BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Registration No : _____

SCT - A

School of Computing Skills

Session: 2020-21 (Summer Semester)

B. Voc. Program, 3rd Semester,

End-Sem. Examination

Course Code: ITN1302 Set-A

Course Name: Wireless Networks

Time: 2 Hours

Max. Marks: 50

Instructions: Answer all the questions.

Section – A

10X01 = 10 Marks

Q1. What is the maximum data rate for the 802.11g standard?

A) 6Mbps

B) 11Mbps

C) 22Mbps

D) 54Mbps

Q2. What is the maximum data rate for the 802.11a standard?

A) 6Mbps

B) 11Mbps

C) 22Mbps

D) 54Mbps

Q3. You are connecting your access point and it is set to root. What does Extended Service Set ID mean?

A) That you have more than one access point and they are in the same SSID connected by a distribution system.

B) That you have more than one access point and they are in separate SSIDs connected by a distribution system.

C) That you have multiple access points, but they are placed physically in different buildings.

D) That you have multiple access points, but one is a repeater access point.

Q4. Which of the following does not come under the teleservices of GSM?

A) Standard mobile telephony

B) Mobile originated traffic

C) Base originated traffic

D) Packet switched traffic

Q5. Which of the following does not come under subsystem of GSM architecture?

A) BSS
B) NSS
C) OSS
D) Channel

Q6. Which of the following subsystem provides radio transmission between mobile station and MSC?

A) BSS
B) NSS
C) OSS
D) BSC

Q7. _____ manages the switching function in GSM.

A) BSS
B) NSS
C) OSS
D) MSC

Q8. An interconnected collection of piconet is called _____

A) scatternet
B) micronet
C) mininet
D) multinet

Q9. What is the frequency range of the IEEE 802.11a standard?

A) 2.4Gbps
B) 5Gbps
C) 2.4GHz
D) 5GHz

Q10. What is the frequency range of the IEEE 802.11b standard?

A) 2.4Gbps
B) 5Gbps
C) 2.4GHz
D) 5GHz

Section – B

04x04=16 Marks

Q11. What are IBSS and BSS?

Q12. What are three basic parameters to configure on a wireless access point?

Q13. Do I Need A License To Operate Wlans?

Q14. What is a Wi-Fi hotspot?

Section – C

04X06 = 24 Marks

Q15. Bluetooth Is Called A Cable Replacement Technology. Explain.

Q16. Explain The Following Terms: Icmp, Arp, Multicast, Broadcast

Q17. What Do You Mean By The Term Frequency-hopping Spread Spectrum (fhss)?

Q18. What Are The Different Modes Of An Access Point (ap) Operation?

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Set-A

Answer Key

School of Computing Skills

Session: 2020-21 (Summer Semester)

B. Voc. Program, 3rd Semester,

End-Sem. Examination

Answer key

Course Code: ITN1302 **Time: 2 Hours**

Course Name: Wireless Networks **Max. Marks: 50**

Instructions: Answer all the questions.

Section – A

10X01 = 10 Marks

Q1. What is the maximum data rate for the 802.11g standard?

A) 6Mbps

B) 11Mbps

C) 22Mbps

D) 54Mbps

Q2. What is the maximum data rate for the 802.11a standard?

A) 6Mbps

B) 11Mbps

C) 22Mbps

D) 54Mbps

Q3. You are connecting your access point and it is set to root. What does Extended Service Set ID mean?

A) That you have more than one access point and they are in the same SSID connected by a distribution system.

B) That you have more than one access point and they are in separate SSIDs connected by a distribution system.

C) That you have multiple access points, but they are placed physically in different buildings.

D) That you have multiple access points, but one is a repeater access point.

Q4. Which of the following does not come under the teleservices of GSM?

A) Standard mobile telephony

B) Mobile originated traffic

C) Base originated traffic

D) Packet switched traffic

Q5. Which of the following does not come under subsystem of GSM architecture?

A) BSS

B) NSS

C) OSS

D) Channel

Q6. Which of the following subsystem provides radio transmission between mobile station and MSC?

A) BSS
B) NSS
C) OSS
D) BSC

Q7. _____ manages the switching function in GSM.

A) BSS
B) NSS
C) OSS
D) MSC

Q8. An interconnected collection of piconet is called _____

A) scatternet
B) micronet
C) mininet
D) multinet

Q9. What is the frequency range of the IEEE 802.11a standard?

A) 2.4Gbps
B) 5Gbps
C) 2.4GHz
D) 5GHz

Q10. What is the frequency range of the IEEE 802.11b standard?

A) 2.4Gbps
B) 5Gbps
C) 2.4GHz
D) 5GHz

Section – B

04x04=16 Marks

Q11. What are IBSS and BSS?

Ans. Independent Basic Service Set (IBSS) allows two or more devices to communicate directly with each other without a need for a central device.

Basic Service Set (BSS) wireless LAN is established using a central device called an Access Point that centralizes access and control over a group of wireless devices.

Q12. What are three basic parameters to configure on a wireless access point?

Ans. 1. SSID
2. RF
3. Channel authentication method

Q13. Do I Need A License To Operate Wlans?

Ans. WLAN equipment operates in a 2.4 GHz and 5 GHz frequency spectrum which are license free. In the United States, spread spectrum devices fall under Federal Communications Commission (FCC) Part 15 of

the rules that govern unlicensed devices. However, other countries might require a license if you operate devices that are partially or completely outdoors, such as point-to-point bridges. In addition, some countries might require the system importer to obtain a telecommunications license to sell the product.

Q14. What is a Wi-Fi hotspot?

Ans. A hotspot is a physical location where people may obtain internet access, typically using wi-fi technology, via a wireless local area network (Wlan) using a router connected to an internet service provider.

Section – C

04X06 = 24 Marks

Q15. Bluetooth Is Called A Cable Replacement Technology. Explain.
Ans.

- Bluetooth allows Personal Area Networks without the cables.
- It provides connectivity to many mobiles users at a time for sharing without wires.
- Bluetooth chip is designed for replacing cables by transmitting the information at a special frequency from sender to receiver.
- Bluetooth is an inexpensive,low-power, short range radio based technology.
- Cabling involves a lot of cost foe execution.
- Bluetooth is much more flexible and robust than cabling.
- They even require a very low bandwidth of data transfer.

Q16. Explain The Following Terms: Icmp, Arp, Multicast, Broadcast
Answer :

- **Internet Control Message Protocol:** This protocol is used for while checking the connectivity using ping command
- **Address Resolution Protocol:** This protocol is used to know about the properties of TCP/IP. For example, to know other system MAC addresses.
- **Multicast:** Communication between single sender and a list of select recipients in a network.
- **Broadcast:** To send messages to all the recipients simultaneously in a network.

Q17. What Do You Mean By The Term Frequency-hopping Spread Spectrum (fhss)?
Ans :

- Flexibility and mobility are the growing reasons to use wireless LAN which uses radio frequencies for transmitting data. Wireless LANs are established for communicating with one another while on the go.
- The data transmitting on one frequency for a specific time limit and jumping randomly to another and transmitting again is the process in FHSS. The RF circuits can utilize class C amplification, efficient non-linear with a normal 1 MHz bandwidth.
- FHSS systems are better for use within indoors and in severe multipath environments. This is because of the frequency hopping scheme could defeat the multipath by hopping to a new frequency.

Q18. What Are The Different Modes Of An Access Point (ap) Operation?
Ans. An AP can be performed by one of these modes of operation:

- **Root Mode**— This is the actual AP mode. It can associate wireless clients and bridge the traffic to the wired network when needed.
- **Bridge Mode**— AP acts as a bridge and can be used to connect wired networks at a distance.
- **Repeater Mode**— When the Ethernet port is disabled, the AP becomes a repeater and associates to a nearby root AP.
- **Work Group Mode**— A Workgroup Bridge (WGB) can provide a wireless infrastructure connection for Ethernet-enabled devices. Devices that do not have a wireless client adapter in order to connect to the wireless network can be connected to the WGB through the Ethernet port. The WGB associates to the root AP through the wireless interface.

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Registration No : _____

SET-B

School of Computing Skills

Session: 2020-21 (Summer Semester)

B. Voc. Program, 3rd Semester,

End-Sem. Examination

Course Code: ITN1302 Set-B **Time: 2 Hours**

Course Name: Wireless Networks **Max. Marks: 50**

Instructions: Answer all the questions.

Section – A

10X01 = 10 Marks

Q1. What is the frequency range of the IEEE 802.11a standard?

A) 2.4Gbps

B) 5Gbps

C) 2.4GHz

D) 5GHz

Q2. What is the frequency range of the IEEE 802.11b standard?

A) 2.4Gbps

B) 5Gbps

C) 2.4GHz

D) 5GHz

Q3. What is the maximum data rate for the 802.11g standard?

A) 6Mbps

B) 11Mbps

C) 22Mbps

D) 54Mbps

Q4. What is the maximum data rate for the 802.11a standard?

A) 6Mbps

B) 11Mbps

C) 22Mbps

D) 54Mbps

Q5. You are connecting your access point and it is set to root. What does Extended Service Set ID mean?

A) That you have more than one access point and they are in the same SSID connected by a distribution system.

B) That you have more than one access point and they are in separate SSIDs connected by a distribution system.

C) That you have multiple access points, but they are placed physically in different buildings.

D) That you have multiple access points, but one is a repeater access point.

Q6. Which of the following does not come under the teleservices of GSM?
A) Standard mobile telephony
B) Mobile originated traffic
C) Base originated traffic
D) Packet switched traffic

Q7. Which of the following does not come under subsystem of GSM architecture?
A) BSS
B) NSS
C) OSS
D) Channel

Q8. Which of the following subsystem provides radio transmission between mobile station and MSC?
A) BSS
B) NSS
C) OSS
D) BSC

Q9. _____ manages the switching function in GSM.
A) BSS
B) NSS
C) OSS
D) MSC

Q10. An interconnected collection of piconet is called _____
A) scatternet
B) micronet
C) mininet
D) multinet

Section – B

04x04=16 Marks

Q11. What is a Wi-Fi hotspot?

Q12. What are IBSS and BSS?

Q13. What are three basic parameters to configure on a wireless access point?

Q14. Do I Need A License To Operate Wlans?

Section – C

04X06 = 24 Marks

Q15. What Are The Different Modes Of An Access Point (ap) Operation?

Q16. Bluetooth Is Called A Cable Replacement Technology. Explain.

Q17. Explain The Following Terms: Icmp, Arp, Multicast, Broadcast

Q18. What Do You Mean By The Term Frequency-hopping Spread Spectrum (fhss)?

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

SET B

Answer Key

School of Computing Skills

Session: 2020-21 (Summer Semester)

B. Voc. Program, 3rd Semester,

End-Sem. Examination

Course Code: ITN1302 Answer Key **Time: 2 Hours**

Course Name: Wireless Networks **Max. Marks: 50**

Instructions: Answer all the questions.

Section – A

10X01 = 10 Marks

Q1. What is the frequency range of the IEEE 802.11a standard?

A) 2.4Gbps

B) 5Gbps

C) 2.4GHz

D) 5GHz

Q2. What is the frequency range of the IEEE 802.11b standard?

A) 2.4Gbps

B) 5Gbps

C) 2.4GHz

D) 5GHz

Q3. What is the maximum data rate for the 802.11g standard?

A) 6Mbps

B) 11Mbps

C) 22Mbps

D) 54Mbps

Q4. What is the maximum data rate for the 802.11a standard?

A) 6Mbps

B) 11Mbps

C) 22Mbps

D) 54Mbps

Q5. You are connecting your access point and it is set to root. What does Extended Service Set ID mean?

A) **That you have more than one access point and they are in the same SSID connected by a distribution system.**

B) That you have more than one access point and they are in separate SSIDs connected by a distribution system.

C) That you have multiple access points, but they are placed physically in different buildings.

D) That you have multiple access points, but one is a repeater access point.

Q6. Which of the following does not come under the teleservices of GSM?

A) Standard mobile telephony
B) Mobile originated traffic
C) Base originated traffic
D) **Packet switched traffic**

Q7. Which of the following does not come under subsystem of GSM architecture?

A) BSS
B) NSS
C) OSS
D) Channel

Q8. Which of the following subsystem provides radio transmission between mobile station and MSC?

A) BSS
B) NSS
C) OSS
D) BSC

Q9. _____ manages the switching function in GSM.

A) BSS
B) NSS
C) OSS
D) MSC

Q10. An interconnected collection of piconet is called _____

A) scatternet
B) micronet
C) mininet
D) multinet

Section – B

04x04=16 Marks

Q11. What is a Wi-Fi hotspot?

Ans. A hotspot is a physical location where people may obtain internet access, typically using wi-fi technology, via a wireless local area network (Wlan) using a router connected to an internet service provider.

Q16. Bluetooth Is Called A Cable Replacement Technology. Explain.

Ans.

- Bluetooth allows Personal Area Networks without the cables.
- It provides connectivity to many mobiles users at a time for sharing without wires.
- Bluetooth chip is designed for replacing cables by transmitting the information at a special frequency from sender to receiver.
- Bluetooth is an inexpensive,low-power, short range radio based technology.
- Cabling involves a lot of cost foe execution.
- Bluetooth is much more flexible and robust than cabling.
- They even require a very low bandwidth of data transfer.

Q17. Explain The Following Terms: Icmp, Arp, Multicast, Broadcast

Answer :

- **Internet Control Message Protocol:** This protocol is used for while checking the connectivity using ping command
- **Address Resolution Protocol:** This protocol is used to know about the properties of TCP/IP. For example, to know other system MAC addresses.
- **Multicast:** Communication between single sender and a list of select recipients in a network.
- **Broadcast:** To send messages to all the recipients simultaneously in a network.

Q18. What Do You Mean By The Term Frequency-hopping Spread Spectrum (fhss)?

Ans :

- Flexibility and mobility are the growing reasons to use wireless LAN which uses radio frequencies for transmitting data. Wireless LANs are established for communicating with one another while on the go.
- The data transmitting on one frequency for a specific time limit and jumping randomly to another and transmitting again is the process in FHSS. The RF circuits can utilize class C amplification, efficient non-linear with a normal 1 MHz bandwidth.
- FHSS systems are better for use within indoors and in severe multipath environments. This is because of the frequency hopping scheme could defeat the multipath by hopping to a new frequency.

Q12. What are IBSS and BSS?

Ans. Independent Basic Service Set (IBSS) allows two or more devices to communicate directly with each other without a need for a central device.

Basic Service Set (BSS) wireless LAN is established using a central device called an Access Point that centralizes access and control over a group of wireless devices.

Q13. What are three basic parameters to configure on a wireless access point?

Ans. 1. SSID

2. RF

3. Channel authentication method

Q14. Do I Need A License To Operate Wlans?

Ans. WLAN equipment operates in a 2.4 GHz and 5 GHz frequency spectrum which are license free. In the United States, spread spectrum devices fall under Federal Communications Commission (FCC) Part 15 of the rules that govern unlicensed devices. However, other countries might require a license if you operate devices that are partially or completely outdoors, such as point-to-point bridges. In addition, some countries might require the system importer to obtain a telecommunications license to sell the product.

Section – C

04X06 = 24 Marks

Q15. What Are The Different Modes Of An Access Point (ap) Operation?

Ans. An AP can be performed by one of these modes of operation:

- **Root Mode**— This is the actual AP mode. It can associate wireless clients and bridge the traffic to the wired network when needed.
- **Bridge Mode**— AP acts as a bridge and can be used to connect wired networks at a distance.
- **Repeater Mode**— When the Ethernet port is disabled, the AP becomes a repeater and associates to a nearby root AP.
- **Work Group Mode**— A Workgroup Bridge (WGB) can provide a wireless infrastructure connection for Ethernet-enabled devices. Devices that do not have a wireless client adapter in order to connect to the wireless network can be connected to the WGB through the Ethernet port. The WGB associates to the root AP through the wireless interface.

Registration No.: .....

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

School of Computing Skills **Set A**

B. Voc. Program, Summer Semester (2020-21)

III Semester, End-Sem. Examination

Course Code: ITN1303 **Time: 2 Hours**

Course Name: Basics of Network Security **Max. Marks: 50**

Section – A

10x01 = 10 Marks

Q1. FTP server listens for connection on which port number?

a) 20 b) 21 c) 22 d) 23

Q2. What is the standard IANA port number used for requesting web pages?

a) 20 b) 80 c) 22 d) 23

Q3. Network layer firewall works as a _____

a) Frame filter b) Packet filter c) Content filter d) Virus filter

Q4. In asymmetric key cryptography, the private key is kept by _____.

a) sender b) receiver c) sender and receiver d) all the connected devices to the network

Q5. The attacker using a network of compromised devices is known as _____.

a) Internet b) Botnet c) Telnet d) D-net

Q6. Which of the following is a form of DoS attack?

a) Vulnerability attack b) Bandwidth flooding c) Connection flooding d) All of the mentioned

Q7. Which of the following is the type of software that has self-replicating software that causes damage to files and system?

a) Viruses b) Trojan horses c) Bots d) Worms

Q8. A port number is a _____.

a) 16-bit unsigned integer b) 16-bit signed integer c) 8-bit unsigned integer d) 8-bit signed integer

Q9. What is the most important activity in System Hacking?

a) Information Gathering b) Cracking Passwords c) Escalating Privileges d) Covering Tracks

Q10. Which of the following is a class of Computer Threat?

a) DoS Attacks b) Phishing c) Stalking d) Soliciting

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Section – B

04x04 = 16 Marks

Q1. What are the basics concepts of network security?

Q2. What is the purpose of port numbers in networking?

Q3. What is the difference between port 80 and port 443?

Q4. Describe the role of key in cryptography.

Section – C

04x06 = 24 Marks

Q1. What are the 3 types of port numbers? Explain. How do network ports work?

Q2. Describe, in brief following security services: Confidentiality, Data integrity, Authentication, Accountability, Availability.

Q3. Why is cyber security important to ports?

Q4. What is a Denial of service attack? Explain.

Registration No.: .....

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

School of Computing Skills **Set A**

B. Voc. Program, Summer Semester (2020-21)

III Semester, End-Sem. Examination

Course Code: ITN1303 Answer key **Time: 2 Hours**

Course Name: Basics of Network Security **Max. Marks: 50**

Section – A

10x01 = 10 Marks

Q1. FTP server listens for connection on which port number?

a) 20 **b) 21** c) 22 d) 23

Answer: b

Q2. What is the standard IANA port number used for requesting web pages?

a) 20 b) 80 c) 22 d) 23

Answer: b

Q3. Network layer firewall works as a _____

a) Frame filter b) Packet filter c) Content filter d) Virus filter

Answer: b

Q4. In asymmetric key cryptography, the private key is kept by _____.

a) sender b) receiver c) sender and receiver d) all the connected devices to the network

Answer: b

Q5. The attacker using a network of compromised devices is known as _____.

a) Internet b) Botnet c) Telnet d) D-net

Answer: b

Q6. Which of the following is a form of DoS attack?

a) Vulnerability attack b) Bandwidth flooding c) Connection flooding d) All of the mentioned

Answer: d

Q7. Which of the following is the type of software that has self-replicating software that causes damage to files and system?

a) Viruses b) Trojan horses c) Bots d) Worms

Answer: d

Q8. A port number is a _____.

a) 16-bit unsigned integer b) 16-bit signed integer c) 8-bit unsigned integer d) 8-bit signed integer

Answer: a

Q9. What is the most important activity in System Hacking?

a) Information Gathering b) Cracking Passwords c) Escalating Privileges d) Covering Tracks

Answer: b

Q10. Which of the following is a class of Computer Threat?

a) DoS Attacks b) Phishing c) Stalking d) Soliciting

Answer: a

Section – B

04x04 = 24 Marks

Q1. What are the basics concepts of network security?

Ans. Network security is the process of taking preventative measures to protect the underlying **networking** infrastructure from unauthorized access, misuse, malfunction, modification, destruction or improper disclosure. The Internet has undoubtedly become a huge part of our lives.

Q2. What is the purpose of port numbers in networking?

Ans. A port number is a way to identify a specific **process** to which an Internet or other network message is to be forwarded when it arrives at a server. For the Transmission Control Protocol and the User Datagram Protocol, a port number is a 16-bit integer that is put in the header appended to a message unit.

Q3. What is the difference between port 80 and port 443?

Ans. **Port 80** and **443** are **ports** generally associated with "the Internet". **Port 443**/HTTPS is the HTTP protocol over TLS/SSL. **Port 80**/HTTP is the World Wide Web. ... If web servers are being hosted, connections will be allowed inbound to those web servers.

Q4. Describe the role of key in cryptography.

Ans. One of the key role is confidentiality - information is only available to those who are supposed to have access to it. Encryption helps protect confidentiality of information transmitted over a network by (if it works as intended) making it difficult or impossible for someone who is not authorized to have the information to make sense of it if they intercept the information in transit. In cases of data stored on a network, if it is stored in encrypted form, it can make it difficult or impossible for an attacker to get anything useful from the encrypted file.

Section – C

05x10 = 50 Marks

Q1. What are the 3 types of port numbers? Explain. How do network ports work?

Well known ports are described by IANA as ports that generally "can only be used by system (or root) processes or by programs executed by privileged users." The ports in this range 0-1023 are registered with IANA. As well as being registered, these ports are also assigned a specific network protocol. Well known ports are usually used to make some kind of network connection using a specific protocol. For instance, the standard telnet port is 23.

One device issues a command to make a telnet connection to another device. The command will identify the protocol to be used. If a port number is not specified in the command, the IP stack of the operating system, will usually assume the Well Known Port number of 23. This number will be put into the packet that is sent to the other device. The device receiving this packet will see that the destination port is 23. At this point the operating system of the device will check the port number and should identify port 23 as the Well Known

Port for telnet. In fact, this may not happen, actually any port number can be used to make the telnet connection. The only requirement is that both devices are expecting the same protocol on the same port.

Examples of Common, Well Know Port Numbers Would Include:

- 21 FTP
- 23 Telnet
- ·25 SMTP
- 80 HTTP

Registered Ports: - IANA defines registered ports as ports that "can be used by ordinary user processes or programs executed by ordinary users." 2 These ports are available to any program wanting to use a specific port. If you send a packet to a network device, using a registered port, the operating system of that device should not decide that a registered port is dedicated to any specific protocol. IANA registers the port numbers in this range, but no common network protocol is assigned to them.

Dynamic Ports: - Dynamic ports are "unassigned and unregistered ports for private applications, client-side processes, or other processes that dynamically allocate port numbers". 1 IANA has this advice regarding the use of unassigned ports: "UNASSIGNED PORT NUMBERS SHOULD NOT BE USED". It is recommended that an application be sent to IANA to have a port number assigned. The port number should not be used until it is assigned.

Q2. Describe, in brief following security services: Confidentiality, Data integrity, Authentication, Accountability, Availability.

Ans: Confidentiality: This term covers two related concepts:

Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

• Integrity: This term covers two related concepts:

Data integrity: Assures that information and programs are changed only in a specified and authorized manner.

System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

• Availability: Assures that systems work promptly and service is not denied to authorized users. Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are as follows:

• Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

• Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after action recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

Q3. Why is cyber security important to ports?

A port is a complex cyber environment that encompasses both land and waterside activities and systems. As illustrated in Figure 3.1, and examined in more detail in Appendix A, a port comprises four main asset types (i.e. buildings, linear infrastructure, plant and machinery, and information and communications systems) that are used to provide a range of operational services and where technology plays an increasingly important role.

The loss, or compromise, of one or more of these assets has the potential to impact upon:

(a) The speed and efficiency at which the port can operate;
(b) The ability of the port to be able to safely carry out particular operations; and
(c) The health and safety of staff and other people impacted upon by the work activities being undertaken and to whom a duty of care is owed.

Further, the failure of an organisation to appreciate the structure and operation of its assets, systems and associated business processes can result in a number of undesirable situations, including:

(a) Accidental or inadvertent exposure of sensitive systems, applications or data to unauthorised users;
(b) Loss of resilience or system redundancy; and
(c) Emergent failure modes that result in the cascade or catastrophic failure of critical systems or processes.

Any of the types of failure described can also have significant financial and reputational consequences.

Q4. What is a Denial of service attack? Explain.

Ans. A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.
DoS attacks can cause the following problems:

1. Ineffective services
2. Inaccessible services
3. Interruption of network traffic

Registration No.: .....

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

School of Computing Skills **Set B**

B. Voc. Program, Summer Semester (2020-21)

III Semester, End-Sem. Examination

Course Code: ITN1303 **Time: 2 Hours**

Course Name: Basics of Network Security **Max. Marks: 50**

Section – A

10x01 = 10 Marks

Q1. Which one of the following is not an objective of network security?

a) Identification b) Access control c) Authentication d) Lock

Q2. Network layer firewall works as a _____

a) Frame filter b) Packet filter c) Content filter d) Virus filter

Q3. In asymmetric key cryptography, the private key is kept by _____.

a) sender b) receiver c) sender and receiver d) all the connected devices to the network

Q4. In cryptography, what is cipher?

a) algorithm for performing encryption and decryption b) encrypted message

c) decrypted message d) None of them

Q5. What is the most important activity in System Hacking?

a) Information Gathering b) Cracking Passwords c) Escalating Privileges d) Covering Tracks

Q6. FTP server listens for connection on which port number?

a) 20 b) 21 c) 22 d) 23

Q7. Which of the following is the type of software that has self-replicating software that causes damage to files and system?

a) Viruses b) Trojan horses c) Bots d) Worms

Q8. Which of the following is a program capable of continually replicating with little or no user intervention?

a) Virus b) Trojan horses c) Rootkit d) Worms

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Q9. What is the most important activity in System Hacking?

a) Information Gathering b) Cracking Passwords

c) Escalating Privileges d) Covering Tracks

Q10. Which one of the following is an example for public key algorithm?

a) DES b) RSA c) RC5 d) AES

Section – B

04x04 = 16 Marks

Q1. What is the purpose of port numbers in networking?

Q2. Describe the role of key in cryptography.

Q3. What is the difference between port 80 and port 443?

Q4. What is CIA? Explain.

Section – C

04x06 = 24 Marks

Q1. What are the important port numbers? Explain.

Q2. Why is cyber security important to ports?

Q3. Explain the symmetric and asymmetric encryption and give difference between symmetric and asymmetric encryption.

Q4. Give the differences between Viruses, Worms and Trojans.

Registration No.: .....

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

School of Computing Skills **Set B**

B. Voc. Program, Summer Semester (2020-21)

III Semester, End-Sem. Examination

Course Code: ITN1303 Answer key **Time: 2 Hours**

Course Name: Basics of Network Security **Max. Marks: 50**

Section – A

10x01 = 10 Marks

Q1. FTP server listens for connection on which port number?
a) 20 b) 21 c) 22 d) 23
Answer: b
Q2. Network layer firewall works as a _____
a) Frame filter b) Packet filter c) Content filter d) Virus filter

Answer: b
Q3. In asymmetric key cryptography, the private key is kept by _____.
a) sender b) receiver c) sender and receiver d) all the connected devices to the network
Answer: b

Q4. In cryptography, what is cipher?
a) algorithm for performing encryption and decryption b) encrypted message
c) decrypted message d) None of them
Answer: a
Q5. The attacker using a network of compromised devices is known as _____
a) Internet
b) Botnet
c) Telnet
d) D-net
Answer: b
Q6. The DoS attack, in which the attacker establishes a large number of half-open or fully open TCP connections at the target host is _____
a) Vulnerability attack
b) Bandwidth flooding
c) Connection flooding
d) UDP flooding

Q7. Which of the following is the type of software that has self-replicating software that causes damage to files and system?

a) Viruses b) Trojan horses c) Bots d) Worms

ANSWER: d

Q8. Which of the following is a program capable of continually replicating with little or no user intervention?

a) Virus b) Trojan horses c) Rootkit d) Worms

ANSWER: A

Q9. What is the most important activity in System Hacking?

a. Information Gathering
b. Cracking Passwords
c. Escalating Privileges
d. Covering Tracks

Q10. Which one of the following ports is used to connect to the Active Directory in Windows 2000?

a) 80 b) 445 c) **389** d) 149

Section – B

Attempt any 06 questions in this section. **04x04 = 24 Marks**

Q1. What is the purpose of port numbers in networking?

Ans. A port number is a way to identify a specific **process** to which an Internet or other network message is to be forwarded when it arrives at a server. For the Transmission Control Protocol and the User Datagram Protocol, a port number is a 16-bit integer that is put in the header appended to a message unit.

Q2. Describe the role of key in cryptography.

Ans. One of the key role is confidentiality - information is only available to those who are supposed to have access to it. Encryption helps protect confidentiality of information transmitted over a network by (if it works as intended) making it difficult or impossible for someone who is not authorized to have the information to make sense of it if they intercept the information in transit. In cases of data stored on a network, if it is stored in encrypted form, it can make it difficult or impossible for an attacker to get anything useful from the encrypted file.

Q3. What is the difference between port 80 and port 443?

Port 80 and **443** are **ports** generally associated with "the Internet". **Port 443**/HTTPS is the HTTP protocol over TLS/SSL. **Port 80**/HTTP is the World Wide Web. ... If web servers are being hosted, connections will be allowed inbound to those web servers.

Q4. What is CIA? Explain.

Ans: - CIA stands for Confidentiality, Integrity, and Availability. CIA is a model designed to guide the policies for information security in organizations.

Section – C

Registration No.: .....

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

05x10 = 50 Marks

Q1. What are the important port numbers? Explain.
Ans.

Notable well-known port numbers

Number	Assignment
20	File Transfer Protocol (FTP) Data Transfer
21	File Transfer Protocol (FTP) Command Control
22	Secure Shell (SSH) Secure Login
23	Telnet remote login service, unencrypted text messages
25	Simple Mail Transfer Protocol (SMTP) E-mail routing
53	Domain Name System (DNS) service
67, 68	Dynamic Host Configuration Protocol (DHCP)
80	Hypertext Transfer Protocol (HTTP) used in the World Wide Web
110	Post Office Protocol (POP3)
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol (IMAP) Management of digital mail
161	Simple Network Management Protocol (SNMP)
194	Internet Relay Chat (IRC)
443	HTTP Secure (HTTPS) HTTP over TLS/SSL

Q2. Why is cyber security important to ports?

A port is a complex cyber environment that encompasses both land and waterside activities and systems. As illustrated in Figure 3.1, and examined in more detail in Appendix A, a port comprises four main asset types (i.e. buildings, linear infrastructure, plant and machinery, and information and communications systems) that are used to provide a range of operational services and where technology plays an increasingly important role.

The loss, or compromise, of one or more of these assets has the potential to impact upon:

(a) The speed and efficiency at which the port can operate;
(b) The ability of the port to be able to safely carry out particular operations; and
(c) The health and safety of staff and other people impacted upon by the work activities being undertaken and to whom a duty of care is owed.

Further, the failure of an organisation to appreciate the structure and operation of its assets, systems and associated business processes can result in a number of undesirable situations, including:

(a) Accidental or inadvertent exposure of sensitive systems, applications or data to unauthorised users;
(b) Loss of resilience or system redundancy; and

(c) Emergent failure modes that result in the cascade or catastrophic failure of critical systems or processes.

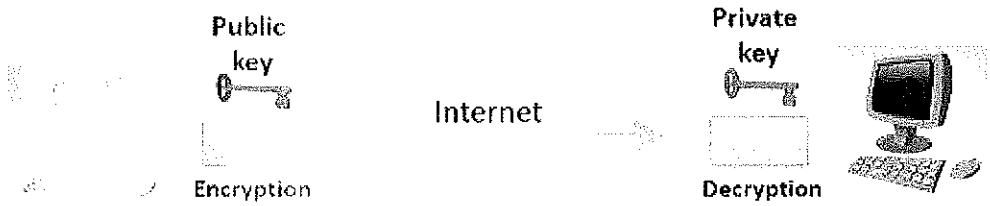
Any of the types of failure described can also have significant financial and reputational consequences.

Q3. Explain the symmetric and asymmetric encryption and give difference between symmetric and asymmetric encryption.

Ans: - Symmetric Encryption: - Symmetric encryption is a technique which allows the use of only one key for performing both the encryption and the decryption of the message shared over the internet. It is also known as the conventional method used for encryption. In symmetric encryption, the plaintext is encrypted and is converted to the ciphertext using a key and an encryption algorithm. While the cipher text is converted back to plain text using the same key that was used for encryption, and the decryption algorithm. The commonly used symmetric encryption algorithms are DES, 3 DES, AES, RC4.

Symmetric Encryption

Asymmetric encryption: - is an encryption technique that uses a pair of keys (private key and public key) for encryption and decryption. Asymmetric encryption uses the public key for the encryption of the message and the private key for the decryption of the message. The public key is freely available to anyone who is interested in sending the message. The private key is kept secret with the receiver of the message. Any message that is encrypted by the public key and the algorithm, is decrypted using the same the algorithm and the matching private key of corresponding public key. The most common asymmetric encryption algorithm are Diffie-Hellman and RSA algorithm.



Asymmetric Encryption

Key Differences between Symmetric and Asymmetric Encryption

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

BSDU

Symmetric encryption always uses a single key for encryption and decryption of the message. However, in asymmetric encryption, the sender uses the public key for the encryption and private key for decryption.

2. The execution of asymmetric encryption algorithms is slower as compared to the symmetric encryption algorithm. This is because the asymmetric encryption algorithms are more complex and has the high computational burden.
3. The symmetric encryption algorithms that are most commonly used are DES, 3DES, AES and RC4. On the other hand, Diffie-Hellman and RSA area the most common algorithm used for asymmetric encryption.
4. The asymmetric encryption is generally used for exchanging secret keys whereas, the symmetric encryption is used for exchanging a bulk of data.

Q4. Give the differences between Viruses, Worms and Trojans.

BASIS FOR COMPARISON	VIRUS	WORM	TROJAN HORSE
Meaning	A computer program that connects itself to another legitimate program to cause harm to the computer system or the network.	It eats resources of a system to bring it down rather than performing destructive actions.	It permits an intruder to obtain some confidential information about a computer network.
Execution	Depends on the transfer of a file.	Replicates itself without any human action.	Downloaded as software and executed.
Replication occurs	Yes	Yes	No
Remotely controlled	No	Yes	Yes
Rate of spreading	Moderate	Faster	Slow
Infection	Initiates by attaching a virus to an executable file.	Utilizes system or application weaknesses.	Attaches itself to a program and interpret as useful software.
Purpose	Modification of the information.	Halt the CPU and memory.	Steals the user's information.

Registration No.: .....

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Set – A

School of Computing Skills
B. Voc. Program, Summer Semester (2020-21)
III Semester, End-Sem. Examination

Course Code: ITN1305 **Time: 2 Hours**

Course Name: Optical Fiber Communication **Max. Marks: 50**

Section – A

10x01 = 10 Marks

Q1. Which one of the following is true for basic safety for good work habits?
a. Do not eat and drink in work area
b. Use tools for the jobs they were designed to perform
c. Keep a clean workspace
d. All are correct

Q2. Which one of the following strength member is used to construct an optical fiber cable?
a. Aramind yarns b. Plastic c. Glass d. Polyethylene

Q3. Which one of the following is the simplest optical fiber cable?
a. Simplex cordage b. Distribution cable c. Breakout cable d. Armored cable

Q4. Which one of the following cable is a convenient solution for space and weight problem?
a. Ribbon cable b. Distribution cable c. Breakout cable d. Armored cable

Q5. Which one of the following zone does not permit defects and scratches at endface?
a. Core b. cladding c. Epoxy ring d. Contact zone

Q6. Which one of the following is not a fiber optic connector component?
a. Cap b. Ferrule c. Core d. Strain relief boot

Q7. Which one of the following is the correct use of a cleaver?
a. To clean fiber
b. To remove residual coating
c. To cut the fiber and provide perpendicular finish
d. To provide non-reflective black surface

Q8. Which one of the following is the correct statement for a loose buffer tube?
a. It has an inner diameter much larger than that of the coated optical fiber
b. It has an inner diameter much smaller than that of the coated optical fiber
c. Its inner diameter is equal to the diameter of the coated optical fiber
d. It is directly applied to outer coating layer of the optical fiber

Q9. Which one of the following is a single fiber contact connector?
a. ST b. SMA c. FDDI d. BICONIC

Q10. Which one of the following effects is caused by optical fiber type mismatch?
a. Attenuation b. Back reflection c. Both are correct d. None of these

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Section – B 04x04 = 16 Marks

Q1. What is total internal reflection? Describe the core/cladding sizes of different optical fiber cables.

Q2. What are bending losses? Explain the different types of bending losses.

Q3. Write a short note on patch cord and pig tails.

Q4. Explain the basic operations of the eye loupe.

Section – C 04x06 = 24 Marks

Q1. Explain the use of the following pieces of test equipment:

Microscope, VFL, Fiber identifier, fusion splicer, Power meter.

Q2. How is a continuity tester used to locate the faults in a fiber cable? What are the drawbacks if a flashlight is used in place of the continuity tester? How does it differ from VFL?

Q3. Write the advantages and disadvantages of optical fibers.

Q4. What is OTDR? How does it work? Explain.

Set – A

School of Computing Skills
B. Voc. Program, Summer Semester (2020-21)

III Semester, End-Sem. Examination

Course Code: ITN1305 **Time: 2 Hours**

Course Name: Optical Fiber Communication **Max. Marks: 50**

Section – A

10x01 = 10 Marks

Q1. Which one of the following is true for basic safety for good work habits?
a. Do not eat and drink in work area
c. Keep a clean workspace
b. Use tools for the jobs they were designed to perform
d. All are correct

Q2. Which one of the following strength member is used to construct an optical fiber cable?
a. **Aramind yarns** b. Plastic c. Glass d. Polyethylene

Q3. Which one of the following is the simplest optical fiber cable?
a. **Simplex cordage** b. Distribution cable c. Breakout cable d. Armored cable

Q4. Which one of the following cable is a convenient solution for space and weight problem?
a. **Ribbon cable** b. Distribution cable c. Breakout cable d. Armored cable

Q5. Which one of the following zone does not permit defects and scratches at endface?
a. **Core** b. cladding c. Epoxy ring d. Contact zone

Q6. Which one of the following is not a fiber optic connector component?
a. Cap b. Ferrule **c. Core** d. Strain relief boot

Q7. Which one of the following is the correct use of a cleaver?
a. To clean fiber
c. **To cut the fiber and provide perpendicular finish**
b. To remove residual coating
d. To provide non-reflective black surface

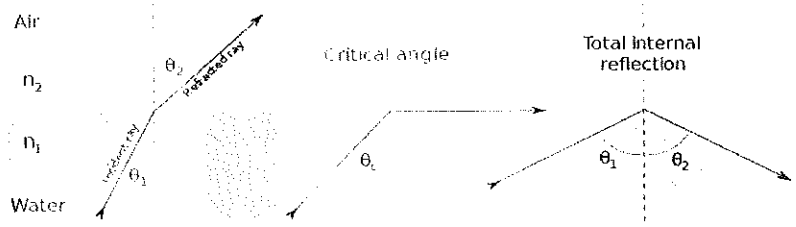
Q8. Which one of the following is the correct statement for a loose buffer tube?
a. **It has an inner diameter much larger than that of the coated optical fiber**
b. It has an inner diameter much smaller than that of the coated optical fiber
c. Its inner diameter is equal to the diameter of the coated optical fiber
d. It is directly applied to outer coating layer of the optical fiber

Q9. Which one of the following is a single fiber contact connector?
a. ST b. SMA c. FDDI d. BICONIC

Q10. Which one of the following effects is caused by optical fiber type mismatch?
a. Attenuation b. Back reflection c. **Both are correct** d. None of these

Section – B 04x04 = 16 Marks

Q1. What is total internal reflection? Describe the core/cladding sizes of different optical fiber cables.
Ans. **Total internal reflection (TIR)**



To consider the propagation of light within an optical fiber utilizing the ray theory model it is necessary to take account of the refractive index of the dielectric medium. The refractive index of a medium is defined as the ratio of the velocity of light in a vacuum to the velocity of light in the medium. A ray of light travels more slowly in an optically dense medium than in one that is less dense, and the refractive index gives a measure of this effect. When a ray is incident on the interface between two dielectrics of differing refractive indices (e.g. glass–air), refraction occurs, as illustrated in Figure 2.2(a). It may be observed that the ray approaching the interface is propagating in a dielectric of refractive index n1 and is at an angle φ 1 to the normal at the surface of the interface. If the dielectric on the other side of the interface has a refractive index n2 which is less than n1, then the refraction is such that the ray path in this lower index medium is at an angle φ 2 to the normal, where φ 2 is greater than φ 1. The angles of incidence φ 1 and refraction φ 2 are related to each other and to the refractive indices of the dielectrics by Snell's law of refraction, which states that:

$n1 \sin \varphi 1 = n2 \sin \varphi 2$

- Optical fiber cores are manufactured in different diameters for different applications. Typical glass cores range from as small as 3.7um up to 200um. Core sizes commonly used in telecommunications are **9um, 50um and 62.5um**. Plastic optical fiber cores can be much larger than glass. A popular plastic core size is 980um.

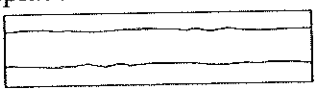
Q2. What are bending losses? Explain the different types of bending losses.
Ans. Bending loss

The loss which exists when an optical fiber undergoes bending is called bending losses.
Macrobending Loss
Macrobending happens when the fiber is bent into a large radius of curvature relative to the fiber diameter (large bends). These bends become a great source of power loss when the radius of curvature is less than several centimeters. Macrobend may be found in a splice tray or a fiber cable that has been bent. Macrobend won't cause significant radiation loss if it has

large enough radius. However, when fibers are bent below a certain radius, radiation causes big light power loss as shown in the figure below.

Microbending Loss

Microbendings are the small-scale bends in the core-cladding interface. These are localized bends can develop during deployment of the fiber, or can be due to local mechanical stresses placed on the fiber, such as stresses induced by cabling the fiber or wrapping the fiber on a spool or bobbin. Microbending can also happen in the fiber manufacturing process. It is sharp but microscopic curvatures that create local axial displacement of a few microns (um) and spatial wavelength displacement of a few millimeters.



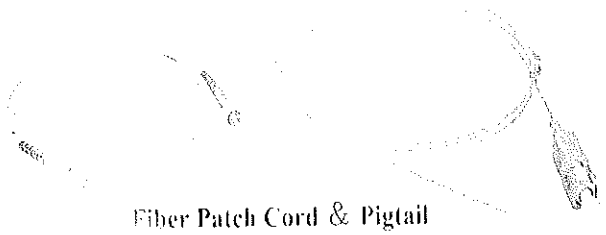
Because external forces are transmitted to the glass fiber through the polymer coating material, the coating material properties and dimensions, as well as external factors, such as temperature and humidity, affect the microbending sensitivity of a fiber.

Q3. Write a short note on patch cord and pig tails.

Ans.- **uctures of Fiber Patch Cords and Pigtails**

Fibe patch cord, also known as fiber optic patch cable or fiber jumper cable, is a sho th of optical fiber cable with a connector on each end. Connector types on eac of the fiber patch cable can be different and they can also be the same.

Fibe pigtail is a piece of cable terminated with a fiber optic connector at only one f the cable and leaves a length of exposed fiber at the other end, so that the lor side can link to the equipment and the other side can be melted with opti ble fibers or stripped and fusion spliced to a single fiber of a multi-fiber tru The following picture shows a fiber patch cord and a fiber pigtail.



Fiber Patch Cord & Pigtail

Fibe patch cords and pigtails structurally have much in common.

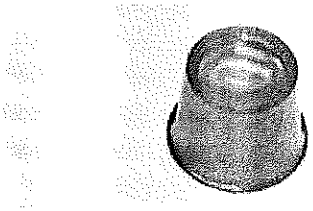
Q4. Explain the basic operations of the eye loupe.

Ans. Eye loupe

- Dirt particles on the connector endface are not the only cause of poor connector performance.

- Dirt anywhere on the connector ferrule or inside the connector receptacle can also cause poor performance. Occasionally epoxy that runs onto the side of the connector ferrule during oven curing goes unnoticed, preventing the connector ferrule from aligning properly in the connector receptacle or mating sleeve. This can result in a high-loss interconnection.
- It is a good idea to have an eye loupe in your tool bag.

- The eye loupe will allow you to spot small dirt or epoxy particles that may be on the connector ferrule. Excess epoxy needs to be removed from the connector ferrule before the connector is inserted into a receptacle. After the connector has been properly cleaned, it should be evaluated with an inspection microscope.



Section – C 04x06 = 24 Marks

Q1. Explain the use of the following pieces of test equipment:

Microscope, VFL, Fiber identifier, fusion splicer, Power meter.

Q2. How is a continuity tester used to locate the faults in a fiber cable? What are the drawbacks if a flashlight is used in place of the continuity tester? How does it differ from VFL?

Q3. Write the advantages and disadvantages of optical fibers.

Ans:
At fiber optics transmissions are light pulses instead of electrical voltage transitions. It encodes the ones and zeroes of a digital network transmission by turning on and off the light pulses of a laser light source, of a given wavelength, at very high frequencies. The light source is usually either a laser or some kind of light-emitting diode (LED). The light from the light source is flashed on and off in the pattern of the data being encoded. The light travels inside the fiber until the light signal gets to its intended destination and is read by an optical detector.

Advantages of optical fiber communication

Communication using an optical carrier wave guided along a glass fiber has a number of extremely attractive features,

(a) Enormous potential bandwidth. The optical carrier frequency yields a far greater potential transmission bandwidth than metallic cable systems (i.e. coaxial cable bandwidth typically around 20 MHz over distances up to a maximum of 10 km) or even millimeter wave radio systems (i.e. systems currently operating with modulation bandwidths of 700 MHz over a few hundreds of meters).

(b) Small size and weight. Optical fibers have very small diameters which are often no greater than the diameter of a human hair. Hence, even when such fibers are covered with protective coatings they are far smaller and much lighter than corresponding copper cables. This is a tremendous boon towards

the alleviation of duct congestion in cities, as well as allowing for an expansion of signal transmission within vehicles such as aircraft, satellites and even ships.

(c) Electrical isolation. Optical fibers which are fabricated from glass, or sometimes a plastic polymer, are electrical insulators and therefore, unlike their metallic counterparts, they do not exhibit earth loop and interface problems. Furthermore, this property makes optical fiber transmission ideally suited for communication in electrically hazardous environments as the fibers create no arcing or spark hazard at abrasions or short circuits.

(d) Immunity to interference and crosstalk. Optical fibers form a dielectric waveguide and are therefore free from electromagnetic interference (EMI), radio-frequency interference (RFI) etc. Hence the operation of an optical fiber communication system is unaffected by transmission through an electrically noisy environment and the fiber cable requires no shielding from EMI. Moreover, it is fairly easy to ensure that there is no optical interference between fibers and hence, unlike communication using electrical conductors, crosstalk is negligible, even when many fibers are cabled together.

(e) Signal security. The light from optical fibers does not radiate significantly and therefore they provide a high degree of signal security. Unlike the situation with copper cables, a transmitted optical signal cannot be obtained from a fiber in a noninvasive manner (i.e. without drawing optical power from the fiber). Therefore, in theory, any attempt to acquire a message signal transmitted optically may be detected. This feature is obviously attractive for military, banking and general data transmission (i.e. computer network) applications.

(f) Low transmission loss. The development of optical fibers over the last 20 years has resulted in the production of optical fiber cables which exhibit very low attenuation or transmission loss in comparison with the best copper conductors. Fibers have been fabricated with losses as low as 0.15 dB km^{-1} and this feature has become a major advantage of optical fiber communications. It facilitates the implementation of communication links with extremely wide optical repeater or amplifier spacing, thereby reducing both system cost and complexity. Together with the already proven modulation bandwidth capability of fiber cables, this property has provided a totally compelling case for the adoption of optical fiber communications in the majority of long-haul telecommunication applications, replacing not only copper cables, but also satellite communications, as a consequence of the avoidable delay incurred for voice transmission when using this latter approach.

(g) Ruggedness and flexibility. Although protective coatings are essential, optical fibers may be manufactured with very high tensile strengths. Perhaps surprisingly for a glassy substance, the fibers may also be bent to quite small radii or twisted without damage. Furthermore, cable structures have been developed which have proved flexible, compact and extremely rugged. Taking the size and weight advantage into account, these optical fiber cables are generally superior in terms of storage, transportation, handling and installation to corresponding copper cables, while exhibiting at least comparable strength and durability.

(h) System reliability and ease of maintenance. These features primarily stem from the low-loss property of optical fiber cables which reduces the requirement for intermediate repeaters or line amplifiers to boost the transmitted signal strength. Hence with fewer optical repeaters or amplifiers, system reliability is generally enhanced in comparison with conventional electrical conductor systems. Furthermore, the reliability of the optical components is no longer a problem with predicted lifetimes of 20 to 30 years being quite common. Both these factors also tend to reduce maintenance time and costs.

(i) Potential low cost. The glass which generally provides the optical fiber transmission medium is made from sand – not a scarce resource. So, in comparison with copper conductors, optical fibers offer the potential for low-cost line communication. Although over recent years this potential has largely been realized in the costs of the optical fiber transmission medium which for bulk purchases has become competitive with copper wires (i.e. twisted pairs), it has not yet been achieved in all the other component areas associated with optical fiber communications. For example, the costs of high-

performance semiconductor lasers and detector photodiodes are still relatively high, as well as some of those concerned with the connection technology (demountable connectors, couplers, etc.). Overall system costs when utilizing optical fiber communication on long-haul links, however, are substantially less than those for equivalent electrical line systems because of the low-loss and wideband properties of the optical transmission medium. The requirement for intermediate repeaters and the associated electronics is reduced, giving a substantial cost advantage. Although this cost benefit gives a net gain for long haul links, it is not always the case in short-haul applications where the additional cost incurred, due to the electrical–optical conversion (and vice versa), may be a deciding factor. Nevertheless, there are other possible cost advantages in relation to shipping, handling, installation and maintenance, which may prove significant in the system choice.

Disadvantages:

fiber-optic cabling does have a couple of disadvantages, including higher cost and a potentially more difficult installation in some cases.

Cost
It's ironic, but the higher cost of fiber-optic cabling has little to do with the cable these days. Increases in available fiber-optic cable–manufacturing capacity have lowered cable prices to levels comparable to high-end UTP on a per-foot basis, and the cables are no harder to pull. Modern fiber-optic connector systems have greatly reduced the time and labour required to terminate fiber. optical fiber offers connections in network topologies that can make the overall network cost lower than a traditional hierarchical star network wired with more copper cabling
(also see TIA's Fiber Optics LAN Section: www.fols.org).

Installation
Fiber-optic cabling can be more difficult to install. Copper-cable ends simply need a mechanical connection, and those connections don't have to be perfect. Fiber-optic cables can be much trickier to make connections for, mainly because of the nature of the glass or plastic core of the fiber cable. When you cut or cleave (in fiber-optic terms) the fiber, the unpolished end consists of an irregular finish of glass that diffuses the light signal and prevents it from guiding into the receiver correctly. The end of a fiber must be polished with a special polishing tool to make it perfectly flat so that the light signal shines through correctly. The polishing step adds extra time to the installation of cable ends and makes it a longer, and thus more expensive, cabling-plant installation.

Q4. What is OTDR? How does it work? Explain.

OTDR Theory
The OTDR is nothing more than a device that launches a pulse or pulses of light into one end of an optical fiber and records the amount of light energy that is reflected back. Unlike all the test equipment discussed up to this point, the OTDR provides a graphical representation of what is happening in the fiber-optic link or cable under test. With the OTDR, the fiber-optic link or cable is no longer a black box. The OTDR shows how light passes through every segment of the fiber optic link.
Light that is sent back in an optical fiber is the result of a reflection or backscatter. Reflections are caused when light traveling through the optical fiber encounters changes in the refractive index. These reflections are called Fresnel reflections. Backscatter, or Rayleigh scattering, results from randomly distributed compositional and density variations in the optical fiber. Photons are scattered along the length of the optical fiber. The photons that travel back to the OTDR are considered backscatter.

Registration No.: .....

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Set – B

School of Computing Skills
B. Voc. Program, Summer Semester (2020-21)
III Semester, End-Sem. Examination

Course Code: ITN1305 **Time: 2 Hours**

Course Name: Optical Fiber Communication **Max. Marks: 50**

Section – A

10x01 = 10 Marks

Q1. Which one of the following zone does not permit defects and scratches at endface?

a. Core b. cladding c. Epoxy ring d. Contact zone

Q2. Which one of the following is not a fiber optic connector component?

a. Cap b. Ferrule c. Core d. Strain relief boot

Q3. The joining of two cables is done by which one of the following methods?

a. OTDR b. Fusion splicing c. Connectors d. Termination

Q4. Which one of the following microscope capacity is required for single mode fiber inspection?

a. 100X b. 220X c. 400X d. 340X

Q5. Which one of the following is Not used as a light source for optical fiber?

a. LED b. LASER c. lamp d. None of these

Q6. Which one of the following effects is caused by optical fiber type mismatch?

a. Attenuation b. Back reflection c. Both are correct d. None of these

Q7. Which one of the following is the cable jacket color of SMF according to TIA-568-C?

a. Orange b. Yellow c. Slate d. Green

Q8. Which one of the following axis is used to displays distance in OTDR?

a. Horizontal axis b. Vertical axis c. No axis is used d. Both axis is used

Q9. Which one of the following can be used to detect infrared light traveling through an optical fiber?

a. OTDR b. Continuity tester c. Fiber identifier d. VFL

Q10. Which one of the following defines the core diameter for endface measurement for SMF?

a. 0 to 25 μm b. 25 to 120 μm c. 120 to 130 μm d. 130 to 250 μm

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Section – B

04x04 = 16 Marks

Q1. What is OTDR? How does it work?

Q2. What are bending losses? Explain the different types of bending losses.

Q3. List out the optical fiber safety rules.

Q4. Explain the basic operations of the Microscope.

Section – C

04x06 = 24 Marks

Q1. Describe different problems that can affect fiber optic cable networks.

Q2. How is a continuity tester used to locate the faults in a fiber cable? What are the drawbacks if a flashlight is used in place of the continuity tester? How does it differ from VFL?

Q3. Draw a cross-section of a fiber optic cable and explain the purpose of each segment. How does light propagate in it?

Q4. What is optical fiber communication? Write the advantages and disadvantages of optical fibers.

Registration No.: ..... CTB

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

School of computing Skills

B. Voc. Program, Summer Semester (2018-19)

III Semester, End-Sem. Examination

ITN1305 Optical Fiber Communication Answer Key **Time: 2 Hours**

Max. Marks: 100

Section – A

10x01 = 10 Marks

Q1. Which one of the following zone **does not permit defects and scratches at endface**?

a. **Core** b. cladding c. Epoxy ring d. Contact zone

Q2. Which one of the following **is not a fiber optic connector component**?

a. Cap b. Ferrule **c. Core** d. Strain relief boot

Q3. The joining of two cables in a long outside plant run is almost always done by which one of the following methods?

a. OTDR **b. Splicing** c. Connectors d. Termination

Q4. Which one of the following microscope capacity is required for single mode fiber inspection?

a. 100X b. 220X c. **400X** d. 340X

Q5. Which one of the following is Not used as a light source for optical fiber?

a. LED b. LASER **c. lamp** d. None of these

Q6. Which one of the following effects is caused by **optical fiber type mismatch**?

a. Attenuation b. Back reflection c. **Both are correct** d. None of these

Q7. Which one of the following is the **cable jacket color of Single Mode Fiber according to TIA-568-C**?

a. Orange **b. Yellow** c. Slate d. Green

Q8. Which one of the following axis is used to displays distance in OTDR?

a. **Horizontal axis** b. Vertical axis c. No axis is used d. Both axis is used

Q9. Which one of the following can be used to detect infrared light traveling through an optical fiber?

a. OTDR b. Continuity tester c. **Fiber identifier** d. VFL

Q10. Which one of the following defines the **core diameter for endface measurement for SMF**?

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Q10. Which one of the following defines the **core diameter for endface measurement for SMF**?

a. **0 to 25 µm** b. 25 to 120 µm c. 120 to 130 µm d. 130 to 250 µm

Section – B

04x04 = 16 Marks

Q1. What is OTDR? How does it work?

OTDR Theory

The OTDR is nothing more than a device that launches a pulse or pulses of light into one end of an optical fiber and records the amount of light energy that is reflected back. Unlike all the test equipment discussed up to this point, the OTDR provides a graphical representation of what is happening in the fiber-optic link or cable under test. With the OTDR, the fiber-optic link or cable is no longer a black box. The OTDR shows how light passes through every segment of the fiber optic link.

Light reflecting back in an optical fiber is the result of a reflection or backscatter. Reflections are when the light traveling through the optical fiber encounters changes in the refractive index. These reflections are called Fresnel reflections. Backscatter, or Rayleigh scattering, results from evenly distributed compositional and density variations in the optical fiber. Photons are scattered along the length of the optical fiber. The photons that travel back toward the OTDR are considered backscatter.

Q2. What are bending losses? Explain the different types of bending losses.

Bending loss

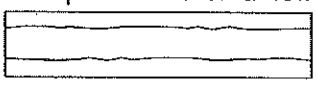
The loss which exists when an optical fiber undergoes bending is called bending losses.

Macrobending Loss

Macrobending happens when the fiber is bent into a large radius of curvature relative to the fiber diameter (large bends). These bends become a great source of power loss when the radius of curvature is less than several centimeters. Macrobend may be found in a splice tray or a fiber cable that has been bent. Macrobend won't cause significant radiation loss if it has large enough radius. However, when fibers are bent below a certain radius, radiation causes big light power loss as shown in the figure below.

Macrobend loss.

Microbending Loss

Microbendings are the small-scale bends in the core-cladding interface. These are localized bends can develop during deployment of the fiber, or can be due to local mechanical stresses placed on the fiber, such as stresses induced by cabling the fiber or wrapping the fiber on a spool or bobbin. Microbending can also happen in the fiber manufacturing process. It is sharp but microscopic curvatures that create local axial displacement of a few microns (um) and spatial wavelength displacement of a few millimeters. 

Because external forces are transmitted to the glass fiber through the polymer coating material, the coating material properties and dimensions, as well as external factors, such as temperature and humidity, affect the microbending sensitivity of a fiber.

Q3. List out the optical fiber safety rules.

Ans.

1. Keep all food and beverages out of the work area. If fiber particles are ingested they can cause internal hemorrhaging.

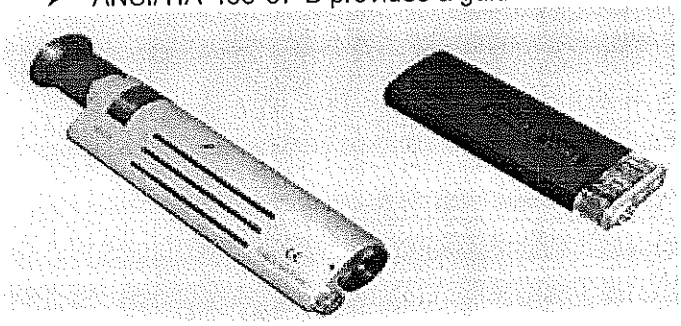
BHARTIYA SKILL DEVELOPMENT UNIVERSITY

2. Wear laboratory coat or disposable apron to minimize fiber particles on your clothing. Fiber particles can become lodged in clothing and can later get into food, drinks, and/or be ingested by other means. A coat also insures laboratory chemicals do not harm clothing.
3. Always wear safety glasses with side shields and protective gloves (particularly if the fibres have been treated with etching chemicals). Treat fiber optic splinters the same as you would glass splinters.
4. Never look directly into the end of fiber cables until you are positive that there is no light source at the other end. For optical light, look at the fibre from a distance first. For infrared light, use a fiber optic power meter to make certain the fiber is dark.
5. Only work in well ventilated areas if using chemicals to clean or process the fibres.
6. Do not touch your eyes or mouth while working with fiber optic systems until your hands have been thoroughly washed. Contact lens wearers must not handle their lenses until they have thoroughly washed their hands.
7. Keep all combustible materials safely away from the curing ovens.
8. Put all cut or broken fiber pieces in the yellow sharps bins for disposal.
9. Thoroughly clean your work area when you are done. Use adhesive tape to pick up any broken fibre pieces from surfaces to ensure no one leans on them or knocks them onto the floor.

Q4. Explain the basic operations of the Microscope.

Microscope

- The endface of a fiber-optic connector can only be properly evaluated with an inspection microscope.
- There are many different inspection microscopes are available in market. Typically, a multimode connector can be evaluated with a 100X microscope, while a single-mode connector requires a minimum of 200X magnification.
- A 400X microscope works even better for both multimode and single-mode.
- The smaller microscope is a 100X and the larger is a 400X.
- ANSI/TIA-455-57-B provides a guideline for examination of an optical-fiber endface.



Section – C

04x06 = 24 Marks

Q1. Describe different problems that can affect fiber optic cable networks.

Ans

Common fiber cable problems
There are a number of problems that can affect fiber optic cable networks. Many of the most common problems are outlined below.

Attenuation/decibel (dB) loss.

All network transmissions degrade over distance. This is called attenuation, or decibel (dB) loss. This loss of signal strength can lead to slower speeds, loss or corruption of network traffic, or loss of the network communication link. The OTDR can diagnose attenuation and can also help in the placement of a repeater station.

Highlights:

- All network transmissions degrade over distance—this is called attenuation or dB loss.
- The OTDR can diagnose attenuation and can help in the placement of a repeater station.

Broken fiber optic cable.

As is the case with all types of cable media, fiber optic cables are subject to breakage. As a matter of fact, in some cases, they are more delicate than other types of media. A common cause of breaks in fiber optic cables is exceeding the bend radius limitations of the cable. Due to the construction of fiber optic cable, it is subject to breakage if it is bent beyond a certain point. Certain types of fiber cable can span many kilometers, often making it difficult to determine where a break has occurred. An OTDR can be used to determine where a break in the fiber optic cable has occurred, allowing a technician to insert a splice at that point.

Highlights:

- As with all types of cable media, fiber optic cables are subject to breakage.
- An OTDR can be used to determine where a break in the fiber optic cable has occurred.

Bad small form-factor pluggable (SPF) or gigabit interface converter (GBIC) transceiver.

It is possible for small form-factor pluggable (SPF) transceivers or for gigabit interface converter (GBIC) transceivers to go bad. The SPF and GBIC transceivers are hot swappable replaceable modules that are used to add gigabit capabilities to switches, routers, and other networking equipment. A bad transceiver will prevent communication from occurring. An OTDR can be used to help diagnose a bad SPF or GBIC module.

Highlights:

- SPF and GBIC transceivers are hot swappable replaceable modules used to add gigabit capabilities to networking equipment.
- An OTDR can be used to help diagnose a bad SPF or GBIC module.

Fiber type mismatch.

It is also possible to have a fiber type mismatch. Single-mode fiber (SMF) and multimode fiber (MMF) use different methods for placing the signal on the optic fiber. If a mismatch occurs, the most common problem is that it will be impossible to make a network connection. This problem can also be referred to as a wavelength mismatch, as the wavelength, or the color of the light being used, is different between the modes of fiber transceivers. The OTDR can be used to determine the types of transceivers that are being used.

Highlights:

- SMF and MMF use different transceivers for placing the signal on the optic fiber.
- A wavelength mismatch will prevent a connection from being made.
- An OTDR can be used to determine the types of transceivers that are being used.

Other fiber optic cable issues.

There are some additional fiber optic cable issues that can arise. Anything that can interrupt the flow of light from transceiver to transceiver will create a problem. Dirt or smudges on the connectors may cause an issue with fiber optic cable transmissions. When this is suspected, using a soft polishing cloth to clean the ends of the cable will solve the problem. However, technicians should exercise

caution when doing so. It is important to never look directly into the ends of connected fiber optic cable, as eye damage can result.

Connectors are also specific to the mode of transmission, such as SMF or MMF. It is also important to check to make sure that the proper connectors are being used with the proper type of fiber optic cables. Connecting the wrong type of connector to a cable will prevent proper communication from occurring.

Worn or broken connectors will create an air gap, which will also create a network transmission problem. Connectors should always be inspected for their condition before being used. An OTDR can be used to determine where the loss of signal is occurring, even if it is at the connector.

Highlights:

- Anything that can interrupt the flow of light from transceiver to transceiver will create a problem.
    - Dirt or smudges on the connectors may cause an issue with fiber optic cable transmissions; a soft polishing cloth can be used to clean the ends of the cable.
    - Connectors are specific to mode of transmission—SMF or MMF.
    - Worn or broken connectors will create an air gap, which will create a network transmission problem; before using, always inspect connectors for their condition.

- An OTDR can be used to determine where the loss of signal is occurring.

Inspection and Evaluation

Good inspection and evaluation skills are essential for anyone attempting to troubleshoot a fiber-optic link or cable. Often the cause of a problem is basic and can be discovered with a thorough inspection. For many troubleshooting scenarios, expensive test equipment is not necessary.

Q2. How is a continuity tester used to locate the faults in a fiber cable? What are the drawbacks if a flashlight is used in place of the continuity tester? How does it differ from VFL?

Continuity Tester Fault Location Techniques

- The continuity tester is a basic and essential tool for every fiber-optic toolkit. It is also one of the least expensive tools in your toolkit. This low-cost tool will allow you to quickly verify the continuity of an optical fiber.
- The continuity tester is really no more than a flashlight. There are many different continuity testers on the market. Some use red LED light sources; others use incandescent lights.
- If you don't have a continuity tester, you can just use a flashlight. The job of the continuity tester is to project light into the core of the optical fiber.
- It has a receptacle at the end of the flashlight which centred and hold the connector ferrule directly above the LED or incandescent lamp. This eliminates the need for a lens to direct light into the core of the optical fiber. However, it directs only a fraction of the light emitted by the lamp or LED into the core of the optical fiber.
- The continuity tester works best with multimode optical fiber; however, it can be used with single-mode optical fiber. For best results with single-mode optical fiber, dim the lights in the test area if possible.
- LED continuity testers have a couple of advantages over incandescent lamp testers. They typically feature a red (635–650nm) LED that is easy to see. They require far less power from the batteries than an incandescent lamp. An LED continuity tester may provide 10 or more times longer battery life compared to an incandescent lamp.
- The first step when using the continuity tester is to clean and visually inspect the endface of the connector before inserting it into the continuity tester. You need to visually inspect the connector to verify that there is no endface damage. A shattered endface will significantly reduce the light coupled into the core of the optical fiber under test.

- After the connector has been cleaned and inspected, you need to verify that the continuity tester is operating properly. Turn the continuity tester on and verify that it is emitting light. (Check dead batteries of continuity tester)
- Depending on where the other end of the fiber-optic cable to be tested is located, you may need an assistant to help you.
- With the continuity tester turned on, insert the ferrule of the connector under test into the receptacle. If light is being emitted from the other end of the optical fiber, there is good continuity. This means only that there are no breaks in the optical fiber. This does not mean that there are no macro-bends or high-loss interconnections in the

fiber-optic cable or link under test.

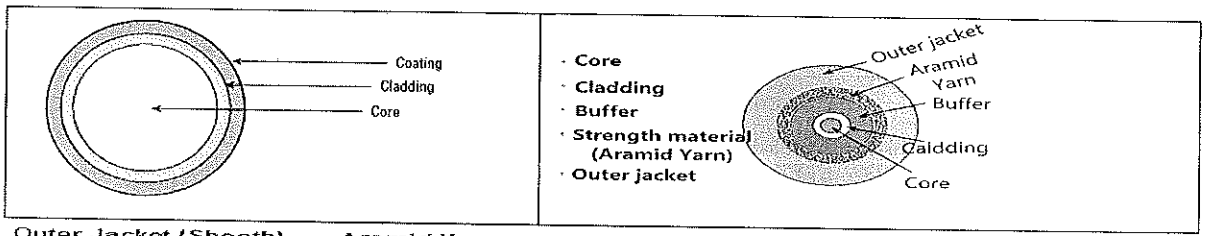
- The continuity tester is often used to verify that there are no breaks in a reel of fiber-optic cable before it is installed. There are a couple of ways you could approach testing the reel. One way would be to install a connector on either end of the cable. The other end of the cable should have the jacket and strength member stripped back so that the buffer is exposed. You should remove a small amount of buffer to expose the optical fiber under test. This will allow you to clearly see the light from the continuity tester, ensuring accurate results.
- Another approach is to use a pigtail with a mechanical splice or alignment sleeve. The pigtail would have a connector on one end that will mate with the continuity tester receptacle.

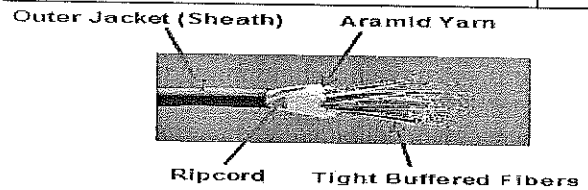
Visual Fault Locator

- Like the continuity tester, the *visual fault locator (VFL)* is an essential tool for every fiber-optic toolkit. Unlike the continuity tester, it is not one of the least expensive tools in your toolkit.
- The VFL will allow you to quickly identify breaks or macrobends in the optical fiber, and identify a poor fusion splice in multimode or single-mode optical fiber.
- The big difference between the continuity tester and the VFL is the light source and optical output power of the light source. The VFL typically uses a red (635–650nm) laser light source. The optical output power of the laser is typically 1mW or less. Because of the high optical output power, you should never view the output of the VFL directly.

Q3. Draw a cross-section of a fiber optic cable and explain the purpose of each segment. How does light propagate in it?

Optical fiber components-:





A typical optical fiber comprises three main components: the core, which carries the light; the cladding, which surrounds the core with a lower refractive index and contains the light; and the coating, which protects the fragile fiber within.

Core

- The *core*, which carries the light, is the smallest part of the optical fiber.
- The optical fiber core is usually made of glass, although some are made of plastic. The glass used in the core is extremely pure silicon dioxide (SiO2). In the manufacturing process, dopants such as germania, phosphorous pentoxide, or alumina are used to raise the refractive index under controlled conditions.
- Optical fiber cores are manufactured in different diameters for different applications. Typical glass cores range from as small as 3.7um up to 200um. Core sizes commonly used in telecommunications are **9um, 50um and 62.5um**. Plastic optical fiber cores can be much larger than glass. A popular plastic core size is 980um.

Cladding

- The *cladding* is surrounding the core and providing the lower refractive index to make the optical fiber work.
- When glass cladding is used, the cladding and the core are manufactured together from the same silicon dioxide-based material in a permanently fused state.
- The manufacturing process adds different amounts of dopants to the core and the cladding to maintain a difference in refractive indexes between them of about 1%.

Coating

- The *coating* is the true protective layer of the optical fiber.
- The coating absorbs the shocks, nicks, scrapes, and even moisture that could damage the cladding. Without the coating, the optical fiber is very fragile. A single microscopic nick in the cladding could cause the optical fiber to break when it's bent. Coating is essential for all-glass fibers, and they are not sold without it.
- The coating is solely protective. It does not contribute to the light-carrying ability of the optical fiber in any way. The outside diameter of the coating is typically either **250um or 500um.** Generally, the coating is colourless. In some applications, however, the coating is coloured, so that individual optical fibers in a group of optical fibers can be identified.

The coating found on an optical fiber is selected for a specific type of performance or environment. Once of the most common types of coating **is acrylate**. This coating is typically applied in two layers. The primary coating is applied directly on the cladding. This coating is soft and provides a cushion for the optical fiber when it is bent. The secondary coating is harder than the primary coating and provides a hard outer surface. Acrylate, however, is limited in temperature performance. A typical acrylate may perform at temperatures up to 125° C. **Silicone, carbon, and polyimide are** coatings that may be found on optical fibers that are used in harsh environments such as those associated with avionics, aerospace, and space. They may also be used on optical fibers designed for mining, or oil and gas drilling.

Safety Note: The tiny diameter of fiber strands makes them extremely dangerous. When stripped of their coating layer, as must be done for some splicing and connectorizing techniques, the strands can easily penetrate the skin. Shards, or broken pieces of strand, can even be carried by blood vessels to other parts of the body (or the brain). They are especially dangerous to the eye because small pieces can pierce the eyeball, doing damage to the eye's surface and possibly getting trapped inside. Safety glasses and special shard-disposal containers are a must when connecting or splicing fibers.

Buffer

The main function of the buffer is to protect the fiber from damage.

Jacket

Fiber optic cable's jackets are available in different colours that can easily make us recognize the exact colour of the cable we are dealing with. The colour yellow clearly signifies a single mode cable, and orange colour indicates multimode.

Cable Jacket Materials

1. **Polyethylene (PE)**

PE (black color) is the standard jacket material for outdoor fiber optic cables. PE has excellent moisture – and weather-resistance properties. It has very stable dielectric properties over a wide temperature range. It is also abrasion-resistant.

2. **Polyvinyl Chloride (PVC)**

PVC is the most common material for indoor cables; however, it can also be used for outdoor cables. It is flexible and fire-retardant. PVC is more expensive than PE.

3. **Polyvinyl difluoride (PVDF)**

PVDF is used for plenum cables because it has better fire-retardant properties than PE and produces little smoke.

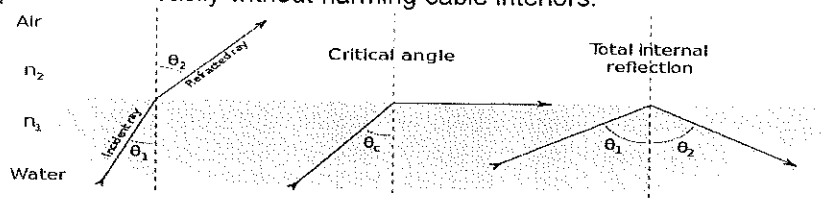
4. **Low Smoke Zero Halogen (LSZH) plastics**

LSZH plastics are used for a special kind of cable called LSZH cables. They produce little smoke and no toxic halogen compounds. But they are the most expensive jacket material.

Aramid Yarn Aramid yarn is a yellow color, fiber looking material. It is strong and is used to bundle and protect the loose tubes or fibers in the cable. It is the strength member to provide tensile strength along the length of the cable during and after installation. When a cable is pulled into a duct, the tension is applied to the aramid yarn instead of the fibers.

Central Strength Member Many fiber optic cables has a central strength member, made of steel, fiberglass or aramid yarn. Central strength members are needed to provide the rigidity to keep the cable from buckling. Central strength members are common in outdoor cables and some high fiber counts indoor cables.

Gel Compound Gel compound fills buffer tubes and cable interiors, making the cable impervious to water. It needs to be completely cleaned off when the cable end is stripped for termination.
Ripcord Ripcord is a thin but very strong thread embedded just below the cable jacket. Its role is to split the cable easily without harming cable interiors.



Q4. What is optical fiber communication? Write the advantages and disadvantages of optical fibers.

Advantages of optical fiber communication

Communication using an optical carrier wave guided along a glass fiber has a number of extremely attractive features,

(a) Enormous potential bandwidth. The optical carrier frequency yields a far greater potential transmission bandwidth than metallic cable systems (i.e. coaxial cable bandwidth typically around 20 MHz over distances up to a maximum of 10 km) or even millimeter wave radio systems (i.e. systems currently operating with modulation bandwidths of 700 MHz over a few hundreds of meters).

(b) Small size and weight. Optical fibers have very small diameters which are often no greater than the diameter of a human hair. Hence, even when such fibers are covered with protective coatings they are far smaller and much lighter than corresponding copper cables. This is a tremendous boon towards the alleviation of duct congestion in cities, as well as allowing for an expansion of signal transmission within mobiles such as aircraft, satellites and even ships.

(c) Electrical isolation. Optical fibers which are fabricated from glass, or sometimes a plastic polymer, are electrical insulators and therefore, unlike their metallic counterparts, they do not exhibit earth loop and interface problems. Furthermore, this property makes optical fiber transmission ideally suited for communication in electrically hazardous environments as the fibers create no arcing or spark hazard at abrasions or short circuits.

(d) Immunity to interference and crosstalk. Optical fibers form a dielectric waveguide and are therefore free from electromagnetic interference (EMI), radio-frequency interference (RFI) etc. Hence the operation of an optical fiber communication system is unaffected by transmission through an electrically noisy environment and the fiber cable requires no shielding from EMI. Moreover, it is fairly easy to ensure that there is no optical interference between fibers and hence, unlike communication using electrical conductors, crosstalk is negligible, even when many fibers are cabled together.

(e) Signal security. The light from optical fibers does not radiate significantly and therefore they provide a high degree of signal security. Unlike the situation with copper cables, a transmitted optical signal cannot be obtained from a fiber in a noninvasive manner (i.e. without drawing optical power from the fiber). Therefore, in theory, any attempt to acquire a message signal transmitted optically may be detected. This feature is obviously attractive for military, banking and general data transmission (i.e. computer network) applications.

(f) Low transmission loss. The development of optical fibers over the last 20 years has resulted in the production of optical fiber cables which exhibit very low attenuation or transmission loss in comparison with the best copper conductors. Fibers have been fabricated with losses as low as 0.15 dB km−1 and this feature has become a major advantage of optical fiber communications. It facilitates the implementation of communication links with extremely wide optical repeater or amplifier spacing, thus reducing both system cost and complexity. Together with the already proven modulation bandwidth capability of fiber cables, this property has provided a totally compelling case for the adoption of optical fiber communications in the majority of long-haul telecommunication applications, replacing not only copper cables, but also satellite communications, as a consequence of the very noticeable delay incurred for voice transmission when using this latter approach.

(g) Ruggedness and flexibility. Although protective coatings are essential, optical fibers may be manufactured with very high tensile strengths. Perhaps surprisingly for a glassy substance, the fibers may also be bent to quite small radii or twisted without damage. Furthermore, cable structures have

been developed which have proved flexible, compact and extremely rugged. Taking the size and weight advantage into account, these optical fiber cables are generally superior in terms of storage, transportation, handling and installation to corresponding copper cables, while exhibiting at least comparable strength and durability.

(h) System reliability and ease of maintenance. These features primarily stem from the low-loss property of optical fiber cables which reduces the requirement for intermediate repeaters or line amplifiers to boost the transmitted signal strength. Hence with fewer optical repeaters or amplifiers, system reliability is generally enhanced in comparison with conventional electrical conductor systems. Furthermore, the reliability of the optical components is no longer a problem with predicted lifetimes of 20 to 30 years being quite common. Both these factors also tend to reduce maintenance time and costs.

(i) Potential low cost. The glass which generally provides the optical fiber transmission medium is made from sand – not a scarce resource. So, in comparison with copper conductors, optical fibers offer the potential for low-cost line communication. Although over recent years this potential has largely been realized in the costs of the optical fiber transmission medium which for bulk purchases has become competitive with copper wires (i.e. twisted pairs), it has not yet been achieved in all the other component areas associated with optical fiber communications. For example, the costs of high-performance semiconductor lasers and detector photodiodes are still relatively high, as well as some of those concerned with the connection technology (demountable connectors, couplers, etc.). Overall system costs when utilizing optical fiber communication on long-haul links, however, are substantially less than those for equivalent electrical line systems because of the low-loss and wideband properties of the optical transmission medium. The requirement for intermediate repeaters and the associated electronics is reduced, giving a substantial cost advantage. Although this cost benefit gives a net gain for long haul links, it is not always the case in short-haul applications where the additional cost incurred, due to the electrical–optical conversion (and vice versa), may be a deciding factor. Nevertheless, there are other possible cost advantages in relation to shipping, handling, installation and maintenance, which may prove significant in the system choice.

Disadvantage-:

fiber-optic cabling does have a couple of disadvantages, including higher cost and a potentially more difficult installation in some cases.

Cost
It's ironic, but the higher cost of fiber-optic cabling has little to do with the cable these days. Increases in available fiber-optic cable–manufacturing capacity have lowered cable prices to levels comparable to high-end UTP on a per-foot basis, and the cables are no harder to pull. Modern fiber-optic connector systems have greatly reduced the time and labour required to terminate fiber. optical fiber offers some options in network topologies that can make the overall network cost lower than a traditional hierarchical star network wired with more copper cabling
(also see TIA's Fiber Optics LAN Section: www.fols.org).

Installation
Fiber-optic cabling can be more difficult to install. Copper-cable ends simply need a mechanical connection, and those connections don't have to be perfect. Fiber-optic cables can be much trickier to make connections for, mainly because of the nature of the glass or plastic core of the fiber cable. When you cut or cleave (in fiber-optic terms) the fiber, the unpolished end consists of an irregular finish of glass that diffuses the light signal and prevents it from guiding into the receiver correctly. The end of the fiber must be polished with a special polishing tool to make it perfectly flat so that the light will shine through correctly. The polishing step adds extra time to the installation of cable ends and amounts to a longer, and thus more expensive, cabling-plant installation.