BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Registration No.: .....

School of Computing Skills

Session: 2019-20 (Summer / Winter Semester)

B. Voc. Program, Third Semester,

End-Sem. Examination

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

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

Instruction: Read the questions carefully before answering.

Section – A

10X01 = 10 Marks

10 Objective type questions, each question carries 01 mark.

Q1. Conversion of digital signal to analog signal is A. Modulation B. Demodulation C. Encapsulation D. Bypass	Q2. A sine wave is defined by A. amplitude B. frequency C. Phase D. All of the above
Q3. Propagation time is equals to A. Distance/Propagation speed B. Propagation speed/Bandwidth C. Message size/ Bandwidth D. Bandwidth/Queuing time	Q4. Digital signals are represented in A. Sine Waves B. Levels C. Stages D. None of the above
Q5. If signal does not change at all, its frequency is A. Zero B. Maximum C. Infinite D. None of Above	Q6. A period of 100 ms in microseconds would be equals to A. 10^3us B. 10^5us C. 10^7us D. 10^9us
Q7. Term that refers to loss of strength of a signal is called A. attenuation B. distortion C. Noise D. Impairments	Q8. Unit that is used to express state of a signal is A. Kilograms B. Seconds C. Decibel D. Hertz

Q9. Bit rate is measured in A. Bits per Hertz B. Bits Per Second C. Nano seconds D. Pixels per second	Q10. Completion of one full pattern is called a A. period B. Cycle C. Frame D. Segment

Section – B

04X04 = 16 Marks

04 short answer type questions, each question carries 04 marks.

Q11. What are the four main parts of WLAN?

Q12. Explain The Following Terms: ICMP, ARP, Multicast, and Broadcast?

Q13. What is BSS, IBSS and ESS? Explain briefly.

Q14. What is Wi-Fi?

Section – C

04X06 = 24 Marks

04 Long type questions, each question carries 06 marks.

Q15. Write down the advantages and disadvantages of the WLAN.

Q16. What is the difference between 802.11a, 11b, 11g and 802.11n?

Q17. Explain CDMA, FDMA and TDMA?

Q18. What are some of the wireless applications?

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Registration No.: .....

School of Computing Skills

Session: 2019-20 (Summer / Winter Semester)

B. Voc. Program, Third Semester,

End-Sem. Examination

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

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

Ans1. A

Ans2. D

Ans3. A

Ans4. B

Ans5. A

Ans6. B

Ans7. A

Ans8. C

Ans9. A

Ans10. B

Ans1. There are four main parts of any WLAN. They are wireless client, access point, wireless bridge and antenna. Wireless client is any device, which are connected to the access point. It can be static or mobile. Access point is the Tx/Rx of Wi-Fi signal. Bridge is the point-to-point link to connect two different networks. Antenna is the radiating device, which radiates into free space.

Ans2.
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.

Ans3. The Basic Service Set (BSS) is the smallest building block of a WLAN. It is the coverage area of single access point. IBSS is independent basic service set. This term is used in adhoc networks and defines the coverage area of the network. ESS is extended service area and is the coverage of the multiple access points.

Ans4. Wi-Fi is a technology that uses radio waves to provide network connectivity. A wi-fi connection is established using a wireless adapter to create hotspots - areas in the vicinity of a wireless router that are connected to the network and allow users to access internet services. Once configured, Wi-Fi provides wireless connectivity to your devices by emitting frequencies between 2.4 GHz - 5 GHz, based on the amount of data on the network

Ans1.
Advantages:
Allow the same features as wired LANs, but without cable limitations.
Mobility
Reduce installation time/cost
Flexibility
May work inside buildings or between buildings
Disadvantages:
Need a transmission medium based on radio frequency (RF) ->
Electromagnetic spectrum is limited
Transmission rates are slower than in wired LANs
Security problems
Wireless networking and Mobile Computing, By Mulatu G. BsC in IT

Ans2. The difference between the 11a, 11b, 11g and 11n lies in terms of data rate, frequency of operation, distance coverage and more.

Modulation Scheme OFDM
Data Rate 6,9,12,18,24,36,48,54 Mbps
RF Carrier 5GHz
Bandwidth 20MHz
Distance covered(appox.)- 35m(indoor),120m(outdoor)

802.11b

Modulation scheme DSSS/CCK
Data rate 1,2,5.5 and 11 Mbps
RF Carrier 2.4Ghz
Distance covered(appox.)- 38m(indoor),140m(outdoor)
Refer CCK vs DSSS vs OFDM>> for more information.
802.11g

Modulation Scheme DSSS/CCK and OFDM both
Data Rate support of both 11b and 11a
RF Carrier 2.4GHz
Bandwidth 20 MHz
Distance covered(appox.)- 38m(indoor),140m(outdoor)
802.11n

Modulation Scheme OFDM and DSSS/CCK
It supports legacy fallbacks of 11a/11b/11g systems
Bandwidth 20MHz and 40MHz

Data rate -As per 11a/11b/11g.
-It supports upto about 72Mbps for 20MHz bandwidth with multiple antennas
-It supports upto about 150Mbps for 40MHz bandwidth with multiple antennas
Distance covered(appox.)- 70m(indoor),250m(outdoor)
MIMO configuration -Most of the devices uses 2T3R(2 antennas in transmit and 3 antennas in receive),
Maximum configuration goes upto 4T4R.

Ans3.

CDMA :

- Same frequency is used by every user and simultaneous transmission occurs
- Every narrowband signal is multiplied by wideband spreading signal, usually known as code word
- Every user has a separate pseudo-code word, i.e., orthogonal to others
- Only the desired code word is detected by the receivers and others appear as noise
- It is mandatory for the receivers to know about the transmitter's code word

FDMA :

- When the channel is not in use, it sits simply idle.
- Bandwidth of Channel is relatively narrow (30 KHz), known as narrowband system.
- Little or no equalization is needed for spreading symbol time.
- Analog links are suitable for FDMA.
- Framing or synchronization bits are not needed for continuous transmission.
- Tight filtering is needed to minimize interference.

TDMA:

- Receiving or transmission is allowed for only one user in a given slot
- All slots are assigned cyclically
- The transmission is non-continuous
- It is essential to use digital data and modulation
- Data rate overhead is between 20% – 30%
- Overhead trade-offs are size of data payload and latency
- Multiple users are shared with single carrier frequency
- Handoff is made simpler by using non-continuous transmission
- All slots are assigned on demand
- Due to reduced inter user interference, the power control is less stringent.

Ans4.

A. Vehicles
Transmission of news, road condition, weather, music via DAB
Personal communication using GSM position via GPS
Emergencies
Just imagine the possibilities of an ambulance with a high-quality wireless connection to a hospital.
Vital information about injured persons can be sent to the hospital from the scene of the accident.

C. Business
Travelling salespersons

Direct access to customer files stored in a central location/company's database:
to ensure that files on his or her laptop reflect the current situation,
to enable the company to keep track of all activities of their travelling employees,
to keep databases consistent etc.
consistent databases for all agents
mobile office

Entertainment and more
Internet everywhere? Not without wireless networks!
Imagine a travel guide for a city.
Static information might be loaded via CD-ROM, DVD, or even at home via the Internet.
But wireless networks can provide up-to-date information at any appropriate location.

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Registration No.: .....

School of Computing Skills

Session: 2019-20 (Summer Semester)

B. Voc. Program, 3rd Semester,

End-Sem. Examination

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

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

Instruction: Answer All Questions

Section – A

10X01 = 10 Marks

Q1. What is the standard IANA port number used for requesting web pages?

a) 80
b) 21
c) 53
d) 25

Q2. When a person is harassed repeatedly by being followed, called the target of?

a) Bullying
b) Identity theft
c) Stalking
d) Phishing

Q3. We don't want our packets to get lost in transit. Which OSI layer is responsible for ordered delivery of packets?

a) Network layer
b) Data-Link layer
c) Transport layer
d) Physical layer

Q4. Which one of the following is a type of social engineering?

a) Shoulder surfing
b) User identification
c) System monitoring
d) Face-to-face communication

Q5. Which one of the following is a class of computer threats?

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

Q6. Which of the following pieces of information can be found in the IP header?

a) Source address of the IP packet
b) Destination address for the IP packet
c) Sequence number of the IP packet
d) Both (A) and (B) only.

Q7. Which of the following is a class of Computer Threat?

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

Q8. In the handshake protocol which is the message type first sent between client and server?

a) Server hello
b) Client hello
c) Hello request
d) Certificate request

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 Malicious Program Do Not Replicate Automatically?

a) Trojan Horse
b) Virus
c) Worm
d) Zombie

Section – B

04X04 = 16 Marks

Q1. What is a denial of service attack? Explain.

Q2. What are the possible results of an attack on a computer network?

Q3. Why are internal threats usually more effective than external threats?

Q.4 What should be our University's password policy?

Section – C

04X06 = 24 Marks

Q1.Ashish while back, the BSDU got a number of complaints that one of our campus computers was sending out Viagra spam. He checked it out, and the reports were true: a hacker had installed a program on the computer that made it automatically send out tons of spam email without the computer owner's knowledge. How do you think the hacker got into the computer to set this up?

Q2. What is CIA? Explain.

Q3. Explain DDOS attack and how to prevent it?

Q4.Explain the symmetric and asymmetric encryption and give difference between symmetric and asymmetric encryption.

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Registration No.: .....

School of Computing Skills

Session: 2019-20 (Summer Semester)

B. Voc. Program, 3rd Semester,

End-Sem. Examination

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

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

Instruction: Answer All Questions

Section – A

10X01 = 10 Marks

Q1. What is the standard IANA port number used for requesting web pages?

a) 80
c) 53
b) 21
d) 25

Q2. When a person is harassed repeatedly by being followed, called the target of?

a) Bullying
c) Stalking
b) Identity theft
d) Phishing

Q3. . We don't want our packets to get lost in transit. Which OSI layer is responsible for ordered delivery of packets?

a) Network layer
c) Transport layer
b) **Data-Link layer**
d) Physical layer

Q4. Which one of the following is a type of social engineering?

a) **Shoulder surfing**
c) System monitoring
b) User identification
d) Face-to-face communication

Q5. Which one of the following is a class of computer threats?

a) Phishing
c) Soliciting
b) **DoS attacks**
d) Stalking

Q6. Which of the following pieces of information can be found in the IP header?

a) Source address of the IP packet
c) Sequence number of the IP packet
b) Destination address for the IP packet
d) Both (A) and (B) only.

Q7. Which of the following is a class of Computer Threat?

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

Q8. In the handshake protocol which is the message type first sent between client and server?

a) Server hello
c) Hello request
b) **Client hello**
d) Certificate request

Q9. What Is the Most Important Activity in System Hacking?

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

Q10. Which Of The Following Malicious Program Do Not Replicate Automatically?

a) Trojan Horse
c) Worm
b) Virus
d) Zombie

Section – B

04X04 = 16 Marks

Q1. 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
4. Connection interference

Q2. What are the possible results of an attack on a computer network?

Ans: - Possible results include:

- Loss or corruption of sensitive data that is essential for a company's survival and success
- Diminished reputation and trust among customers
- The decline in value with shareholders
- Reduced brand value
- Reduction in profits

Q3. Why are internal threats usually more effective than external threats?

Ans: - Internal threats are potential threat actors who are members of the organization. They have access to computers and network resources of the organization and can misuse their access to perform malicious actions. This can include stealing on sensitive information, installing malware or causing denial of service.

From a detection perspective internal actors are less monitored. An organization puts a certain amount of trust on its employees and their actions are expected to match the interests of the organization. This trust is misused by the employees to perform malicious activity.

For example, a developer might have permission to create and run new programs which has access to critical data of the organization. The developer can choose to develop and run a program which copies and sends this data to a competing actor. The actions of the developer might look benign. After all, he is pulling the data and processing it as he usually does, but since the organization lacks complete visibility, the developer is able to do the unauthorized access. The organization can choose to have more visibility into what each user is doing. But this will result is too much alerts, analyzing which becomes expensive.

Q.4 What should be our University's password policy?

Ans: - A password policy should require that a password:

1. Be at least 8 characters long
2. Contain both alphanumeric and special characters
3. Change every 60 days
4. Cannot be reused after every five cycles
5. Is locked out after 3 failed attempts In addition, you should be performing regular password auditing to check the strength of passwords; this should also be documented in the password policy.

Section – C

04X06 = 24 Marks

Q.1 Ashish while back, the BSDU got a number of complaints that one of our campus computers was sending out Viagra spam. He checked it out, and the reports were true: a hacker had installed a program on the computer that made it automatically send out tons of spam email without the computer owner's knowledge. How do you think the hacker got into the computer to set this up?

Ans: - This was actually the result of a hacked password. Using passwords that can't be easily guessed, and protecting your passwords by not sharing them or writing those down can help to prevent this. Passwords should be at least 8 characters in length and use a mixture of upper and lower case letters, numbers, and symbols.

Even though in this case it was a hacked password, other things that could possibly lead to this are:

- Out of date patches/updates
- No anti-virus software or out of date anti-virus software

Q2. 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.

Confidentiality is almost equivalent to privacy. Computer networks must ensure confidentiality to mitigate attacks in order to avoid sensitive information from falling into wrong hands. Confidentiality is ensured by implementing access restriction mechanisms. Confidentiality can be understood as ensuring user privacy in the system.

Integrity refers to maintaining consistency, accuracy, and trust of data over its entire lifecycle. It must be understood that data is vulnerable during transit and steps must be taken to ensure that data during transit cannot be modified by unauthorized people, thus compromising confidentiality. There are many methods to ensure data integrity, for example, the use of cryptographic checksums to verify the data integrity. Also, measures such as backup and redundant storage may be required to restore lost data immediately.

Availability refers to the entire network with resources and hardware infrastructure is available to authorized users. Availability is ensured by maintaining all hardware is working well and carrying out repairs immediately, also availability is needed to maintain a fully functional operating system which is free of software conflicts. It is also important to perform necessary upgrades, software patches, and security patches as and when they are available from the vendor.

Hence, adequate precautions and safeguards to protect all information in the computer network must be planned and security procedures must be implemented to ensure uninterrupted network services.

Q3. Explain DDOS attack and how to prevent it?

Ans: - A DDOS (Distributed Denial of Service) attack is a cyberattack that causes the servers to refuse to provide services to genuine clients. DDOS attack can be classified into two types:

Flooding attacks: In this type, the hacker sends a huge amount of traffic to the server which the server cannot handle. And hence, the server stops functioning. This type of attack is usually executed by using automated programs that continuously send packets to the server.

Crash attacks: In this type, the hackers exploit a bug on the server resulting in the system to crash and hence the server is not able to provide service to the clients.

You can prevent DDOS attacks by using the following practices:

- Use Anti-DDOS services
- Configure Firewalls and Routers

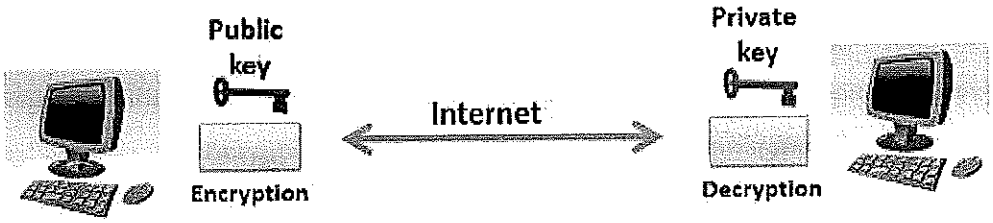
- Use Front-End Hardware
- Use Load Balancing
- Handle Spikes in Traffic

Q4. 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

1. 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.

The asymmetric encryption is generally used for exchanging secret keys whereas, the symmetric encryption is used for exchanging a bulk of data.

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Registration No.: .....

School of Computing Skills

Session: 2019-20 (Summer Semester)

B. Voc. Program, 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 **NOT** used as a light source for optical fiber?

a. LED b. LASER c. Flash light d. None of these

Q2. The OTDR displays amplitude in _____on the _____ axis.

a. dB, vertical b. dBm, horizontal c. dBm, vertical d. dB, horizontal

Q3. 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

Q4. Which one of the following is attached to pulling eye?

a. Outer jacket b. Strength member c. Fiber d. Armor

Q5. When is a splice enclosure used?

a. Whenever a fiber has been spliced
b. When a splice must be placed underground
c. When a splice must be placed underwater
d. Splice enclosures are optional.

Q6. Which part of the connector holds the fiber in place?

a. Ferrule b. Cap c. Boot d. Body

Q7. Intrinsic factors in connector performance are determined by:

a. Precision and geometry of the ferrule end
b. Construction of the connector and the fiber itself
c. Relationship of the fiber to the connector
d. The type of connector being used

Q8. Which geometry of the connector and fiber end ensures an Angled Physical Contact (APC) finish?

a. Flat b. Rough c. Curved d. None

Q9. Which one of the following explains the structure of breakout cables?

a. Tightly bundled tight-buffered cables
b. Fibers in a loose tube buffer
c. Simplex cables grouped around a central strength member
d. A mix of loose tube and tight-buffered fibers

Q10. Which one of the following is primary advantage of ribbon cable?

a. Strength b. Small size c. Low cost d. Fire resistance

Section – B

04X04 = 16 Marks

Q1. Explain how the color coding is used to identify individual cables.

Q2. What is TIR? Explain how it helps in propagation of signal at optical fiber.

Q3. What is the difference between plenum and riser cables?

Q4. What is the principle of OTDR? Explain.

Section – C

04X06 = 24 Marks

Q1. How is a continuity tester used to locate the faults in a fiber cable? What are the drawbacks if a flash light

is used in place of the continuity tester? How does it differ from VFL?

Q2. What are the most common optical fiber cable problems?

Q3. Explain the different steps for terminating epoxy and polished SC connectors.

Q4. What is the principle of optical Fiber? What are the advantage and disadvantage of optical fiber? Explain.

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Registration No.: .....

School of Computing Skills

Session: 2019-20 (Summer Semester)

B. Voc. Program, 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 **NOT** used as a light source for optical fiber?

a. LED b. LASER c. Flash light d. None of these

b.

Q2. The OTDR displays amplitude in _____on the _____ axis.

a. dB, vertical b. dBm, horizontal c. dBm, vertical d. dB, horizontal

a

Q3. 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

d

Q4. Which one of the following is attached to pulling eye?

a. Outer jacket b. Strength member c. Fiber d. Armor

b.

Q5. When is a splice enclosure used?

a. Whenever a fiber has been spliced
b. When a splice must be placed underground
c. When a splice must be placed underwater
d. Splice enclosures are optional.

Q6. Which part of the connector holds the fiber in place?

a. Ferrule b. Cap c. Boot d. Body

Q7. Intrinsic factors in connector performance are determined by:

a. Precision and geometry of the ferrule end
b. Construction of the connector and the fiber itself
c. Relationship of the fiber to the connector
d. The type of connector being used

Q8. Which geometry of the connector and fiber end ensures an Angled Physical Contact (APC) finish?

a. Flat b. Rough c. Curved d. None

Q9. Which one of the following explains the structure of breakout cables?

a. Tightly bundled tight-buffered cables
b. Fibers in a loose tube buffer
c. Simplex cables grouped around a central strength member
d. A mix of loose tube and tight-buffered fibers

Q10. Which one of the following is primary advantage of ribbon cable?

a. Strength b. Small size c. Low cost d. Fire resistance

Section – B

04X04 = 16 Marks

Q1. Explain how the color coding is used to identify individual cables.

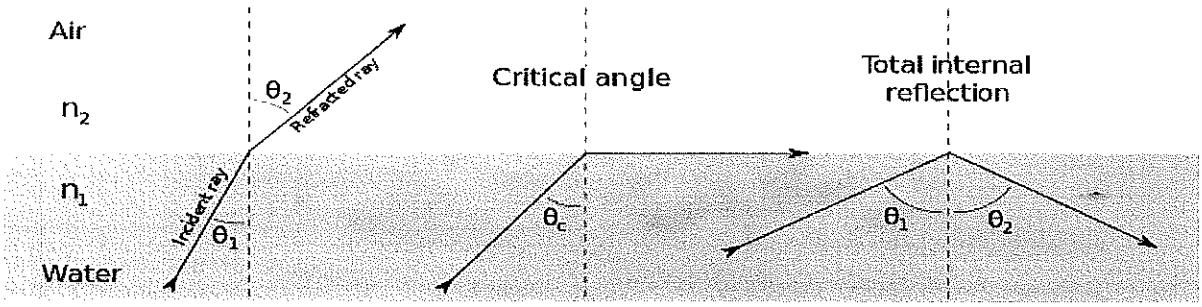
Inside the cable or inside each tube in a loose tube cable, individual fibers will be colour coded for identification. Fibers follow the convention created for telephone wires except fibers are identified individually, not in pairs. For splicing, like colour fibers are spliced to ensure continuity of colour codes throughout a cable run.

Table 1 - Individual fiber, unit, and group identification

Position #	Base color/tracer per TIA/EIA	Abbreviation/print legend
1	Blue	1 or BL or 1-BL
2	Orange	2 or OR or 2-OR
3	Green	3 or GR or 3-GR
4	Brown	4 or BR or 4-BR
5	Slate	5 or SL or 5-SL
6	White	6 or WH or 6-WH
7	Red	7 or RD or 7-RD
8	Black	8 or BK or 8-BK
9	Yellow	9 or YL or 9-YL
10	Violet	10 or VI or 10-VI
11	Rose	11 or RS or 11-RS
12	Aqua	12 or AQ or 12-AQ

Q2. What is TIR? Explain how it helps in propagation of signal at optical fiber.

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:

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

The light refracts through core and does not travel on taking n1 lesser than n2.

Q3. What is the difference between plenum and riser cables?

A plenum is a building space, compartment, duct or chamber used for air flow or to form part of an air distribution system. A plenum is a space used to move air to workspaces for the purpose of ventilation, heating or cooling. The informal words for plenums are "air duct" and "air return". The cable used in these areas are plenum cable.
A riser is a floor opening, shaft, or duct that runs vertically through one or more floors. Riser cable is intended for use in vertical shafts that run between floors. Many buildings have a series of equipment rooms that are placed vertically in a reinforced shaft for the purpose of enclosing power distribution equipment, HVAC units, telephone distribution and other utility services throughout the building. The cable used in these areas are riser cable.

Q4. What is the principle of OTDR? Explain.
Definition: OTDR is an acronym used for **O**ptical **T**ime **D**omain **R**eflectometer. It is an **instrument that is used to detect or analyze the scattered or back reflected light** through an optical fiber due to impurities and imperfections in the fiber. The operating principle of an OTDR is similar to that of radar. **OTDR performs timed measurements of reflected light.**

OTDR basically determines the characteristics of an optical fiber cable through which optical signal propagates.

It is also used to evaluate parameters such as splice losses, reflectance angle of a light signal, fiber attenuation etc.
When a signal is transmitted through an optical fiber cable then during transmission some part of the signal gets reflected. This reflection results in signal attenuation that mainly occurs due to defects in the fiber cable.

Thus, an OTDR is used as **testing equipment** in optical fiber communication system in order to determine the signal loss level inside a fiber cable.

Section – C

04X06 = 24 Marks

Q1. 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?

- 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.

Q2. What are the most common optical fiber cable problems?

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.

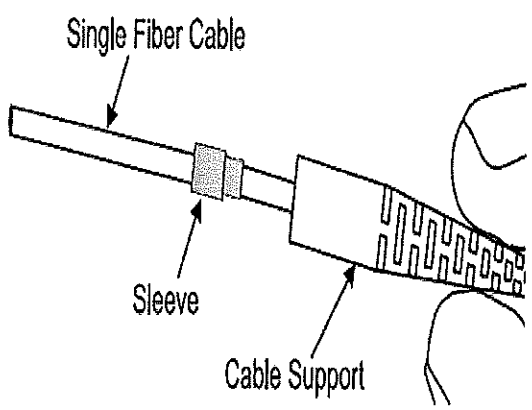
- An OTDR can be used to determine where the loss of signal is occurring.

Q3. Explain the different steps for terminating epoxy and polished SC connectors.

Step 1: Cable and fiber preparation

1. Place cable support (rubber boot) and crimp sleeve onto fiber cable

Slip the cable support (rubber boot) and the crimp sleeve onto the fiber cable.

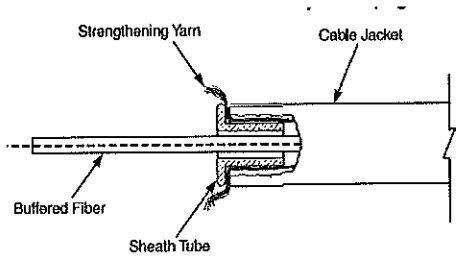


2. Measure and mark cable

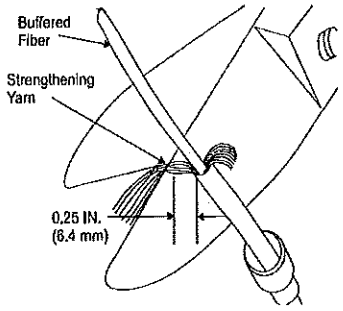
3. Remove outer jacket

4. Insert sheath tube into cable jacket

For 3mm cable, insert the sheath tube over the buffer fiber and into the cable jacket



5. Trim strength member (Kevlar)



6. **Measure and mark buffered fiber**

Measure and mark the buffered fiber 19mm (0.75 inch) from the end of the buffered fiber.

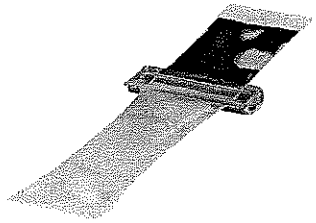
7. Remove buffer and fiber coating

8. Set aside prepared cable

Step 2: Epoxy preparation

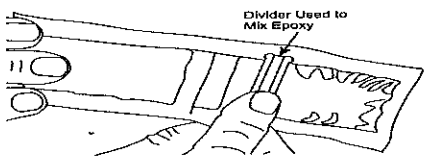
1. Remove epoxy divider

This is a two-part epoxy separated with a divider. The divider must be removed to allow the epoxy to be mixed.



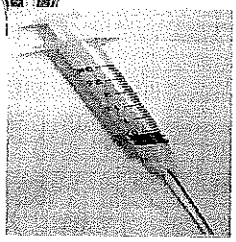
2. Mix the epoxy

Using the divider, thoroughly mix the epoxy until both parts are blended into a smooth, uniform color



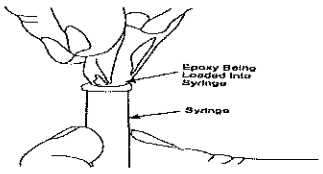
3. Install the syringe tip

Place the syringe tip onto the syringe and twist to lock it in place. Then remove the plunger to allow the mixed epoxy to be loaded into the syringe.



4. Pour mixed epoxy into syringe

Fold the epoxy package in half, cut the corner of the package, and squeeze the mixed epoxy into the syringe.



Replace the plunger in the syringe.

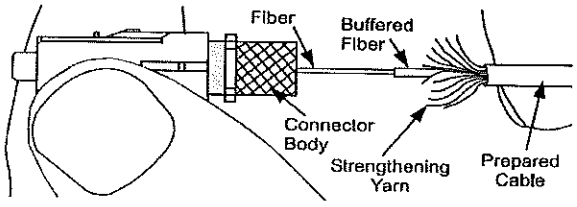
5. Remove air from syringe

Remove air pockets from the syringe by holding the syringe tip upward and ejecting epoxy until the air pockets are removed.

Step 3: Connector installation

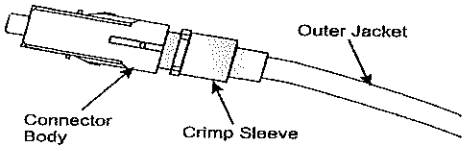
1. **Inject epoxy into connector body-**

2. Insert fiber into connector body



3. Install cable sleeve

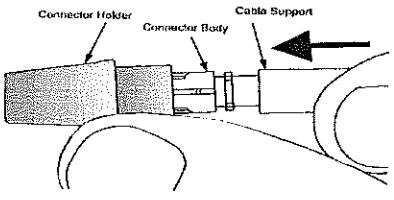
Slip the cable sleeve (crimp sleeve) over the outer jacket and the connector body to capture the Kevlar yarn between the connector body and sleeve.



4. Secure crimp sleeve

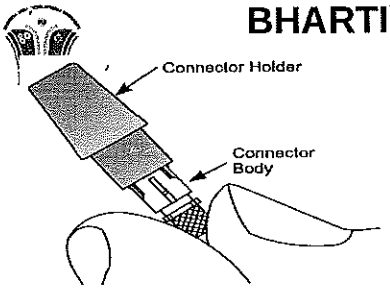
5. Install cable support (rubber boot)

Push the cable support (rubber boot) over the crimp sleeve and onto the connector body.



6. Install connector holder

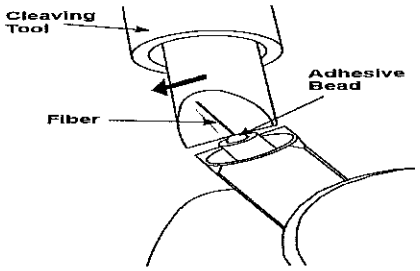
Place the connector body in a connector holder.



Step 4: Cure the epoxy

Step 5: Cleave fiber and polish connector ends

1. Cleave the fiber

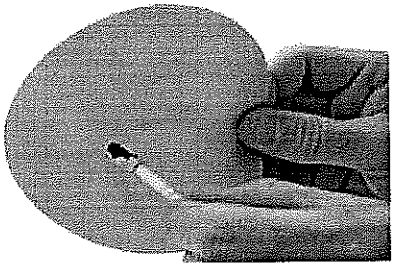


2. Pull away the fiber stub

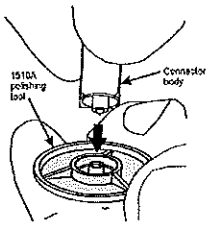
3. Prepare polishing material

4. Prepare polishing tool

5. Air polish the cleaved fiber



6. Insert connector into polishing tool (polishing puck)



7. First polish - single mode and multimode connectors

Step 6: Inspection

Q4. What is the principle of optical Fiber? What are the advantage and disadvantage of optical fiber? Explain.

Fiber Optics Technology

- The need for transporting data faster and over longer distances led to the development of new technologies.
- Using photons instead of electrons for signal transmission through cables allows much higher bandwidths at much lower costs.

- The advantages of fiber optic cables come from the fact, that glass is an isolator. No disturbing energy fields are emitted or absorbed. Glass has very little attenuation, which is independent of the modulation frequency. Compared to a copper cable of same transmission capability, the optic fiber is much smaller and lighter in weight.
- It is much cheaper even when considering all necessary driving devices and installation costs.

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

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.