policy can be based on a combination of addresses and port numbers.
- Filtering can also be based on whether or not the TCP ACK bit is set.
- Firewall rules are implemented in routers with access control lists, with each router interface having its own list

Stateful Packet Filters:

In a traditional packet filter, filtering decisions are made on each packet in isolation.

Stateful filters actually track TCP connections, and use this knowledge to make filtering

Decisions the firewall can observe the beginning of a new connection by observing a three-way handshake (SYN, SYNACK, and ACK); and it can observe the end of a connection when it sees a FIN packet for the connection. The firewall can also (conservatively) assume that the connection is over when it hasn't seen any activity over the connection for, say, 60 seconds. An example connection table for a firewall is shown in Table 8.7. This connection

table indicates that there are currently three ongoing TCP connections, all of which have been initiated from within the organization. Additionally, the stateful filter includes a new column, "check connection," in its access control list, as shown in Table 8.8. Note that Table 8.8 is identical to the access control list in Table 8.6, except now it indicates that the connection should be checked for two of the rules.

source address	dest address	source port	dest port
222.22.1.7	37.96.87.123	12699	80
222.22.93.2	199.1.205.23	37654	80
222.22.65.143	203.77.240.43	48712	80

Table 8.7 ♦ Connection table for stateful filter

action	source address	dest address	protocol	source port	dest port	flag bit	check conxion
allow	222.22/16	outside of 222.22/16	TCP	>1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	>1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	>1023	53	—	
allow	outside of 222.22/16	222.22/16	UDP	53	>1023	—	X
deny	all	all	all	all	all	all	

Table 8.8 ♦ Access control list for stateful filter

Application Gateway: To have finer-level security, firewalls must combine packet filters with application gateways. Application gateways look beyond the IP/TCP/UDP headers and make policy decisions based on application data. An application gateway is an application-specific server through which all application data (inbound and outbound) must pass. Multiple application gateways can run on the same host, but each gateway is a separate server with its own processes.

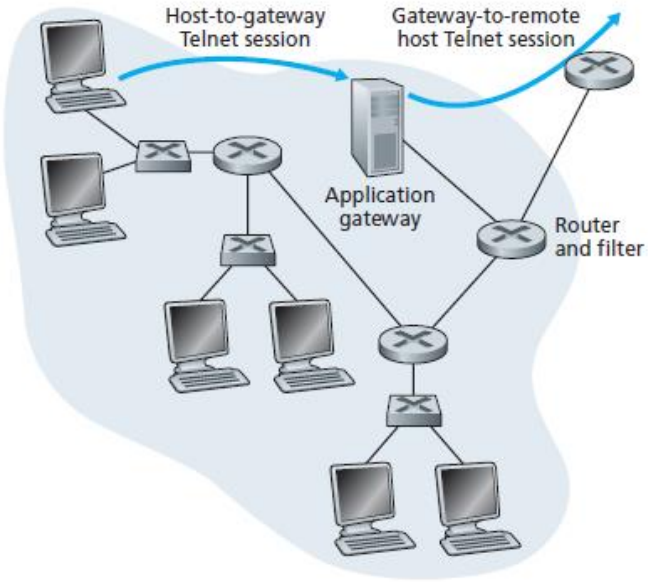


Figure 8.34 ♦ Firewall consisting of an application gateway and a filter

Application gateways do not come without their disadvantages. First, a different application gateway is needed for each application. Second, there is a performance penalty to be paid, since all data will be relayed via the gateway. This becomes a concern particularly when multiple users or applications are using the same gateway machine. Finally, the client software must know how to contact the gateway when the user makes a request, and must know how to tell the application gateway what external server to connect to.