USN | | | | | | | | | | |

Internal Assessment Test 1 – September 2025

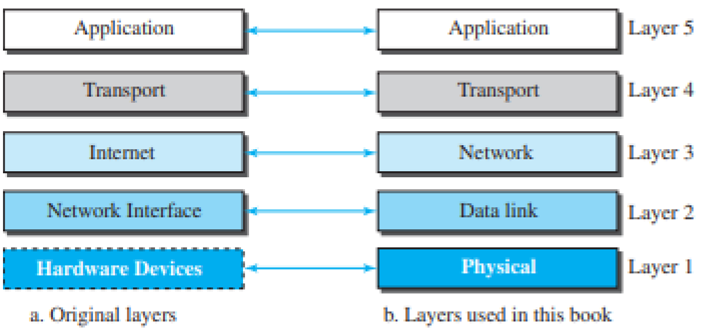
Sub:	Computer Networks					Sub Code:	BCS502	Branch:	CSE
Date:	26.09.2025	Duration:	90 mins	Max Marks:	50	Sem / Sec:	V (A, B & C)		OBE

	Answer any FIVE FULL Questions	MARKS	CO	RBT
1 (a)	With the help of a neat diagram, explain the functionalities of each layer in TCP/IP Protocol.	7	CO2	L2

2.2 TCP/IP PROTOCOL SUITE

Now that we know about the concept of protocol layering and the logical communication between layers in our second scenario, we can introduce the TCP/IP (Transmission Control Protocol/Internet Protocol). TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internet today. It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality. The term *hierarchical* means that each upper level protocol is supported by the services provided by one or more lower level protocols. The original TCP/IP protocol suite was defined as four software layers built upon the hardware. Today, however, TCP/IP is thought of as a five-layer model. Figure 2.4 shows both configurations.

Figure 2.4 *Layers in the TCP/IP protocol suite*



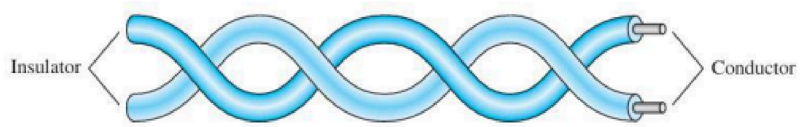
Physical Layer

We can say that the physical layer is responsible for carrying individual bits in a frame across the link. Although the physical layer is the lowest level in the TCP/IP protocol suite, the communication between two devices at the physical layer is still a logical communication because there is another, hidden layer, the transmission media, under the physical layer. Two devices are connected by a transmission medium (cable or air). We need to know that the transmission medium does not carry bits; it carries electrical or optical signals. So the bits received in a frame from the data-link layer are transformed and sent through the transmission media, but we can think that the logical unit between two physical layers in two devices is a *bit*. There are several protocols that transform a bit to a signal. We discuss them in Part II when we discuss the physical layer and the transmission media.

	Data-link Layer We have seen that an internet is made up of several links (LANs and WANs) connected by routers. There may be several overlapping sets of links that a datagram can travel from the host to the destination. The routers are responsible for choosing the *best* links. However, when the next link to travel is determined by the router, the data-link layer is responsible for taking the datagram and moving it across the link. The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wireless WAN. We can also have different protocols used with any link type. In each case, the data-link layer is responsible for moving the packet through the link. ***Network Layer*** The network layer is responsible for creating a connection between the source computer and the destination computer. The communication at the network layer is host-to-host. However, since there can be several routers from the source to the destination, the routers in the path are responsible for choosing the best route for each packet. We can say that the network layer is responsible for host-to-host communication and routing the packet through possible routes. Again, we may ask ourselves why we need the network layer. We could have added the routing duty to the transport layer and dropped this layer. One reason, as we said before, is the separation of different tasks between different layers. The second reason is that the routers do not need the application and transport layers. Separating the tasks allows us to use fewer protocols on the routers. ***Transport Layer*** The logical connection at the transport layer is also end-to-end. The transport layer at the source host gets the message from the application layer, encapsulates it in a transport-layer packet (called a *segment* or a *user datagram* in different protocols) and sends it, through the logical (imaginary) connection, to the transport layer at the destination host. In other words, the transport layer is responsible for giving services to the application layer: to get a message from an application program running on the source host and deliver it to the corresponding application program on the destination host. We may ask why we need an end-to-end transport layer when we already have an end-to-end application layer. The reason is the separation of tasks and duties, which we discussed earlier. The transport layer should be independent of the application layer. In addition, we will see that we have more than one protocol in the transport layer, which means that each application program can use the protocol that best matches its requirement. ***Application Layer*** As Figure 2.6 shows, the logical connection between the two application layers is end-to-end. The two application layers exchange *messages* between each other as though there were a bridge between the two layers. However, we should know that the communication is done through all the layers.			
1 (b)	Consider n devices in a network, Identify the number of cable links required for the following topologies: a. Mesh b. Ring c. Star Solution: a. n(n-1)/2 b. N c. n	3	CO1	L3
2 (a)	What are guided transmission media? Explain Twisted pair cable in detail. Solution:	5	CO1	L2

6.2 Twisted-Pair Cable

A twisted pair cable consists of two insulated copper conductors twisted together. Each wire in the pair serves a different function: one carries the signal to the receiver, and the other acts as a ground reference. The receiver processes the difference between the two wires to retrieve the signal.

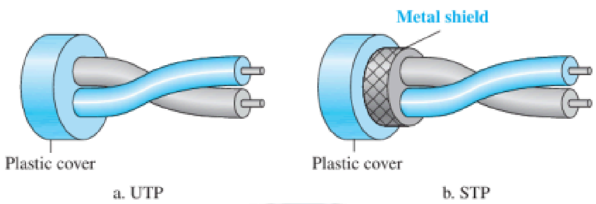


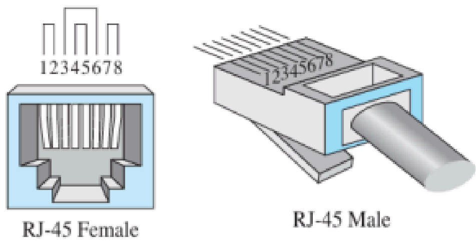
Noise and Interference

Twisted pair cables are designed to minimize the impact of interference (noise) and crosstalk. When the wires are parallel, noise or crosstalk can affect each wire differently due to their varying distances from the sources of interference. By twisting the wires, the cable maintains a balance. In each twist, the relative positions of the wires to the noise source change, helping to ensure that both wires experience similar levels of interference. This twisting reduces the impact of unwanted signals, as the receiver calculates the difference between the wires, canceling out most of the noise.

Shielded vs. Unshielded Twisted-Pair Cables

1. **Unshielded Twisted-Pair (UTP):** The most common type used in communications, UTP cables do not have additional shielding. They are less expensive and less bulky but can be more susceptible to interference.
2. **Shielded Twisted-Pair (STP):** STP cables have an additional metal foil or braided mesh covering each pair of conductors. This shielding reduces interference and improves signal quality but makes the cables bulkier and more costly.





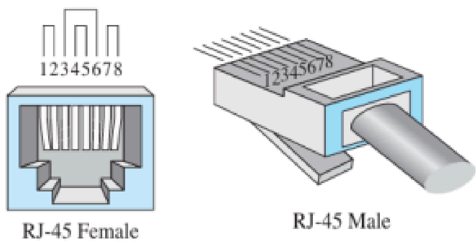
Performance

The performance of twisted-pair cables is often assessed by measuring attenuation (signal loss) in relation to frequency and distance. Although twisted-pair cables can handle a broad range of frequencies, attenuation increases significantly at frequencies above 100 kHz. Attenuation is measured in decibels per kilometer (dB/km), and higher frequencies result in greater signal loss.

Applications

Twisted-pair cables are widely used in various applications:

1. **Telephone Lines:** Used for voice and data transmission in the local loop connecting subscribers to telephone offices.
2. **DSL Lines:** Provide high-data-rate connections by utilizing the high bandwidth of UTP cables.
3. **Local-Area Networks (LANs):** Employed in networks such as 10Base-T and 100Base-T for data transmission.



Performance

The performance of twisted-pair cables is often assessed by measuring attenuation (signal loss) in relation to frequency and distance. Although twisted-pair cables can handle a broad range of frequencies, attenuation increases significantly at frequencies above 100 kHz. Attenuation is measured in decibels per kilometer (dB/km), and higher frequencies result in greater signal loss.

Applications

Twisted-pair cables are widely used in various applications:

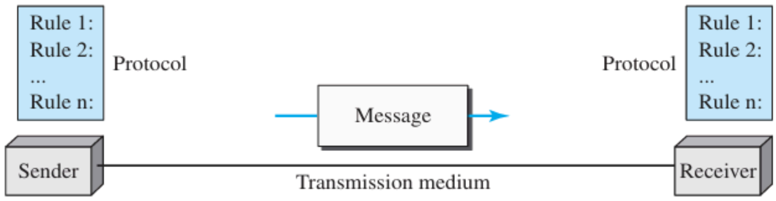
1. **Telephone Lines:** Used for voice and data transmission in the local loop connecting subscribers to telephone offices.
2. **DSL Lines:** Provide high-data-rate connections by utilizing the high bandwidth of UTP cables.
3. **Local-Area Networks (LANs):** Employed in networks such as 10Base-T and 100Base-T for data transmission.

2 (b)	Identify the five components of a data communications system and explain the components briefly with the help of a neat diagram Solution	5	CO1	L2

1.1.1 Components

A data communications system has five components (see Figure 1.1).

Figure 1.1 *Five components of data communication*



1. **Message.** The **message** is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. **Sender.** The **sender** is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. **Receiver.** The **receiver** is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. **Transmission medium.** The **transmission medium** is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
5. **Protocol.** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

3 (a)	Outline Bellman ford algorithm to find single source shortest path.	4	CO	L2

Solution:

Algorithm

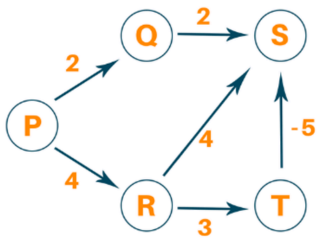
```
BellmanFord()
   for each v ∈ V
      d[v] = ∞;
   d[s] = 0;
   for i=1 to |V|-1
      for each edge (u,v) ∈ E
         Relax(u,v, w(u,v));
   for each edge (u,v) ∈ E
      if (d[v] > d[u] + w(u,v))
           return "no solution";
```

What will be the running time?

A: O(VE)

```
Relax(u,v,w): if (d[v] > d[u]+w) then d[v]=d[u]+w
```

3 (b)	Given a source vertex P find out the shortest paths using Bellman ford Algorithm.	6	CO2	L3



SOLUTION

Edge	Weight
P → Q	2
P → R	4
Q → S	2
R → S	4
R → T	3
T → S	-5

Source vertex = **P**

Vertex	Initial Distance from P	Predecessor
P	0	—
Q	∞	—
R	∞	—
S	∞	—
T	∞	—

Iteration 1

1. P → Q :

   0 + 2 = 2 → Q = 2

2. P → R :

   0 + 4 = 4 → R = 4

3. Q → S :

   2 + 2 = 4 → S = 4

4. R → S :

   4 + 4 = 8 → (S already 4, no change)

5. R → T :

   4 + 3 = 7 → T = 7

6. T → S :

   7 + (-5) = 2 → S = 2

Iteration 2

Check all edges again — no further updates (distances remain the same).

Iteration 3 & 4

No further updates — algorithm converges.

Vertex	Distance from P	Shortest Path
P	0	P
Q	2	P → Q
R	4	P → R
S	2	P → R → T → S (cost 4 + 3 - 5 = 2)
T	7	P → R → T

4(a)	Given the data word 1 0 0 1 0 0 1 1 and the divisor 1 1 0 1, show the generation of CRC code word at the sender side.	4	CO2	L3

SOLUTION

- **Data word:** 10010011 (8 bits)
- **Divisor:** 1101 (4 bits)
- **Number of redundant bits:** 4 - 1 = 3

```
          11000100   (Quotient)
        ________
1101 | 10010011000  (Augmented data word)
     - 1101       (First 4 bits of dividend are 1001, so divide)
     ______
       01000
     -  1101
     ______
       01011
     -   1101
     ______
         01100
     -    1101
     ______
          00010
     -      0000
     ______
     ______
          000100
     -      0000
     ______
          0001001
     -      0000
     _______
          00010010
     -       1101
     _______
            01000
     -       1101
     _______
            01010
     -        1101
     _______
            0111   (Remainder)
```

4(b)	Assume even parity (for bit 1) find the parity bit for each of the following data units. a. 1 0 0 1 0 1 1 c. 1 0 0 0 0 0 0	2	CO2	L3

	b. 0 0 0 1 1 0 0 d. 1 1 1 0 1 1 1 Solution: a. 0 b. 0 c. 1 d. 0			
4(c)	A slotted ALOHA network transmits 200-bit frames on a shared channel of 200kbps. what is the throughput if the system produces: a. 1000 frames per second b. 500 frames per second c. 250 frames per second Solution **Solution** This situation is similar to the previous exercise except that the network is using slotted ALOHA instead of pure ALOHA. The frame transmission time is 200/200 kbps or 1 ms. **a.** In this case G is 1. So $S = G \times e^{-G} = 0.368$ (36.8 percent). This means that the throughput is $1000 \times 0.0368 = 368$ frames. Only 368 out of 1000 frames will probably survive. Note that this is the maximum throughput case, percentagewise. **b.** Here G is 1/2. In this case $S = G \times e^{-G} = 0.303$ (30.3 percent). This means that the throughput is $500 \times 0.0303 = 151$. Only 151 frames out of 500 will probably survive. **c.** Now G is 1/4. In this case $S = G \times e^{-G} = 0.195$ (19.5 percent). This means that the throughput is $250 \times 0.195 = 49$. Only 49 frames out of 250 will probably survive.	4	CO2	L3
5	Define HDLC. Explain the frame format of HDLC with types. Solution **HDLC** • High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links. • Implements stop and wait protocol. HDLC provides two common transfer modes: • Normal Response Mode (NRM) • Asynchronous Balanced Mode (ABM)	10	CO2	L2

Figure 11.14 *Normal response mode*

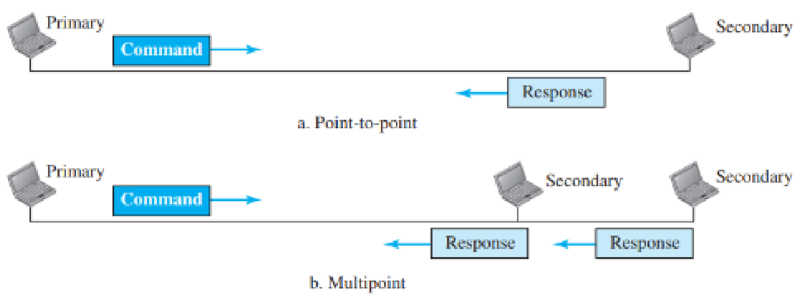
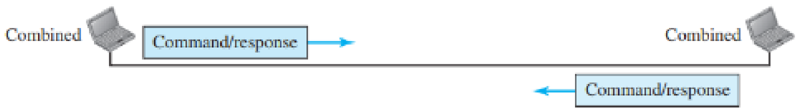


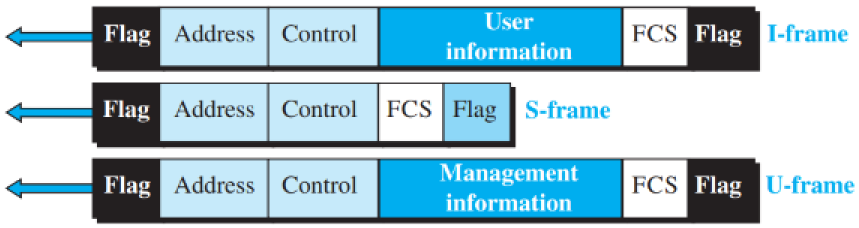
Figure 11.15 *Asynchronous balanced mode*



HDLC defines three types of frames:

- Information Frames (I-Frames)
- Supervisory frames (S-Frames)
- Unnumbered frames (U-Frames)

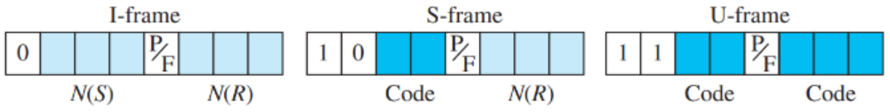
Figure 11.16 *HDLC frames*



Frames

- **Flag field:** Contains flag 01111110, which identifies both the beginning and the end of a frame.
- **Address field:** Contains the address of the secondary station.
- **Control Field**: One or two bytes used for flow or error control.
- **Information Field**: Contains the User's data from the network layer.
- **FCS Field**: Frame Check Sequence is the HDLC error detection field.

Figure 11.17 *Control field format for the different frame types*



Control Field for I frames

- I-frames are designed to carry user data from network layer.
- First bit defines the type.
- If the first bit is 1, it is an I-Frame.
- Next 3 bits, defines a sequence number.
- Last N(R) corresponds to the acknowledgement number.
- P/F is poll or Final. If it is set to 1, it means frame is sent by primary to secondary.

Control Field for S-Frames

- Supervisory frames are used for flow and error control.
- S-Frames do not have information fields.
- If the first two bits are 10, then its an S-Frame.
- Last 3 bits, N(R) correspond to acknowledgement number (ACK) or NAK.
- The 2 bits called code are used to define S-Frame.

Control Field for S-Frames

- 00 – Receive Ready (RR): This frame acknowledges the receipt of the frame or group of frames.
- 10 - Receive not Ready (RNR): It acknowledges the frame and announces that the receiver is busy and cannot receive more frames.
- 01 – Reject (REJ): It is a NAK frame. Informs the sender about the loss or damage of the frame.
- 11 – Selective Reject (SREJ): Informs the receiver that error is detected in a specific frame in sequence

	Control Field of U-Frames • U-Frames contain an information field, but used for system management information. • U-frame codes are divided into two sections: • a 2-bit prefix before the P/F bit and a 3-bit suffix after the P/F bit. • Together, these two segments (5 bits) can be used to create up to 32 different types of U-frames.			
6(a)	Using RSA Algorithm, encrypt a message M = 8. Assume p =3 and q = 7. Find the public key, private key. Also show the cipher text. Solution: **Here are the steps for the RSA algorithm:** **1. Calculate n** : $n = p \times q = 3 \times 7 = 21$ **2. **Calculate **** $\phi(n)$****: $\phi(n) = (p-1) \times (q-1) = (3-1) \times (7-1) = 2 \times 6 = 12.$ **3. Choose e** : Select an integer e such that $1 < e < \phi(n)$ and $gcd(e, \phi(n)) = 1$. The number $e = 7$ works, as $gcd(7, 12) = 1$. Thus, the public key is $\{e, n\} = \{7, 21\}$. **4. Calculate d** : Find the private key component d such that $(d \times e) \pmod{\phi(n)} = 1$. This means $(d \times 7) \pmod{12} = 1$. • $7 \times 1 = 7 \pmod{12}$ • $7 \times 2 = 14 \pmod{12} = 2$ • $7 \times 3 = 21 \pmod{12} = 9$ • $7 \times 5 = 35 \pmod{12} = 11$ • $7 \times 7 = 49 \pmod{12} = 1.$ • So, $d = 7$. The private key is $\{d, n\} = \{7, 21\}$.	3	CO2	L3

	5. Encrypt the message: The ciphertext C is calculated as $C = M^e \pmod{n}$. • $M = 8$, $e = 7$, $n = 21$. • $C = 8^7 \pmod{21}$. • $8^2 = 64 \pmod{21} = 1$. • $8^7 = (8^2)^3 \times 8 = (1)^3 \times 8 = 8$. • $C = 8$. In this case, the ciphertext is the same as the original message. This happens because $8^2 \equiv 1 \pmod{21}$. • **Public Key**: $\{7, 21\}$ • **Private Key**: $\{7, 21\}$ • **Ciphertext**: 8			
6(b)	Explain three persistence methods in CSMA with the help of flow charts. Solution: •CSMA can reduce the possibility of collision, but it cannot eliminate it. •The possibility of collision still exists because of propagation delay. •At time t1, station B senses the medium and finds it idle, so it sends a frame. •At time t2 (t2 > t1), station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C. •Station C also sends a frame. The two signals collide and both frames are destroyed **Methods :** •1-persistent method •Non-persistent method •P-persistent method	7	CO2	L3

1-Persistent

The *1-persistent method* is simple and straightforward. In this method, after the station finds the line idle, it sends its frame immediately (with probability 1). This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately. We will see later that Ethernet uses this method.

Nonpersistent

In the *nonpersistent method,* a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again. The nonpersistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously. However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

p-*Persistent*

The p-*persistent method* is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time. The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency. In this method, after the station finds the line idle it follows these steps:

1. With probability p, the station sends its frame.

2. With probability $q = 1 - p$, the station waits for the beginning of the next time slot and checks the line again.
   a. If the line is idle, it goes to step 1.
   b. If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.

Figure 12.9 *Behavior of three persistence methods*

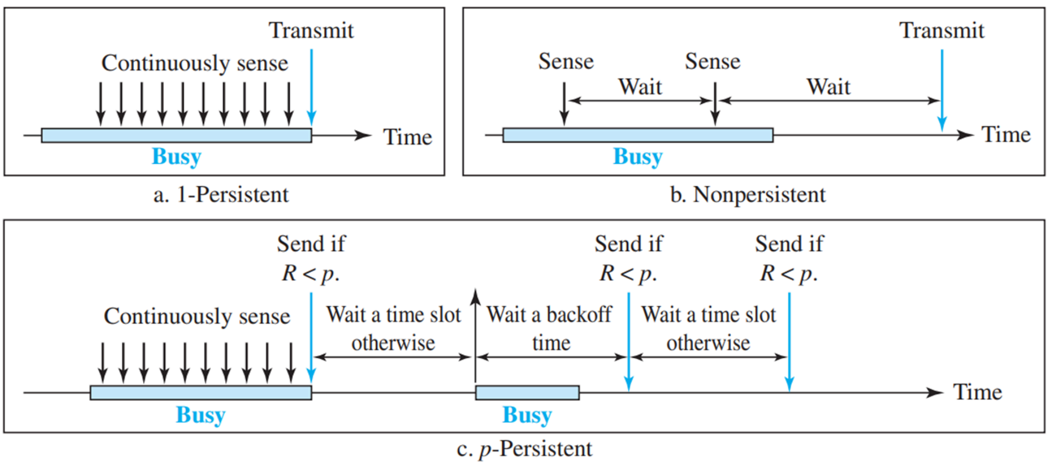
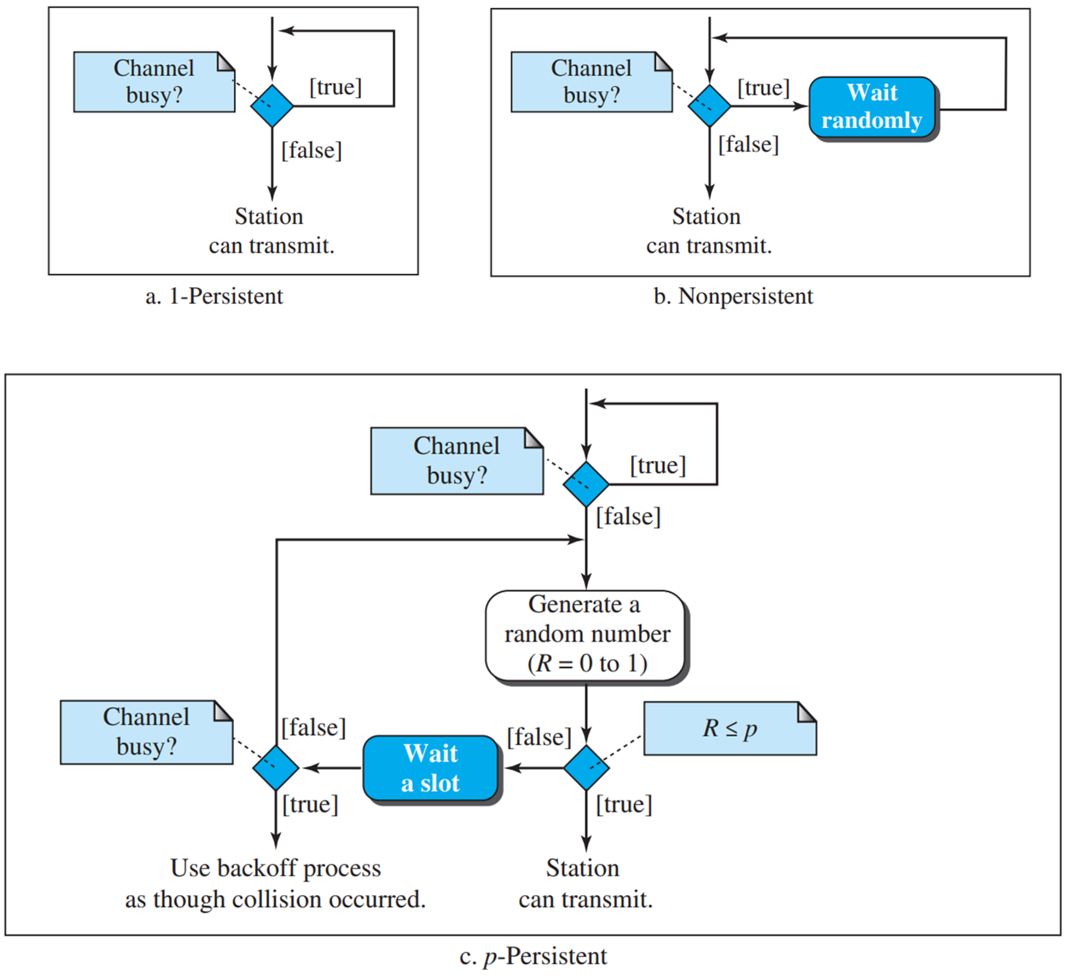


Figure 12.10 *Flow diagram for three persistence methods*



CI **CCI** **HOD**