LEARNER GUIDE

Describe data communications

Unit Standard 14947

Level 3 Credits 4

&

Describe Synchronous/ Asynchronous Communication with computers

Unit Standard 14932

Level 4 Credits 7

TABLE OF CONTENTS

PERSONAL INFORMATION

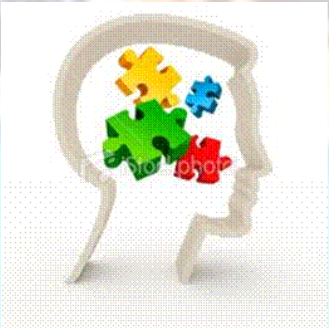
NAME	
CONTACT ADDRESS	
Code	
Telephone (H)	
Telephone (W)	
Cellular	
Learner Number	
Identity Number	

EMPLOYER	
EMPLOYER CONTACT ADDRESS	
Code	
Supervisor Name	
Supervisor Contact Address	
Code	
Telephone (H)	
Telephone (W)	
Cellular	

INTRODUCTION

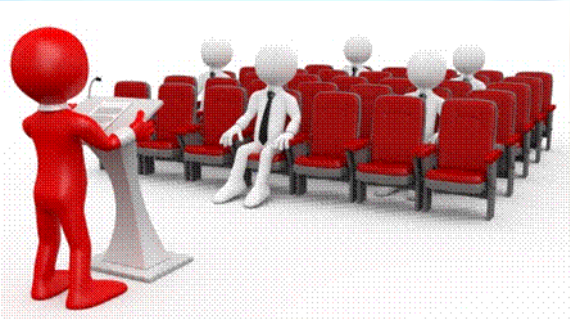
Welcome to the learning programme

Follow along in the guide as the training practitioner takes you through the material. Make notes and sketches that will help you to understand and remember what you have learnt. Take notes and share information with your colleagues. Important and relevant information and skills are transferred by sharing!



This learning programme is divided into sections. Each section is preceded by a description of the required outcomes and assessment criteria as contained in the unit standards specified by the South African Qualifications Authority. These descriptions will define what you have to know and be able to do in order to be awarded the credits attached to this learning programme. These credits are regarded as building blocks towards achieving a National Qualification upon successful assessment and can never be taken away from you!

Programme methodology



The programme methodology includes facilitator presentations, readings, individual activities, group discussions and skill application exercises.

Know what you want to get out of the programme from the beginning and start applying your new skills immediately. Participate as much as possible so that the learning will be interactive and stimulating.

The following principles were applied in designing the course:

- ✓ Because the course is designed to maximise interactive learning, you are encouraged and required to participate fully during the group exercises
- ✓ As a learner you will be presented with numerous problems and will be required to fully apply your mind to finding solutions to problems before being presented with the course presenter's solutions to the problems
- ✓ Through participation and interaction the learners can learn as much from each other as they do from the course presenter
- ✓ Although learners attending the course may have varied degrees of experience in the subject matter, the course is designed to ensure that all delegates complete the course with the same level of understanding
- ✓ Because reflection forms an important component of adult learning, some learning resources will be followed by a self-assessment which is designed so that the learner will reflect on the material just completed.

This approach to course construction will ensure that learners first apply their minds to finding solutions to problems before the answers are provided, which will then maximise the learning process which is further strengthened by reflecting on the material covered by means of the self-assessments.

Different role players in delivery process

- ✓ Learner
- ✓ Facilitator
- ✓ Assessor
- ✓ Moderator

What Learning Material you should have

This learning material has also been designed to provide the learner with a comprehensive reference guide.

It is important that you take responsibility for your own learning process; this includes taking care of your learner material. You should at all times have the following material with you:

Learner Guide 	***This learner guide is your valuable possession:*** This is your textbook and reference material, which provides you with all the information you will require to meet the exit level outcomes. During contact sessions, your facilitator will use this guide and will facilitate the learning process. During contact sessions a variety of activities will assist you to gain knowledge and skills.

	Follow along in the guide as the training practitioner takes you through the material. Make notes and sketches that will help you to understand and remember what you have learnt. Take and share information with your colleagues. Important and relevant information and skills are transferred by sharing! This learning programme is divided into sections. Each section is preceded by a description of the required outcomes and assessment criteria as contained in the unit standards specified by the South African Qualifications Authority. These descriptions will define what you have to know and be able to do in order to be awarded the credits attached to this learning programme. These credits are regarded as building blocks towards achieving a National Qualification upon successful assessment and can never be taken away from you!
Formative Assessment Workbook 	The Formative Assessment Workbook supports the Learner Guide and assists you in applying what you have learnt. The formative assessment workbook contains classroom activities that you have to complete in the classroom, during contact sessions either in groups or individually. You are required to complete all activities in the Formative Assessment Workbook. The facilitator will assist, lead and coach you through the process. These activities ensure that you understand the content of the material and that you get an opportunity to test your understanding.

Different types of activities you can expect

To accommodate your learning preferences, a variety of different types of activities are included in the formative and summative assessments. They will assist you to achieve the outcomes (correct results) and should guide you through the learning process, making learning a positive and pleasant experience.

The table below provides you with more information related to the types of activities.

Types of Activities	***Description***	***Purpose***
Knowledge Activities 	You are required to complete these activities on your own.	These activities normally test your understanding and ability to apply the information.
Skills Application Activities 	You need to complete these activities in the workplace	These activities require you to apply the knowledge and skills gained in the workplace
Natural Occurring Evidence 	You need to collect information and samples of documents from the workplace.	These activities ensure you get the opportunity to learn from experts in the industry. Collecting examples demonstrates how to implement knowledge and skills in a practical way

Learner Administration

Attendance Register

You are required to sign the Attendance Register every day you attend training sessions facilitated by a facilitator.

Programme Evaluation Form

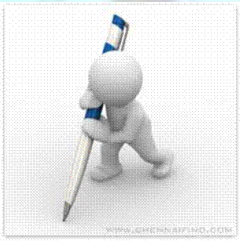
On completion you will be supplied with a "Learning programme Evaluation Form". You are required to evaluate your experience in attending the programme.

Please complete the form at the end of the programme, as this will assist us in improving our service and programme material. Your assistance is highly appreciated.

Assessments

The only way to establish whether a learner is competent and has accomplished the specific outcomes is through the assessment process. Assessment involves collecting and interpreting evidence about the learners' ability to perform a task.

To qualify and receive credits towards your qualification, a registered Assessor will conduct an evaluation and assessment of your portfolio of evidence and competency.
This programme has been aligned to registered unit standards. You will be assessed against the outcomes as stipulated in the unit standard by completing assessments and by compiling a portfolio of evidence that provides proof of your ability to apply the learning to your work situation.



How will Assessments commence?

Formative Assessments

The assessment process is easy to follow. You will be guided by the Facilitator. Your responsibility is to complete all the activities in the Formative Assessment Workbook and submit it to your facilitator.

Summative Assessments

You will be required to complete a series of summative assessments. The Summative Assessment Guide will assist you in identifying the evidence required for final assessment purposes. You will be required to complete these activities on your own time, using real life projects in your workplace or business environment in preparing evidence for your Portfolio of Evidence. Your Facilitator will provide more details in this regard.

To qualify and receive credits towards your qualification, a registered Assessor will conduct an evaluation and assessment of your portfolio of evidence and competency.

Learner Support

The responsibility of learning rests with you, so be proactive and ask questions and seek assistance and help from your facilitator, if required.

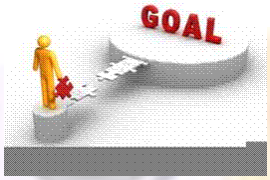
Please remember that this Skills Programme is based on outcomes based education principles which implies the following:

- ✓ You are responsible for your own learning – make sure you manage your study, research and workplace time effectively.
- ✓ Learning activities are learner driven – make sure you use the Learner Guide and Formative Assessment Workbook in the manner intended, and are familiar with the workplace requirements.
- ✓ The Facilitator is there to reasonably assist you during contact, practical and workplace time for this programme – make sure that you have his/her contact details.

- ✓ You are responsible for the safekeeping of your completed Formative Assessment Workbook and Workplace Guide
- ✓ If you need assistance please contact your facilitator who will gladly assist you.
- ✓ If you have any special needs please inform the facilitator

Learner Expectations

Please prepare the following information. You will then be asked to introduce yourself to the instructor as well as your fellow learners



Your name:
The organisation you represent:
Your position in organisation:
What do you hope to achieve by attending this course / what are your course expectations?

UNIT STANDARD 14947

Unit Standard Title

Describe data communications

NQF Level

3

Credits

4

Purpose

This unit standard is intended:

- ✓ to provide fundamental knowledge of the areas covered
- ✓ for those working in, or entering the workplace in the area of Data Communication & Networking
- ✓ as additional knowledge for those wanting to understand the areas covered

Learning assumed to be in place

The credit value of this unit standard is calculated assuming a person has the prior knowledge and skills to:

- ✓ Demonstrate an understanding of fundamental mathematics (at least NQF level 1).
- ✓ Demonstrate PC competency skills (End-User Computing unit Standards, at least up to NQF level 3.)
- ✓ Demonstrate competence to resolve technical computer problems (DC301/ 302).

Specific Outcomes and Assessment Criteria

Specific Outcome 1: Describe past, present and emerging developments in data communication

Assessment Criteria

- ✓ The description explains the origin of current data communications with an outline of past developments.
- ✓ The description provides a taxonomy for current systems.
- ✓ The description identifies and projects trends from emerging developments in data communications.

Specific Outcome 2: Describe synchronous and asynchronous data communications.

Assessment Criteria

- ✓ The description outlines the characteristics of each form of data communication.
- ✓ The description explains the features of data communication equipment with respect to synchronous and asynchronous data communication.

Critical Cross-field Outcomes (CCFO)

- ✓ Organise and manage him/her self and his/her activities responsibly and effectively.
- ✓ Collect, analyse, organise, and critically evaluate information.
- ✓ Use science and technology effectively and critically, showing responsibility towards the environment and health of others.
- ✓ Contribute to his/her full personal development and the social and economic development of the society at large by being aware of the importance of: reflecting on and exploring a variety of strategies to learn more effectively, exploring education and career opportunities and developing entrepreneurial opportunities.

UNIT STANDARD 14932

Unit Standard Title

Describe Synchronous/ Asynchronous Communication with computers

NQF Level

4

Credits

7

Purpose

This unit standard is intended:

- ✓ To provide a fundamental knowledge of the areas covered.
- ✓ For those working in, or entering the workplace in the area of Systems Support.
- ✓ As additional knowledge for those wanting to understand the areas covered.

The performance of all elements is to a standard that allows for further learning in this area

Learning assumed to be in place

The credit value of this unit is based on a person having prior knowledge and skills to:

- ✓ Demonstrate an understanding of fundamental mathematics (at least NQF level 3).

- ✓ Demonstrate PC competency skills (End-User Computing unit Standards, at least up to NQF level 3.)

Specific Outcomes and Assessment Criteria

Specific Outcome 1: Describe past, present and emerging developments in data communication.

Assessment Criteria

- ✓ The description explains the origin of current data communications with an outline of past developments.
- ✓ The description provides a taxonomy for current systems.
- ✓ The description identifies and mentions trends from emerging developments in data communications.

Specific Outcome 2: Describe synchronous and asynchronous data communication.

Assessment Criteria

- ✓ The description outlines the characteristics of each form of data communication.
- ✓ The description explains the features of data communications equipment with respect to synchronous and asynchronous data communication.

Specific Outcome 3: Describe communication with computers using telephone networks.

Assessment Criteria

- ✓ The description distinguishes types of telephone network services and outlines their features and costs.
- ✓ The description outlines the functions of telephone network components.
- ✓ The description outlines the types of problems encountered in digital transmission.
- ✓ The description outlines the options available as distance increases.

Specific Outcome 4: Describe asynchronous and synchronous communication with computers.

Assessment Criteria

- ✓ The description outlines the interface of the physical layer for synchronous and asynchronous communication.
- ✓ The description outlines the application and operation of protocols.
- ✓ The description outlines the delays incurred in transmissions.
- ✓ The description outlines the operation of link control protocols.

Unit Standard Essential Embedded Knowledge

- ✓ Performance of all elements is to be carried out in accordance with organisation standards and procedures, unless otherwise stated. Organisation standards and

procedures may cover: quality assurance, documentation, security, communication, health and safety, and personal behaviour.

- ✓ Performance of all elements complies with the laws of South Africa, especially with regard to copyright, privacy, health and safety, and consumer rights.
- ✓ All activities must comply with any policies, procedures and requirements of the organisations involved the ethical codes of relevant professional bodies and any relevant legislative and / or regulatory requirements.
- ✓ Performance of all elements should be performed with a solid understanding of the use of development tools needed in the areas applicable to the unit standard. An example of such tools are, but is not limited to CASE tools, programming language editors with syntax checking, program source version control systems.

Critical Cross-field Outcomes (CCFO)

- ✓ Organise and manage him/her self and his/her activities responsibly and effectively.
- ✓ Use science and technology effectively and critically, showing responsibility towards the environment and health of others.
- ✓ Demonstrate an understanding of the world as a set of related systems by recognising that problem solving contexts do not exists in isolation.
- ✓ Contribute to his/her full personal development and the social and economic development of the society at large by being aware of the importance of: reflecting on and exploring a variety of strategies to learn more effectively, exploring education and career opportunities and developing entrepreneurial opportunities.

SECTION 1: DEVELOPMENTS IN DATA COMMUNICATION

Outcomes

Describe past, present and emerging developments in data communication

Criteria

Skills / Knowledge

On completion of this section you will be able to ensure that:

- ✓ The description explains the origin of current data communications with an outline of past developments.
- ✓ The description provides taxonomy for current systems.
- ✓ The description identifies and projects trends from emerging developments in data communications.

The Origin Of Data Communications

Imagine twenty years ago when people were working in an office with little or no computer equipment. It's hard to imagine now, isn't it? One could say that we take for granted a lot of what we have gained in technology the past few decades. Now, imagine having to send a memo to everyone in the company. Back then we used interoffice mail; today we use e-mail. This is one form of communication that only became available due to the introduction and growth of networks.

In this section we will be looking at components, standards, protocols and media.

Let's look at the past of LAN's and WAN's first. LAN's were introduced to connect computers in a single office. WAN's came to expand the LAN's to include networks outside of the local environment and also to distribute resources across distances. Today, LAN's can be seen in a lot of businesses, from small to large. WAN's are becoming more widely accepted as businesses are becoming more mobile and as more of them are spanning across greater and greater distances. It is important to have an understanding of LANs and WANs as a service professional, because when you're repairing computers you are likely to come in contact with problems that are associated with the computer being connected to a network.

LANs

The 1970s brought us the minicomputer, which was a smaller version of the mainframe. Whereas the mainframe used centralized processing (all programs ran on the same computer), the minicomputer used distributed processing to access programs across other computers.

Distributed processing allows a user at one computer to use a program on another computer as a "back end" to process and store the information. The user's computer would be the "front end," performing the data entry. These allowed programs to be distributed across computers rather than centralized. This was also the first time computers used cable to connect rather than phone lines.

By the 1980s, offices were beginning to buy PCs in large numbers. Also, portables were introduced, allowing computing to become mobile. Neither PC's nor portables, however, were efficient in sharing information. As timelines and security became more important, diskettes were just not cutting it (sneaker net). Offices needed to find a way to implement a better means to share and access resources. This led to the introduction of the first type of PC LAN: ShareNet, by Novell. LANs are simply the linking of computers to share resources within a closed environment. The first simple LANs were constructed a lot like the figure on the right.

After the introduction of ShareNet, more LANs sprouted. The earliest LANs could not cover a great distance. Most of them could only stretch across a single floor of the office, and could support no more than 30 users. Further, they were still simple, and only a few software programs supported them. The first software programs that ran on a LAN were not capable of permitting more than one user at a time to use a program (this constraint was known as file locking).

Nowadays, we can see multiple users accessing a program at one time, limited only by restrictions at the record level.

WANs

By the late 1980s, networks were expanding to cover ranges considered geographical in size and were supporting thousands of users. Wide area networks, or WANs, first implemented with mainframes at massive government expense, started attracting PC users as networks went to this whole new level. Businesses with offices across the country communicated as if they were only desks apart. Soon the whole world would see a change in its way of doing business, across not only a few miles but across countries. Whereas LANs are limited to single buildings, WANs are able to span buildings, states, countries, and even continental boundaries.

Networks of today and tomorrow are not limited anymore by the inability of LANs to cover distance and handle mobility. WANs play an important role in the future development of corporate networks worldwide.

Let's take a closer look at current LANs.

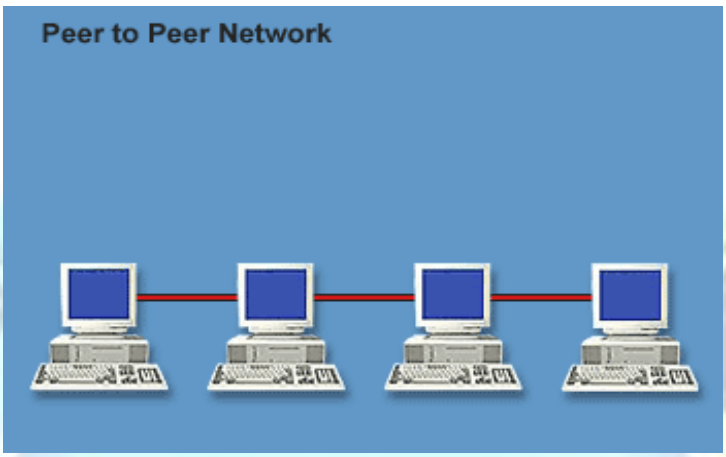
There are different types of configurations that can be implemented. The first configuration we are going to discuss is a ***workgroup***.

A workgroup is also known as a ***peer-to-peer*** network. All computers are considered equal (peers). No centralized computer is responsible for security functions such as user authentication.

Each computer acts as both a ***client*** that can access other shared resources on the network, and a ***server*** that can provide shared resources to the network. Each individual user decides what will be shared and with whom.

Workgroups are generally small (typically no more than 12 users) and easy to implement. They are also less expensive than larger network configurations because fewer components need to be purchased.

All current Windows family operating systems (since Windows for Workgroups) support workgroup configurations. The default when installing Windows 9x or Windows 2000 is to configure a new installation as a workgroup member.



Client/Server

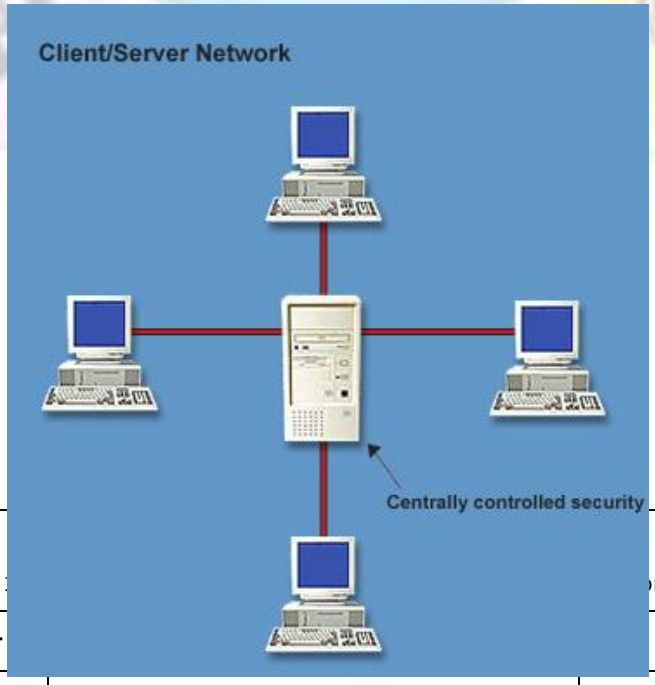
This is what most people think of when they think about a PC-based network.

In a client/server network, security is centrally controlled through network servers. A server is a high-powered computer running a ***network operating system***.

Security is managed by ***network administrators.***

Network administrators are responsible for user access and network resources. Each server is managed separately in a client/server network.

Novell's NetWare network operating system, through NetWare version 3.x, supports a client/server network configuration.



Domain Based

In a domain-based network, user workstations and servers are grouped by logical divisions known as ***domains***. The primary difference between a domain-based network and a client/server network is that the domain servers are managed as a group.

Users ***log on*** and access the domain as a whole, whereas a client/server network requires users to attach to each server separately.

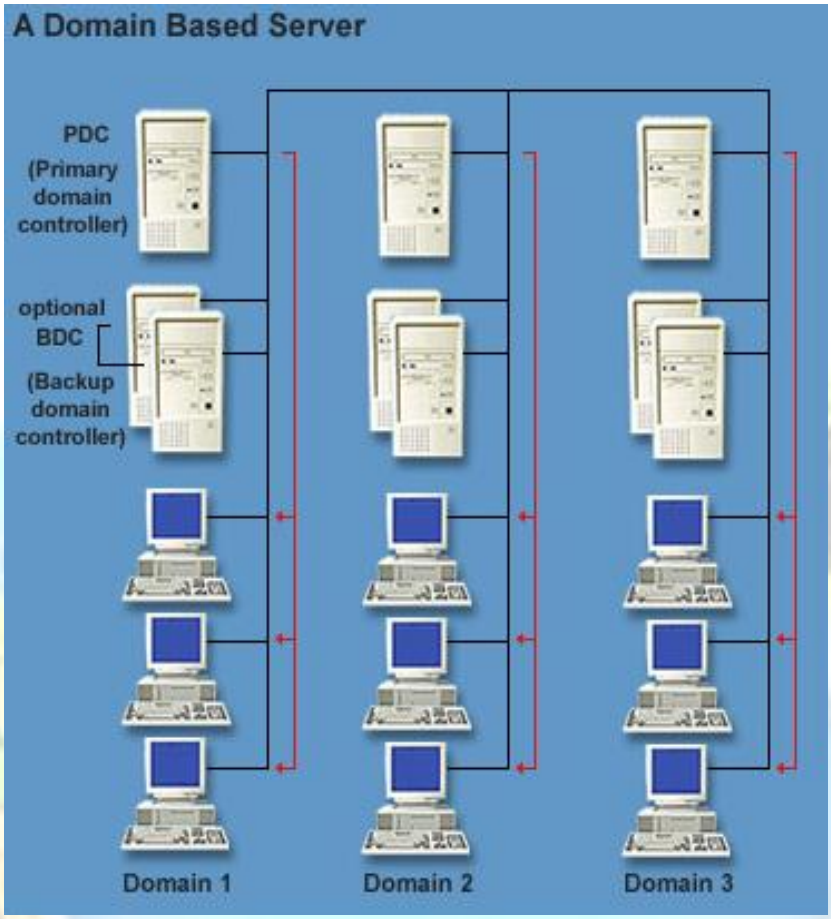
All versions of Windows NT Server support domain-based network configurations. Windows NT Server systems can also be used in as peers in a workgroup and as clients in a client/server network.

Directory Based

Directory-based networks use a more advanced management model than domain-based networks. Users, computers, servers and other network components are treated as a ***logical group.***

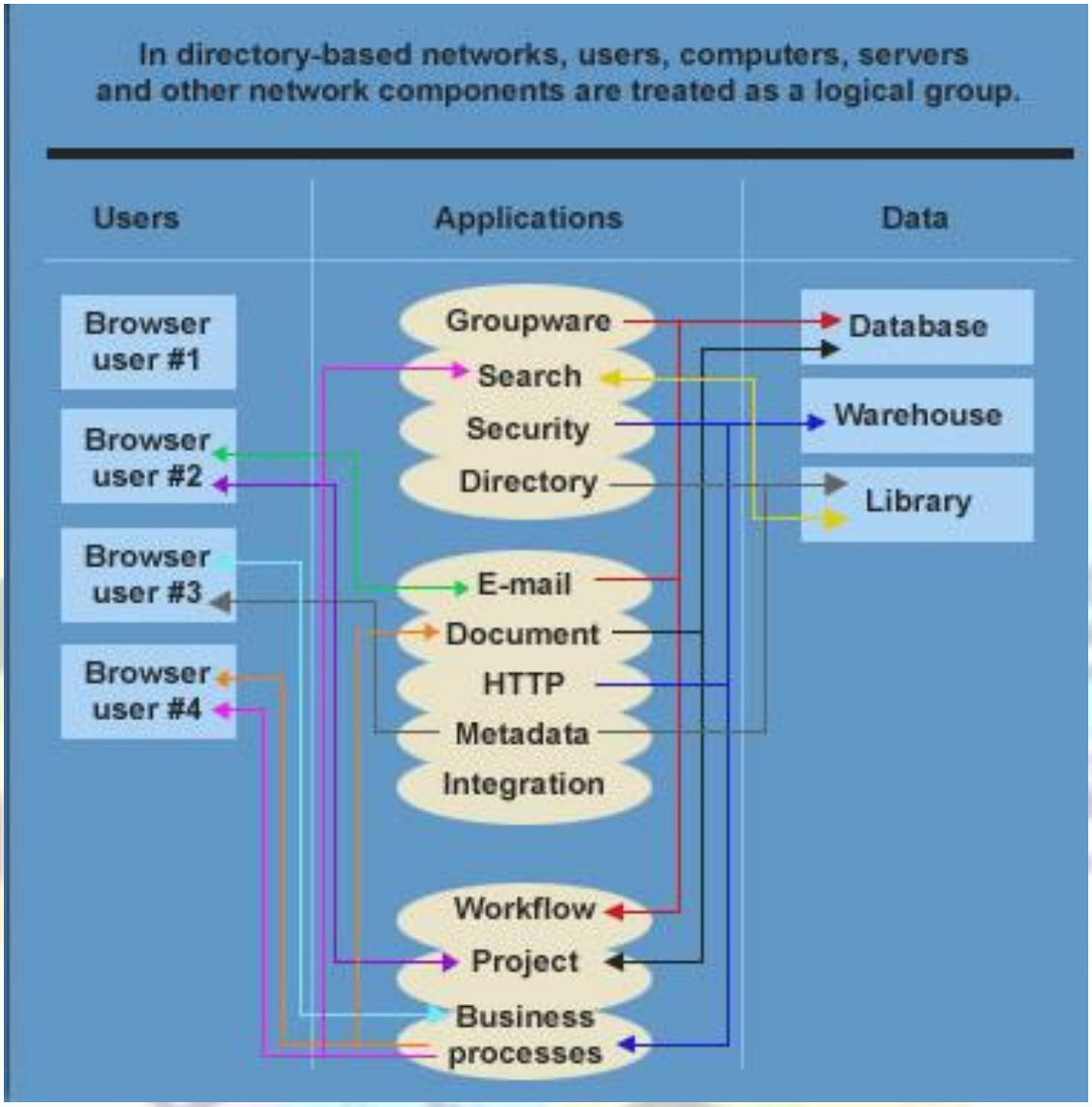
Directory-based networks have a great deal more flexibility and control built into them than domain-based networks. One advantage of a directory-based network is that no one server is the primary controlling server on the network. The responsibility can be shared equally among network servers.

Windows 2000, as well as Novell NetWare 4.x (and later), support directory-based networking. Microsoft and Novell implement directory-based networking somewhat differently, but the basic models are much the same.



Note Network management is shared between servers that are configured as domain controllers, which are servers that have been identified as acting in a management role.

The network can also include member servers, which are servers configured primarily as resource and application servers. Member servers are not involved in network management.



Network Standards Overview

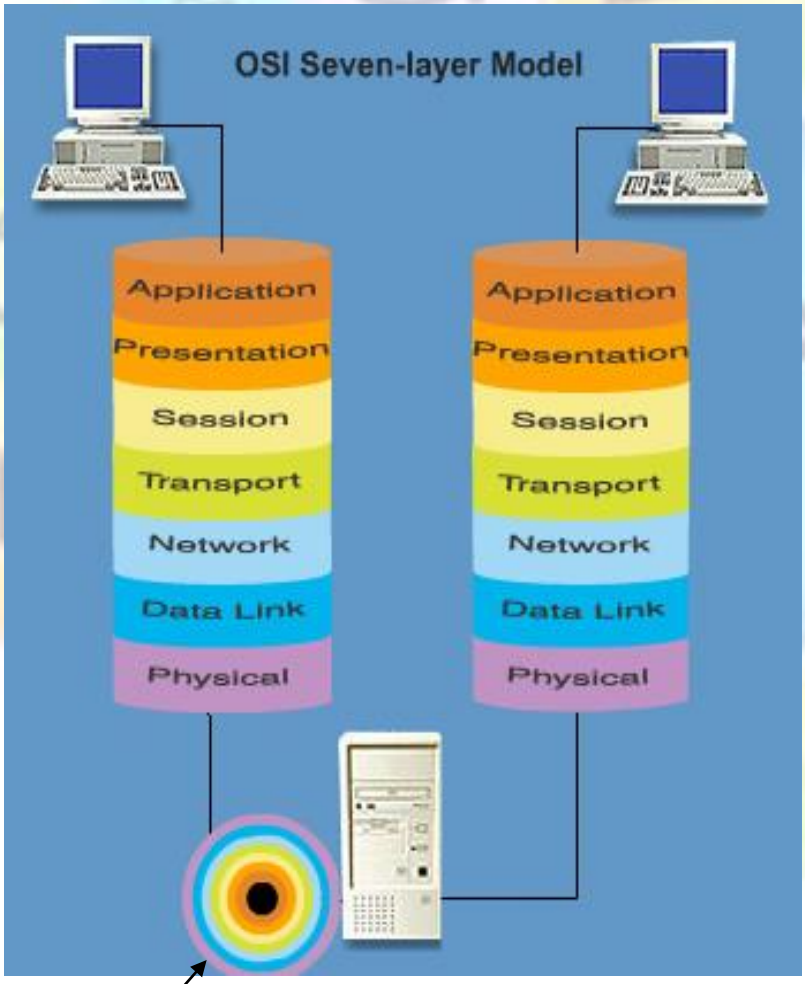
Standards are critical to network computing. Network standards define how computers communicate over a network, including the physical attachments to the network cabling, the way data must be formatted for transmission and how data error recovery is managed.

The OSI Model

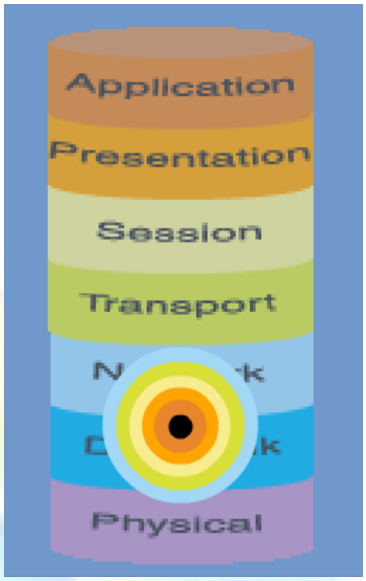
In 1978, the ***Open Systems Interconnection (OSI)*** model was developed by the ***International Standards Organization (ISO)*** to establish rules, or standards, for network communications.

The OSI model is a conceptual framework that attempts to establish a methodology for communications. It does not perform any of the functions in the communications process, but instead defines the tasks that need to be done and assigns responsibilities for those tasks.

It is a ***layered model*** that defines how each layer interacts with the layer directly above and below it.



Packet



The OSI model describes how data moves during data communication and how data communication is managed and controlled.

Before data can be passed down from one layer to the next, it is broken into smaller units of information called packets. As the packets pass between layers, each layer attaches formatting or addressing information.

At the physical layer of the sending computer, the bottom layer of the model, the packet passes across the network to the receiving computer.

Upon reaching the physical layer of the receiving computer, the formatting and addressing information is removed as data passes back up through the model.

Before looking at the OSI model layers, you need to learn a new terms. You will see the term ***node*** commonly used in network communication discussions. A node is any device that is communicating on the network. This definition includes networked computers, and any other device that is capable of network communications, such as a printer that is directly connected to the network.

Let's look at the functions and responsibilities of each layer in the table below:

Layer	Description
Application	The application or program used by the end user to communicate with the computer is implemented at this layer. For example, an electronic mail message being composed for transmission to another person, enters the OSI model at this level.
Presentation	The presentation layer acts to translate and interpret data. For example, if data is encoded in a manner, foreign to a receiving system the presentation layer will convert the data to a usable form. The presentation layer is also responsible for data encryption and protocol conversion.
Session	The session layer establishes, manages and terminates connections (called sessions) between communicating nodes. It also performs name recognition and security functions that are necessary for applications to communicate with each other. The session layer is also responsible for error detection.
Transport	The transport layer breaks the data into datagrams and provides addressing and identifications necessary for one node to find another. It ensures that all packets are delivered in sequence and

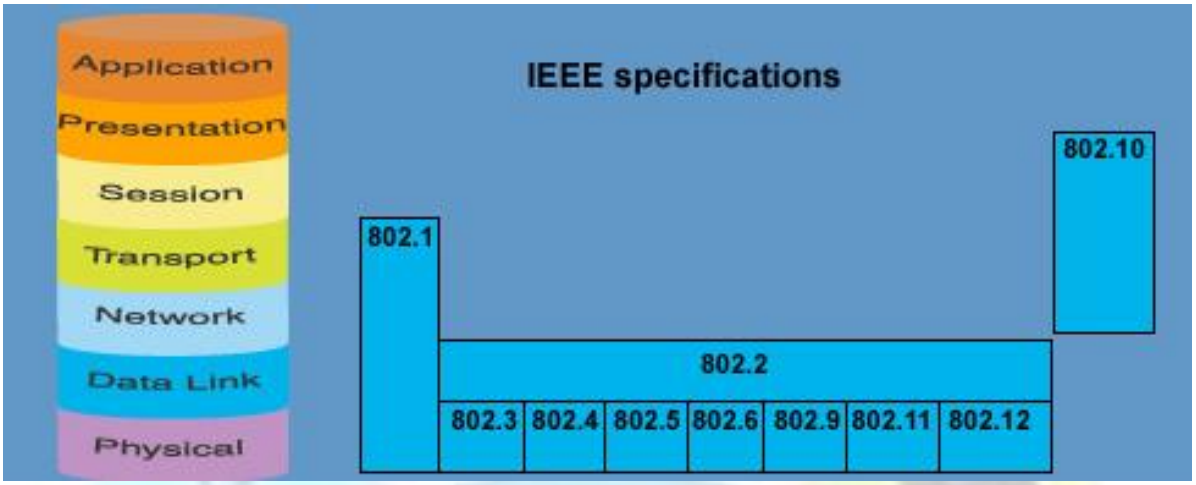
	without error, detecting errors such as missing and duplicate packets.
Network	The network layer controls the physical path the data should take based on factors such as network outages and priority of service. It also translates logical addresses and names to physical machine addresses.
Data Link	The data link layer provides for the flow of data from one node to another by controlling the data that is sent to the physical layer. Provisions are made for error checking and correcting data. The data link layer is divided into the media access control (MAC) and logical link control (LLC) sublayers. The MAC sublayer controls how devices share a media channel (communications channel) The LLC sublayer establishes and maintains links between network devices.
Physical	The physical layer is concerned with the electrical, mechanical and functional interface with the physical media. It establishes and maintains the physical links between nodes. The physical layer sends raw, unconstructed bits between nodes.

You might wonder why a conceptual model such as the OSI model is important when discussing physical aspects of network communications. One reason is that the OSI model provides a common, generally accepted set of terms and concepts for discussing network technologies. For example, you might hear someone speak of a technology providing layer 3 support. This is referring to layer 3 of the OSI model. Network connectivity devices are commonly described by the level of OSI model support they implement.

IEEE Standards

In 1980, the ***Institute of Electrical and Electronics Engineers (IEEE)*** began ***Project 802***, which defined networking standards for networking hardware that interacts with the bottom two layers of the OSI model.

These specifications establish standards for network interface cards, wide area networking components and the components used to make twisted-pair and coaxial cable networks. The 802 specifications define how network interface cards access and transfer data over the cable.



Data Communication Fundamentals

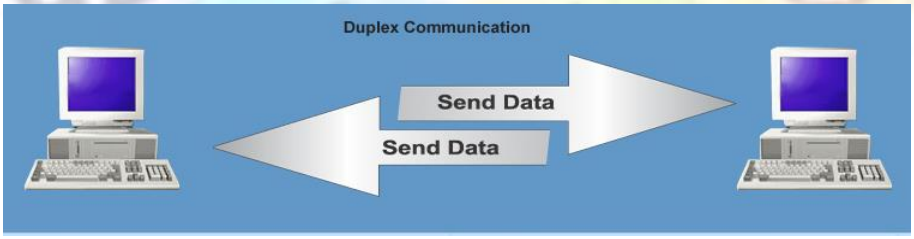
Signalling

Signalling refers to the method used to transmit data between nodes. The data must be formatted and presented in such a way that the sender can create the message and the receiver can understand it.

Because computers operate digitally, computer networks use digital signalling. However, when linking wide area networks, you may sometimes need to use an analogue signalling method.

Full-Duplex

Full-duplex data transmission means that data can be transmitted in both directions at the same time. Typically, full-duplex communication requires dual communication paths between two devices, one path for each data direction. Full-duplex communication is most commonly used in specialized, high-speed communication applications.

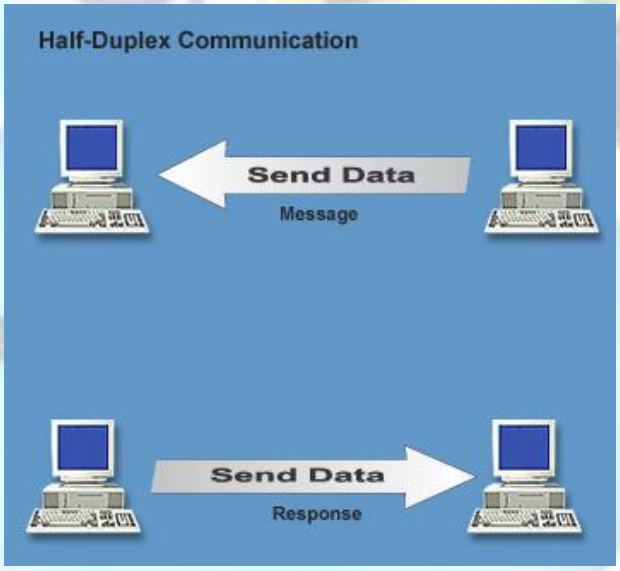


Half-Duplex

Half-duplex data transmission means that data can be transmitted in both directions, but not at the same time. This communication method is the one most commonly used in PC network communication.

In general, any two computers in a network will be able to communicate with each other. In order to communicate, they must be able to pass data in both directions. However, each computer must take its turn communicating. They cannot both communicate at the same time.

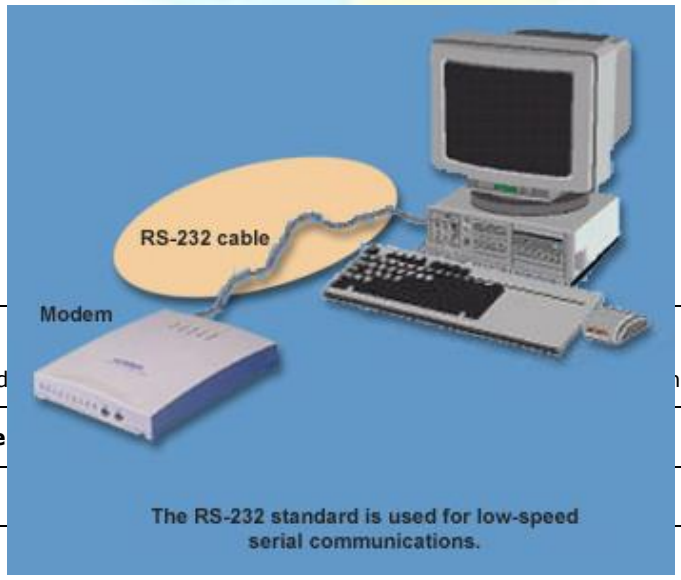
How this communication is managed is a function of the network's ***access method*** and ***access protocol.*** Two common access protocols, ***Ethernet*** and ***token ring***, will be discussed later.



RS-232

The RS-232 standard is used for low-speed serial communications. It is being mentioned as part of the introduction to networking because many networks support remote users through low-speed serial communications, specifically through dial-up connections.

RS-232 also needs to be mentioned because there is a local application of RS-232 that is similar to networking. Many PC operating systems, as well as a number of support utilities, support point-to-point connectivity between two computer systems through a serial modem eliminator cable.



DB-9 and DB-15 connectors are commonly used for RS-232 serial connections. Do not assume, however, that a DB-9 connector is always used for RS-232 communication. A DB-9 connector is one of the connector options supported for token ring network connections.

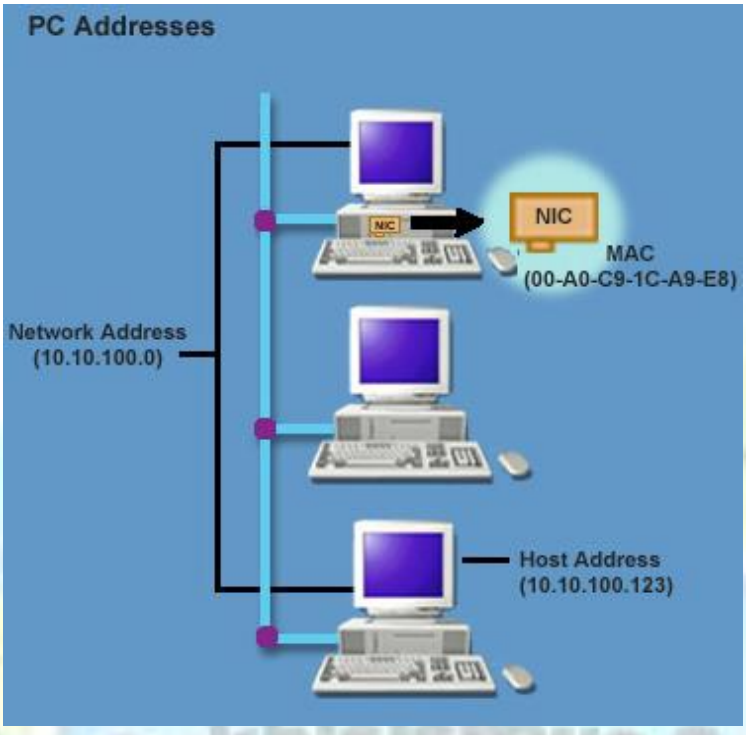
Network Addresses

Network addressing can be confusing because of the number of ways in which a PC can be identified on a network. These can include the ***MAC address, host address and network address.*** In most network environments, each PC will also have one or more ***symbolic names.***

First, every device that communicates on the network will have a physical, or MAC, address. This address is ***hard-coded*** into the device's network adapter card, though it can be overridden in some situations. The MAC address is contained in ROM and is assigned by the manufacturer.

Every network adapter ships with a unique MAC address. The only way to physically change the MAC address is to exchange the ROM containing the address with another network adapter.

Each manufacturer is assigned a unique value that is used as part of the MAC address. This value allows you to identify a card's manufacturer from its MAC address. The manufacturer generates the rest of the MAC address and is responsible for ensuring that each adapter has a unique address.



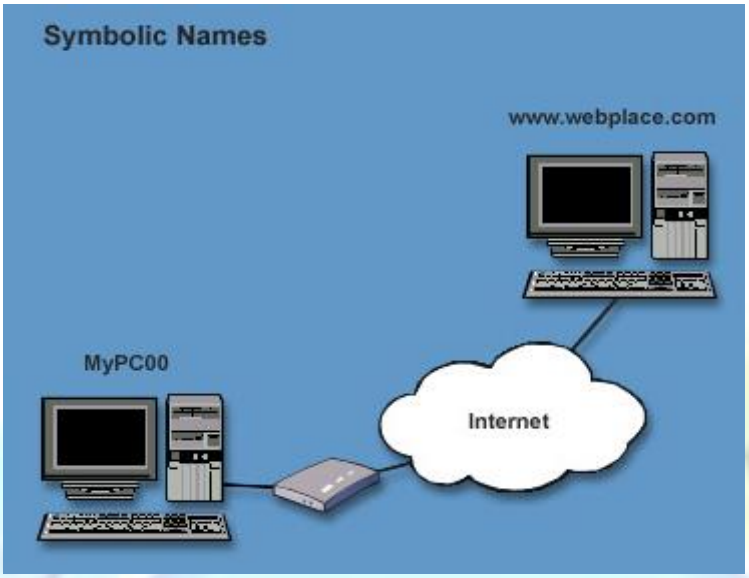
The ***host address*** is used by some network communication protocols to uniquely identify each machine on the network. It is used for managing machines at a communication protocol level, but the ***MAC address*** is still required for communicating at the physical level.

Some communication protocols also support network addresses. The ***network address*** is used to divide the network into more manageable segments, or sub-networks. The network address makes it easier to locate an individual system on the network.

The ***symbolic name*** is a "human-compatible" name that has been assigned to the computer. They are used because they are typically easier to remember than network addresses. All Windows 9x and Windows 2000 systems, for example, will have a machine name that is assigned during installation. They may also have an additional name that is assigned as part of communication protocol management.

When you access Internet locations, you typically do so through symbolic names known as ***domain names.***

Even though a network is divided into sub-networks, it can still be configured as a LAN. Large LANs commonly contain several sub-networks. A WAN, in almost every situation, will be made up of multiple sub-networks.



Network Component Basics

At its most basic, a PC network requires only a few components. A network is made up of both hardware and software components that work together to create the network environment.

For two PCs to communicate, they must have:

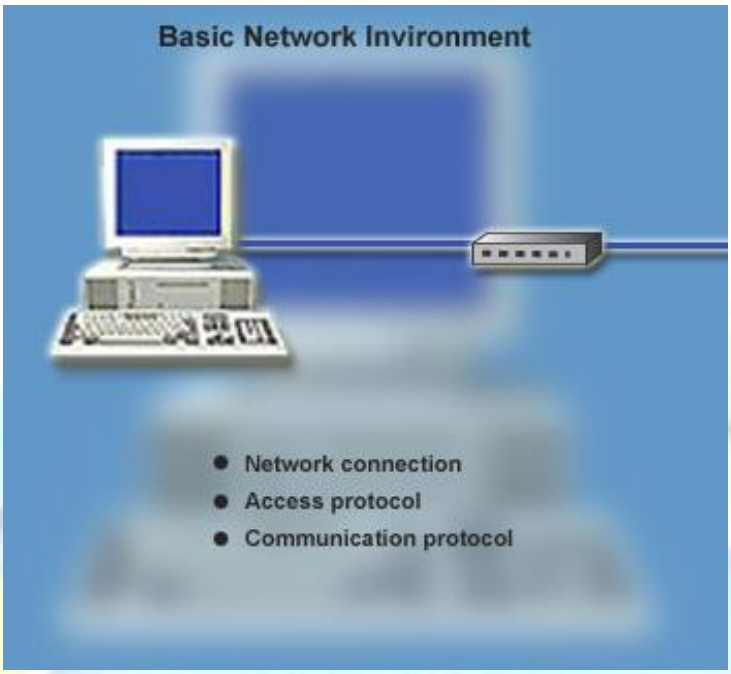
- ✓ A Communication Path
- ✓ A Common Access Protocol
- ✓ One or more Communication Protocols in Common

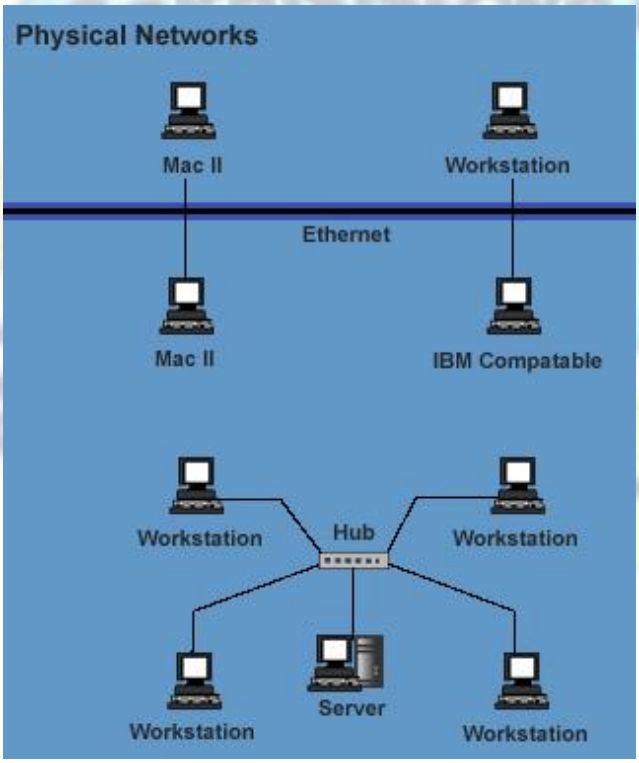
This is, of course, a simplified view of communication requirements. Other devices may be required, depending on your network configuration. Communication protocol support may sometimes require additional components.

The physical network is the communication media that ties the networked computers together. This physical network is often called the ***cable plant,*** though some newer network configurations communicate using wireless connections. We will limit ourselves to traditional wired networks.

Each PC must have a way of connecting to the cable plant in order to communicate. This connection is provided through a ***network adapter.*** The network adapter is installed in the PC and physically connects to the network cable. The network adapter will define the ***access protocol*** that the PC will use. The access protocol defines low-level communication characteristics

Each PC must also have a network-compatible operating system. Installed with the operating system will be one or more ***communication protocols.*** These are higher-level protocols that operate in the upper layers of the OSI model, defining communication methods, network addressing, error detection and correction methods, and so forth.





Media Overview

We begin our detailed look at networking and network components with the ***communication path.*** This will include the ***communication media*** that carries data communication and the ***topology,*** which is the media's physical layout.

Communication media is implemented at the physical layer of the OSI model. The communication media provides a communication path between networked devices. Communication media can be divided into ***wire and wireless media***. Of the two, most people are more familiar with wire media, but wireless has been gaining in popularity, especially in network implementations where running cable is too difficult or too expensive.

We will be focusing on wire communication. Before looking at cable types in detail, however, we will briefly compare wire and wireless communication. This comparison is done to provide additional background information about data communication.

Wire Media

In most cases, communication media is some form of cable, typically a ***copper wire cable.*** Cable-based media is sometimes referred to as ***bounded media.***

Common wire media types used in network communications include the following:

- ✓ Thick Coaxial Cable
- ✓ Thin Coaxial Cable
- ✓ Shielded Twisted-pair Cable
- ✓ Unshielded Twisted-pair Cable
- ✓ Fiber Optic

Of these, ***fiber optic cable*** is an exception to the copper wire model. Fiber optic cable uses glass or plastic fibers and carries data as light levels rather than electronic signal levels.

Wireless Media

Wireless media uses either radio broadcast signals or infrared light to communicate. Wireless media is sometimes referred to as ***unbounded media.*** Wireless media can be used when using a physical cable is impractical. Wireless media is also used in some long-range, high-volume communication applications.

Infrared communication is relatively easy to implement. It is often used as a supplement to other network communication media rather than as a primary communication method.

For example, you might use infrared to provide network support to laptop users who need infrequent access to the network.

One of the biggest drawbacks to infrared communication is that it is a ***line-of site communication*** method. A clear path between the sending and receiving systems is required. Communication can sometimes be degraded by strong light sources, as well.

Other wireless communication methods that are gaining popularity in specialized applications are ***microwave and satellite communication*** methods.

One of the more common uses of microwave systems is ***terrestrial microwave,*** a point-to-point communication method requiring a microwave antenna at each end. Terrestrial microwave can be a cost-effective solution for linking two sites when a wire-based communication method could prove more expensive over time.

For example, you can sometimes find microwave links used between two offices in the same metropolitan area.

Satellite systems transmit signals from the ***transmitting antenna*** to a ***satellite*** in space, back to a ***receiving antenna.***

To use a satellite system, you need to launch your own satellite or lease a service from a company offering these services. Due to the costs involved, you will seldom see satellite links used except in specialized applications.

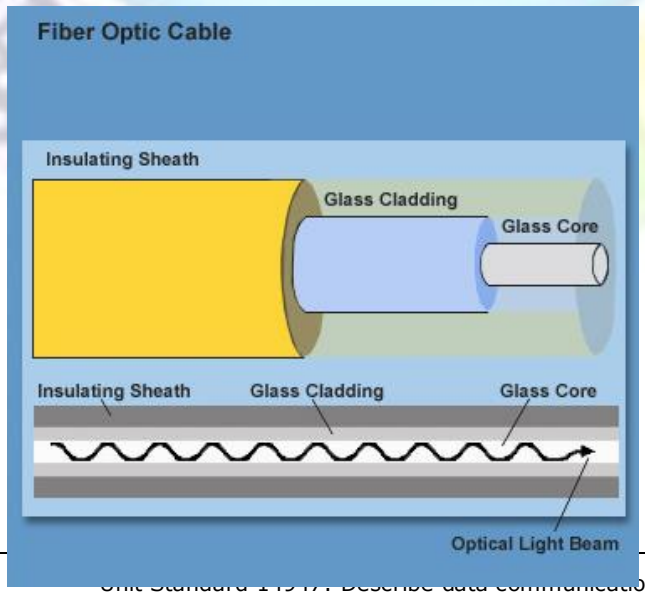
All radio frequency broadcast wireless communication methods, including microwave and satellite links, are susceptible to weather and other environmental influences.

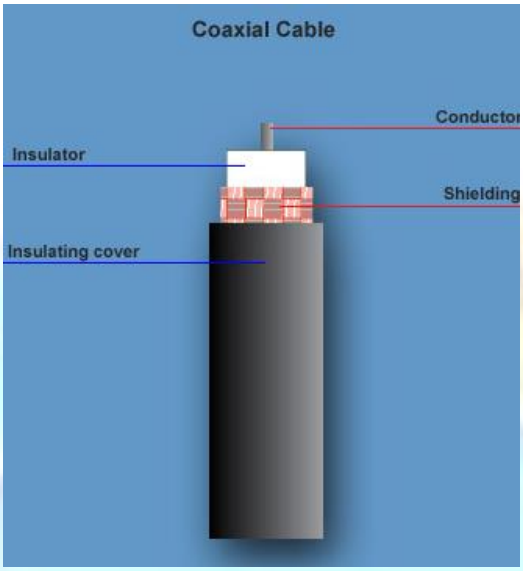
It can be difficult to justify the expense required in setting up these systems unless an organization is willing to take a very long-term outlook for cost justification.

Other types of media that falls in this section, would be wire media but since you have covered wire media, numerous times I will only repeat the wire types instead of entire specifications for each type of wire media. For specifics on the types of wires please refer back to previous modules.

The main types of wire media in networking are:

- ✓ Coaxial
- ✓ Twisted Pair Cables (UTP and STP)
- ✓ Fiber Optic




Coaxial Cable
Conductor
Insulator
Shielding
Insulating cover

Trends From Emerging Developments

For this section I chose to use an article on wireless, since this is where the world of communication is heading. (Don't forget that Bluetooth is a fast increasing means of communication as well, but for now, let's discuss wireless)

The article is from .net magazine

Cut the cables!

Whether you want to network your house or simply surf from your shed, wireless networks give you the Net wherever you want it. ***Gary Marshall*** finds out more

If you've ever despaired at the Spaghetti Junction behind your PC or wished you could surf the Web from your garden shed, wireless technology could be the answer. By banishing cable clutter, you'll also discover a world of possibilities: with the right kit you can have Internet access whenever and wherever you want it, or set up a home network for frantic multiplayer gaming. Wireless technology brings the Net out of your spare room and into the heart of you home, but we're not talking about gadgets that the manufacturers will never make, or prototypes of products that won't go on sale until 2020. Everything you need is available right now and the technology is faster, more flexible and cheaper than you might expect.

Time for change

Networks have been around for ages - the internet is, of course, the world's biggest computer network – and they're popular for a number of reasons. By connecting a bunch of computers together, you can share hardware such as printers and CD-ROM drives; you can communicate between machines, share files or run multiplayer games and you can share expensive resources, such as your speed broadband connection. In the home, that means you can share one modem or satellite connection between several PCs, or give the kids Internet access without letting them get their hands on your important documents.

The problem with traditional networks is that they use cable – fine if you've got a nice open-plan office, but not so good if you're trying to network your house or if you plan to move from room to room with your PC. By getting rid of the cables, wireless networks give you all the power of a traditional cabled network but with the same flexibility you get from a cordless phone. Depending on the hardware you choose, a wireless network can run at speeds of up to 11Mbps at a range of 300 to 500 feet. Apple's AirPort (www.apple.com/airport) is a good example of wireless networking in action. Simply slot an AirPort card into your iBook, plug the AirPort base station into your Net connection and, after a bit of fiddling, you can access the Net from anywhere in your home. The whole system takes just 15 minutes to set up, and you don't need a degree in computer science to install or use it.

3Com is one of the world's biggest providers of wireless gear, and Business Development Manager Rami Houbby believes that the technology's time has come. "Wireless has definitely become mainstream," he says. "Prices have fallen substantially and will continue to do so."

What do you need

The simplest way to set up a wireless network is to buy a pair of wireless networking cards. These work just like normal network cards and enable you to set up a simple system called a peer-to-peer network. Although this is fine for basic tasks such as transferring files, the easiest way to share your hardware or you Net connection between several machines is to shell out for a bit of a kit called a base station (also known as a wireless gateway). This massively increases the number of machines you can add to your network – for example, each AirPort base station supports up to 50 users – but more importantly, it makes it much easier to get your network up and running.

Before you rush off to PC World, it's important to know what you're looking for. There are three main types of wireless technology and while they all use radio waves to communicate – just like cordless phones – each one is designed for different things.

HomeRF is designed for home networking, 802.11b o4 Wi-Fi is designed for corporate networks and Bluetooth is a way fro phones, PDAs and other low-bandwidth devices to communicate with each other and with your PC. Different technologies offer differing connection speeds: HomeRF communicates at a maximum or 2Mbps; Wi-Fi delivers 11Mbps, while Bluetooth offers a paltry 1Mbps. In the future, HomeRF should exceed 10Mbps – but the boffins behind Wi-Fi are already working on versions that run at 22Mbps, and soon, 54Mbps. Then there's the issue or range. In perfect conditions, HomeRF and Wi-Fi operate at distances of more than 400 feet (121,92m); Bluetooth runs out of steam at 30 feet (9m).

In the battle of the standards, it seems that HomeRF is likely to be the loser. Although it's cheaper than a Wi-Fi kit, it's not as fast. More importantly, it doesn't have the same level of hardware and software support as Wi-Fi, which has attracted stacks of big names including Apple, Intel and 3Com (not to mention the Linux community). HomeRF kit is relatively difficult to find in the UK and in the long term, it looks likely to be the Betamax to Wi-Fi's VHS.

Bluetooth is different – rather than competing with Wi-Fi, it's designed to work alongside it. As Rami Houbby explains: "Wireless in the home has become the de-facto standard for sharing broadband (cable or DSL) internet connections in the home. Bluetooth is a cable replacement technology ideally used for synchronizing hand-held devices (PDAs, phones) with notebooks. It's a complimentary technology to Wi-Fi".

Another reason for Wi-Fi's popularity is that it's scalable: the same kit you use at home to network two or three computers can be used to network dozens of machines in an office. BY setting up multiple base stations, business users can hook in to the office network from anywhere in the building. In America, the same technology is being used in airports and other public places to provide Internet access for busy executives. Even cybercafés are getting in on the act – the Surf and Sip chain (www.surfandsip.com) uses Wi-Fi connections to provide fast Internet access to its customers, either through its own laptops or by hiring a wireless-enabled PC. If Wi-Fi is getting faster, cybercafés and other public places could soon be offering wireless internet access at speeds your modem can only dream of.

Beyond the hype

So much for the hype – what about the reality? Wi-Fi is very clever, but it's not perfect. There are some serious security issues to consider, too. That maximum range of 300 to 500 feet is as realistic as Microsoft's system requirements for Windows XP; in real-world situations, expect Wi-Fi's performance to drop dramatically if you're more than 100 feet away from a base

station or gateway. The data transfer speed is a maximum, too – the advertised 11Mbps transfer speed decreases rapidly if several computers are using the network at the same time.

There has also been speculation about whether wireless networks pose a health risk. However, while blathering away on a mobile phone may have similar effect to sticking your head in a microwave oven, wireless networks use a different form of technology – similar to cordless phones and the emergency services' communications systems. Provided you don't spend all day with your tongue against a base station, your Wi-Fi gear should be perfectly safe. Although wireless kit probably won't fry your brain, it could put a big dent in your wallet. Prices are falling but Wi-Fi hardware is still more expensive than traditional networking gear. Base stations cost around R6000, while the necessary cards for your PC or Mac cost R2500 to R3000 each (at the time of this article). If you're buying a card for a desktop machine, make sure you buy the right thing. Many manufacturers' Wi-Fi cards are designed for laptops and come in PC Card (PCMCIA) format. Unless you buy a PCI version, you'll need to fit an adaptor in your PC in order to use a Wi-Fi PC Card. Watch out, too, for the version of WEP (Wired Equivalent Privacy, a form of encryption) supported by the cards. Newer hardware uses 128-bit WEP but older equipment used 40-bit WEP. It makes sense to buy the latest – and most secure – hardware. If your planning to link together two desktop PCs or Macs, then wireless isn't for you.

It's much cheaper to buy a pair of cheap network cards and a bit of cable to link your machines together. However, if you've got several computers including at least one notebook PC, then wireless is a much more attractive option that provides all the benefits of a traditional network with the convenience of cordless communications. It's really handy if you use a wireless network at work; the same Wi-Fi card that hooks into your office's network will work just as well at home.

Broadband bonus

Wireless really comes into its own when you've got a fast broadband connection that you want to use on several different computers. Instead of knocking holes in walls you can power up your laptop and take advantage of ADSL or cable from anywhere in the house. If the UK follows America's lead, you'll be able to use the same equipment to log on to wireless networks almost everywhere. If you've ever struggled to find a phone point for your laptop or attempted to get a connection using a GSM modem, wireless will make your life easier. In years to come, the only place you'll see network or modem cables could be in a museum.

Formative assessment

In a group discuss the article from .Net magazine. Make notes for yourself about the following:

- ✓ The simplest way to set up a wireless network
- ✓ What a base station is
- ✓ HomeRF
- ✓ Wi-Fi
- ✓ Bluetooth

Write a short essay about the development of PC's from the 1970's to the introduction of ShareNet.

SECTION 2: SYNCHRONOUS AND ASYNCHRONOUS COMMUNICATIONS

Outcomes

Describe synchronous and asynchronous data communications

Assessment Criteria

On completion of this section you will be able to ensure that:

- ✓ The description outlines the characteristics of each form of data communication.
- ✓ The description explains the features of data communication equipment with respect to synchronous and asynchronous data communication.

Characteristics Data Communication Forms

All IBM PC and compatible computers are typically equipped with two serial ports and one parallel port. Although these two types of ports are used for communicating with external devices, they work in different ways.

A parallel port sends and receives data eight bits at a time over 8 separate wires. This allows data to be transferred very quickly; however, the cable required is more bulky because of the number of individual wires it must contain. Parallel ports are typically used to connect a PC to a printer and are rarely used for much else. A serial port sends and receives data one bit at a time over one wire. While it takes eight times as long to transfer each byte of data this way, only a few wires are required. In fact, two-way (full duplex) communications is possible with only three separate wires - one to send, one to receive, and a common signal ground wire.

There are two basic types of serial communications, synchronous and asynchronous. With Synchronous communications, the two devices initially synchronize themselves to each other, and then continually send characters to stay in sync. Even when data is not really being sent, a constant flow of bits allows each device to know where the other is at any given time. That is, each character that is sent is either actual data or an idle character. Synchronous communications allows faster data transfer rates than asynchronous methods, because additional bits to mark the beginning and end of each data byte are not required. The serial ports on IBM-style PCs are asynchronous devices and therefore only support asynchronous serial communications.

Asynchronous means "no synchronization", and thus does not require sending and receiving idle characters. However, the beginning and end of each byte of data must be identified by start and stop bits. The start bit indicates when the data byte is about to begin and the stop bit signals when it ends. The requirement to send these additional two bits cause asynchronous communications to be slightly slower than synchronous, however it has the advantage that the processor does not have to deal with the additional idle characters.

An asynchronous line that is idle is identified with a value of 1, (also called a mark state). By using this value to indicate that no data is currently being sent, the devices are able to distinguish between an idle state and a disconnected line. When a character is about to be transmitted, a start bit is sent. A start bit has a value of 0, (also called a space state). Thus, when the line switches from a value of 1 to a value of 0, the receiver is alerted that a data character is about to come down the line.

Features Of Data Communication Equipment

Most communications circuits perform functions described in the physical and data link layer of the OSI Model. There are two general strategies for communicating over a physical link: Asynchronous and Synchronous. Each has it's advantages and disadvantages.

Asynchronous

Sending data encoded into your signal requires that the sender and receiver are both using the same encoding/decoding method, and know where to look in the signal to find data. Asynchronous systems do not send separate information to indicate the encoding or clocking information. The receiver must decide the clocking of the signal on it's own. This means that the receiver must decide where to look in the signal stream to find ones and zeroes, and decide for itself where each individual bit stops and starts. This information is not in the data in the signal sent from transmitting unit.

When the receiver of a signal carrying information has to derive how that signal is organized without consulting the transmitting device, it is called asynchronous communication. In short, the two ends do not synchronize the connection before communicating. Asynchronous communication is more efficient when there is low loss and low error rates over the transmission medium because no data is not retransmitted. In addition, there is no time spent at the beginning of setting up the connection. One side simply transmits, and the other does it's best to receive.

Examples:

Asynchronous communication is used on RS-232 based serial devices such as on an IBM-compatible computer's COM 1, 2, 3, 4 ports. Asynchronous Transfer Mode (ATM) also uses this means of communication. Your PS2 ports on your computer also use this method. This is the method is also used to communicate with an external modem. Asynchronous communication is also used for things like your computer's keyboard and mouse.

Think of asynchronous as a faster means of connecting, but less reliable.

Synchronous

Synchronous systems negotiate the connection at the data-link level before communication begins. Basic synchronous systems will synchronize two clocks before transmission, and reset their numeric counters for errors etc. More advanced systems may negotiate things like error correction and compression.

It is possible to have both sides try to synchronize the connection at the same time. Usually, there is a process to decide which end should be in control. Both sides can go through a lengthy negotiation cycle where they exchange communications parameters and status

information. Once a connection is established, the transmitter sends out a signal, and the receiver sends back data regarding that transmission, and what it received. This takes longer on low error-rate lines, but is highly efficient in systems where the transmission medium itself (an electric wire, radio signal or laser beam) is not particularly reliable.

Glossary

Hard-coded: A value that cannot be overwritten.

Log on: The process of gaining access to a network through validation of a user name and password.

Network Operating system: Operating system software that enables a PC to act as a network server.

Peer-to-peer: In peer-to-peer networks there is no dedicated server, but instead, each computer connected to the network acts as both a server and client - i.e. each computer is a 'peer' of the other computers. These types of networks were originally developed as a low-cost alternative to server-based systems for use in smaller companies and organizations where there are approximately ten to fifteen users. A major drawback to this type of network is a comparative lack of security whereby each user must control access to resources on his/ her machine

Windows for Workgroups: Family of Microsoft products which provided a graphical user interface (see GUI) for the DOS operating system. Various versions were released throughout the early 1990s. Windows 3.11 (often also referred to as Windows for Workgroups) also provided 32 bit networking support. Windows 3.x utilized a co-operative multi-tasking kernel and was restricted to 12Mb RAM.

SECTION 3: COMMUNICATION USING TELEPHONE NETWORKS

Outcomes

Describe communication with computers using telephone networks.

Assessment Criteria

- ✓ The description distinguishes types of telephone network services and outlines their features and costs.
- ✓ The description outlines the functions of telephone network components.
- ✓ The description outlines the types of problems encountered in digital transmission.
- ✓ The description outlines the options available as distance increases.

Types Of Telephone Network Services

In this section we will look at Dedicated/leased lines, VAN, ISDN and Packet Switched

Dedicated/Leased Lines

A ***dial-up*** line provides a temporary connection using the public switched telephone network. Each transmission using a dial-up line must establish a circuit between the source and destination machines. Switches that make a logical connection between the circuit and the computers create a circuit. The circuit quality for each session can vary considerably with a 'bad connection', resulting in more errors and sometimes premature loss of the circuit.

A dedicated (leased) line, on the other hand, provides a permanent connection that links two locations using any one of a variety of technologies. These dedicated lines establish a connection without any delay and offer a faster and more reliable service, as the line quality is always consistent. Service providers often offer a variety of line qualities with varying levels of reliability and bandwidth.

The dedicated nature of this service means the costs are high as the telecommunications carrier dedicates the resources regardless of usage. Therefore, it is often more economical to pay on a usage basis using a dial-up service. Dedicated lines are only economical when large amounts of data are transferred at all times of the day.

The two types of dedicated or leased line available are ***digital*** and ***analogue.***

Analogue

The use of analogue technology requires the use of modems to convert between the digital data used by the computer to an analogue signal to send over the media. Analogue signaling

is considered to be more prone to errors that digital systems, often because of high noise levels.

Digital

Digital technology is preferable to analogue because the error rates are much lower. It also provides the high reliability that is desirable fro critical applications and data. Unfortunately, this often means paying more for the service.

Channel Service Units/Data Service Units

Digital system use devices called ***Channel Service Units*** or ***Data Service Units*** (CSU/DSU) instead of the modems used for analogue systems. These convert the digital signals from the computer to a different form of digital signal that is more suitable for use in WAN environments. They can also provide protection fro the service provider's network.

Switched Networks

Switching is the process used to connect the source and destination computers and the process by which the data is forwarded at intermediary points. Switched networks provide a way of sharing access to transmission media between two or more locations. A switched network is more efficient than a series of leased lines for connecting multiple locations because the required number of connections is reduced.

Switched networks are either ***circuit*** switching networks or ***packet*** switching networks.

Circuit Switching

The best known example of a circuit-switched network is the ***Public Switched Telephone Network*** (PSTN), otherwise known as the ***Plain Old Telephone System*** (POTS).

Circuit switching enables a temporary dedicated path to be established between two locations such as two computers. Once the connection is established, communication starts and, at the end of the communication, the connection is broken down.

A connection is established as follows:

- ✓ The source computer requests the connection
- ✓ The destination computer signals readiness to receive data.
- ✓ The source and destination computer exchange communication parameters for the connection.

Circuit-switched networks provide guaranteed bandwidth. The overall level of network utilization has no effect on performance because the connection is dedicated. Predictable levels of bandwidth are important for time-sensitive data such as voice and video. Once a connection is established, there is no channel access delay.

Circuit-switched networks make inefficient use of the media as, by definition, a dedicated channel cannot be shared even when it is not being utilized. The technology is also impractical for some applications because they time-out before a circuit is established, often for as long as 10-20 seconds. The use of dedicated channels is expensive compared with packet-switched

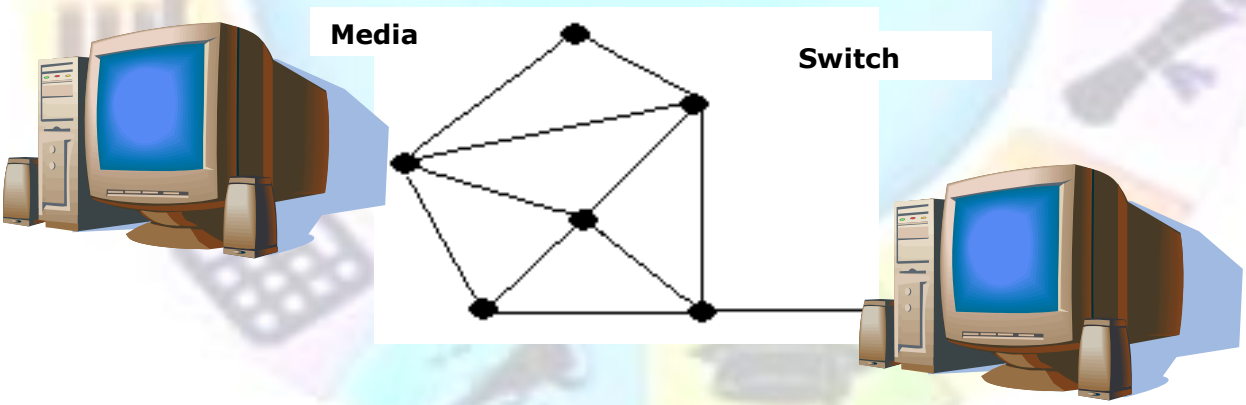
systems that share the available media and bandwidth. The costs are based on a flat fee for line rental and a variable cost dependent on time and distance.

The PSTN was originally devised just for voice data but it has gradually been upgraded to use digital technology, making it suitable for other forms of data. The PSTN is universally available and offers the cheapest and simplest method for providing connections to remote computers and networks, so many older WAN links use it. It is particularly useful for workers on the road.

The continued presence of analogue equipment means data must be converted from digital to analogue using a modem at each end of the connection. A low quality connection can result in high errors, and consequently a reduced modem speed and throughput. Although the fastest modems theoretically provide 56Kbps they are not able to utilize this speed when the system is purely analogue and the actual limit is 33.6Kbps (V.34+).

Packet Switching

This technology was developed on the idea that a change should be levied only when data is transported and customers shared the network infrastructure. It is a cost-effective alternative to dedicated lines and provides more efficient use of the network infrastructure than switched-circuit technology.



The figure above shows a packet-switching network. The data is divided into small numbered chunks called packets that contain addressing and other information such as the packet sequence number. There is a strictly defined maximum packet length that is kept small for two reasons:

- ✓ The small packets can be processed by the switches more quickly to keep the switch availability high and prevent the switches from becoming clogged.

- ✓ If a packet arrives in a damaged state, then only the small packet must be re-transmitted.

The individual packets are routed to their destination using media shared with other data so there can be no guaranteed bandwidth. The switches direct the packets from the source to the destination. They read the address information contained in the packet and route it using the best path available at the time.

There are two distinct categories of packet switching:

- ✓ Connectionless (or ***Datagram Packet Switching***)
- ✓ Connection-orientated (or ***Virtual Circuit Packet Switching***)

Connectionless or Datagram Packet Switching

This is the simpler form of packet switching that routes each packet independently using its address information. Individual packets can follow completely different routes and the sequence numbers may need to recompile data if delpackets that become lost or damaged and must be re-transmitted. If a link failure occurs during a transmission, packets can be routed around the problem. The delays in this system cannot be predicted so voice and video data are unsuitable for this type of packet switching.

Connection-orientated or Virtual Circuit Packet Switching

This system establishes a specific path for all packets to follow. This is known as a ***logical connection*** or ***virtual circuit.*** The connection is established once the source and destination machines agree on communication parameters such as packet size. This technology is often used for time-sensitive services such as video and voice.

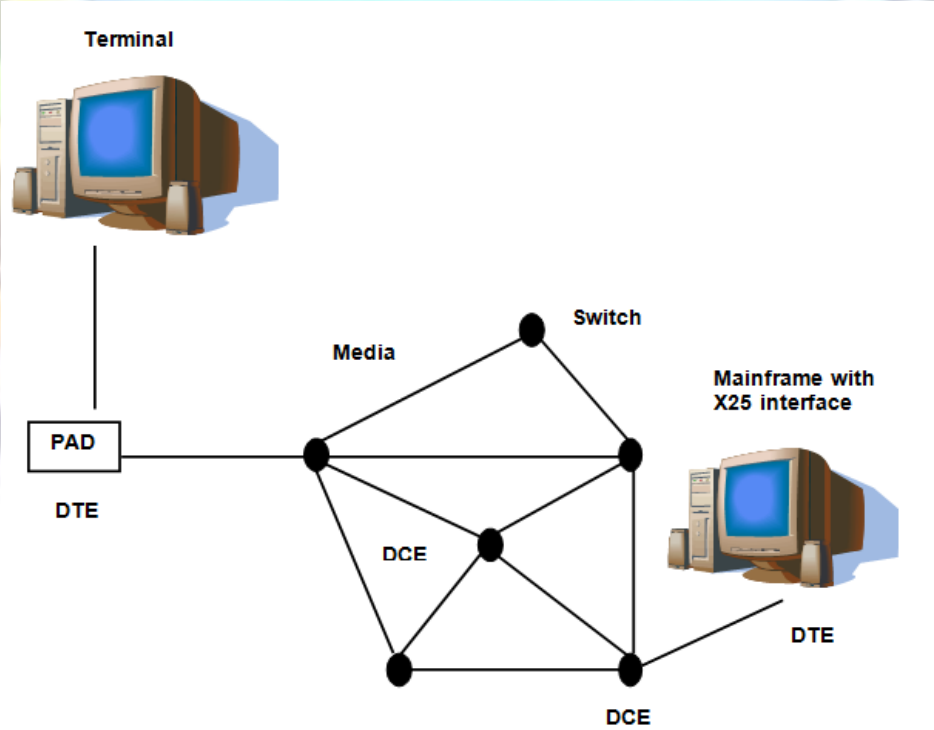
There are two forms of virtual circuits:

- ✓ ***Private (or Permanent) Virtual Circuit (PVC)*** uses a fixed path between two nodes that is established by the service provider.
- ✓ ***Switched Virtual Circuit (SVC)*** where the path is established just for the duration of session.

Packet-switched networks provide optimal use of available bandwidth. There is no connection setup delay and the packets can be routed around link problems. The cost is spread across all network users. The customer needs a link to the nearest switch connection on the ***Public Packet-Switched Data Network (PPSDN)***.

X.25

X.25 was originally used in the 1960s for connecting remote terminals to mainframe hosts without having to pay for a dedicated leased line. It is a mature and well-understood technology based on the X.25 packet-switching protocol suite. X-25 networks are universally available, require low maintenance and are usually charged for on a volume basis.



The figure above shows an example of an X.25 network that comprises multiple switches connected together using some form of transmission media. The remote terminal is connected to the network using a ***Packet Assembler/Disassembler (PAD)*** that sends and receives data from the local switch. The switches route the packets to the destination mainframe computer

using addressing information contained in each packet. The PADs are connected to the local switch using a leased line. An X.25 network is often represented in diagrams as a cloud because data can take any of the numerous possible paths through the X.25 network.

X.25 was conceived at a time when the remote terminals employed did not have the necessary processing capability to handle flow control and perform extensive error checking, so the X.25 network switches perform such tasks. The common use of analogue lines made error checking especially important. This overhead on the switches means that X.25 networks are limited to a throughput of up to 64Kbps[43].

X,25 systems are not suitable for time-sensitive data like voice and video because of the low bandwidth, the shared nature of the network (slow when the network is congested) and the variable packet-length, which means that delays cannot be predicted.

X.25 is commonly used by retail outlets to connect point-of-sale equipment to a central location.

ISDN

ISDN (Integrated Services Digital Network) is the digital version of the PSTN. It has been provided by telecommunication companies since the 1980s. ISDN is a digital switched-circuit technology for voice, video and data (hence 'integrated services'). Although ISDN makes use of existing copper telephone wiring, its implementation has been delayed by the requirement to upgrade analogue uipment to digital equipment. As with other PSTN systems, it is a dial-up service that is billed for by line rental and usage. The most common uses of ISDN are for interconnection of LANs and remote users (teleworkers) to businesses.

There are two classes of ISDN:

- ✓ ***Basic Rate Interface (BRI)*** provides two 64 Kbps (B Channels) for data and one 16Kbps (D channel) for link management control signals. It is sometimes called 2B+D and can provide a 128Kbps connection without compression by concatenating the two B channels. It is common to use one B channel for data and leave the other for voice or fax. This fro of ISDN is intended for ***Small Office or Home (SOHO)*** use.
- ✓ ***Primary Rate Interface (PRI)*** provides either T1 or E1 capacity level (23B or 30B) channels, depending on location in the world and one 64Kbps D channel. This form of ISDN is intended for larger companies and is commonly used to provide a PBX link between two company locations.

Although ISDN is a dial-up technology, it is capable of establishing a circuit connection in less than 1 second. This means that many applications that time-out when using the analogue PSTN can be used with ISDN. ISDN prices were initially high, but as telecommunication companies compete their digital upgrades, the prices have been reduced to attract customers. ISDN can prove to be expensive if used continuously, and in these circumstances, a dedicated line should be considered.

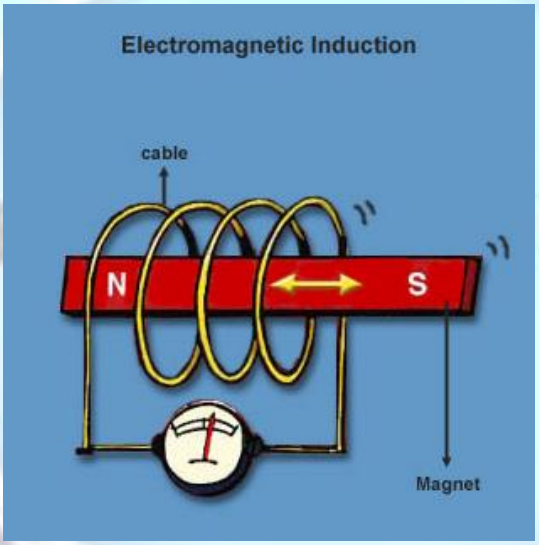
Problems Encountered In Digital Transmission

One of the biggest problems in digital transmission is ***Attenuation.*** As signals travel along the transmission media, the process of attenuation means they degrade and become distorted.

As a result of attenuation, each media type has a maximum length over which data can be transferred reliably. A repeater can be used to amplify the signal, and consequently extend the maximum allowable distance for a media type. For example, the maximum length of thin Ethernet cable is 202 yards (185m); connecting a repeater at one end of the cable would allow the network to be extended by a further 202 yards (185m).

Attenuation/distortion

The progressive degradation of a signal as it travels along a cable. Signals travelling along a medium will suffer from misshaping and weakening because of energy loss and absorption. A characteristic of media is its propensity to absorb and lose power is a signal. As a result, the further a signal travels along the media the more difficult a correct reading of the signal becomes at the receiving end. Attenuation is responsible fro the distance limitations imposed on any particular type of media.



Noise

EMI is electronic noise, random variations in voltages or data signals. It can originate from a number of sources, such as:

Fluorescent Lights

- ✓ Electric Motors (especially copiers and any type of compressor, such as those found in refrigerators)
- ✓ Power Lines
- ✓ Switches and Relays

To understand EMI's effects, you need to understand the concept of ***induction.*** When a conductor, such as a cable, passes through an electromagnetic field, it tends to pick up a

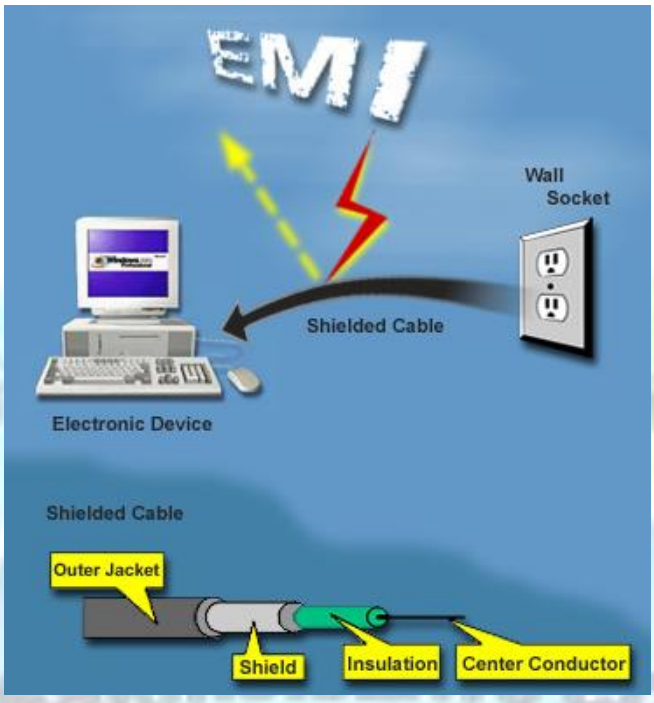
voltage generated (or induced) by that field. The voltage is sometimes strong enough to degrade the signal that the cable is carrying.

EMI can wreak havoc on electronic communications. Its impact is often seen on poorly routed network cables, causing intermittent failures and performance degradation, but that is not the only place where EMI will be evident.

Serial communication cables such as those used to connect modems or serial printers to computers are often highly susceptible to EMI.

The best way of avoiding EMI is to route ***cables away from EMI sources whenever possible.*** Avoid running cables in parallel with fluorescent lights or under or near devices such as copiers and water coolers. Do not run power cables and communication cables through the same ***conduit***.

EMI sources cannot always be avoided, but even when you cannot avoid them, you can minimize their impact through the use of shielded cable. A ***shielded cable*** has a wire mesh or foil under the cable casing. One end of the cable is connected to ground, providing a path for the voltages generated by the electromagnetic field. Although they are not 100% effective, shielded cables can result in a significant improvement.



Formative assessment

Contact Telkom and get prices for: An ADSL line and an ISDN line

SECTION 4: ASYNCHRONOUS AND SYNCHRONOUS COMMUNICATION

Outcomes

Describe asynchronous and synchronous communication with computers

Criteria

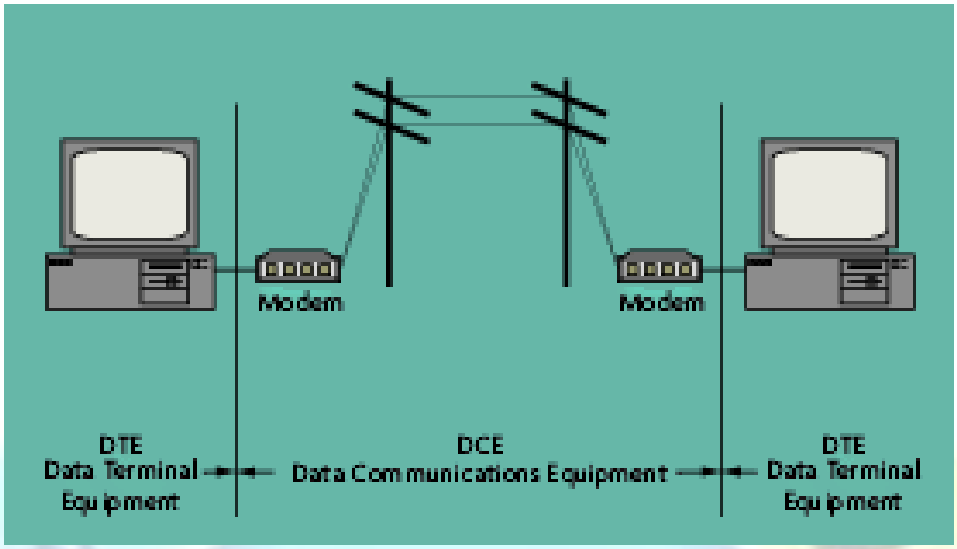
On completion of this section you will be able to:

- ✓ The description outlines the interface of the physical layer for synchronous and asynchronous communication.
- ✓ The description outlines the application and operation of protocols.
- ✓ The description outlines the delays incurred in transmissions.
- ✓ The description outlines the operation of link control protocols.

The Interface Of The Physical Layers

There are a number of implementations of the physical layer. Network devices allow a wide range of connectivity options. Some networks are well defined using the OSI model, where cables, bridges, routers, servers, modems, and PCs are easily identified. Sometimes only a few devices are linked together in some kind of proprietary network, or where the network services are bundled in a black-box fashion with the device.

The most common serial data exchange interfaces are RS-232, RS-422, and RS-485 for connecting two or more devices together. All three interfaces use data terminal equipment (DTE) and data communication equipment (DCE) terminology. The DTE is the component that wants to communicate with another component somewhere else, such as a PC communicating with another PC. The DCE is the component actually doing the communicating, or, performing the functions of the generator and receiver discussed in the standards. A modem is a common example of a DCE.



The interfaces between DTE and DCE can be categorized by mechanical, electrical, functional, and procedural aspects. Mechanical specifications define types of connectors and numbers of pins. Electrical specifications define line voltages and waveforms, as well as failure modes and effects. Functional specifications include ***timing, data, control and signal grounds***, and which pin(s) the functions are to use. The procedural interface specifies how signals are exchanged.

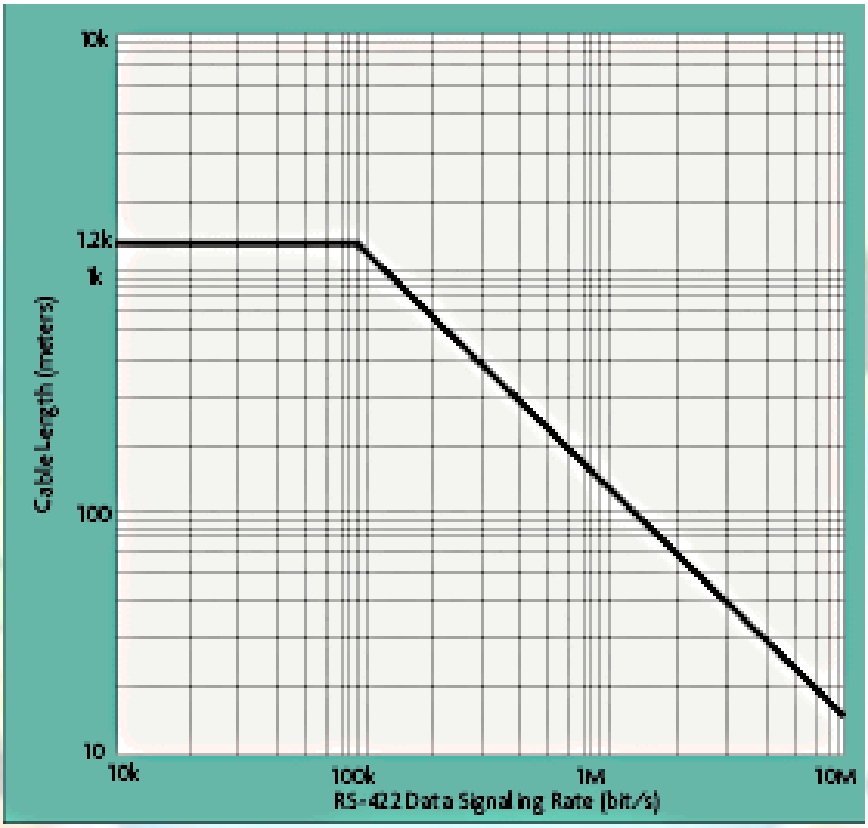
RS-485 is another serial data transmission method. Officially, it is EIA 485, or "Standard for Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems" by the Electronics Industry Association (EIA). This standard defines a method for generating ones and zeroes as voltage pulses. Remember, for all the data handling, framing, packeting, routing and addressing performed by the upper layers, it still comes down to pushing ones and zeroes over some physical media.

What is important to know about RS-485 is that it allows multiple receivers and generators, and it specifies cable characteristics in terms of signalling speeds and lengths. A typical cable is a shielded twisted copper pair, which is adequate for the typical signalling rate of 10 million bits per second (Mbps). This standard only defines the electrical characteristics of the waveforms. Note that RS-485 does not specify any media control functions-that is strictly up to the device connected to the generator (usually a chip). RS-485 is generally good for cable lengths up to 2,000 feet.

One example of a simple serial network might be a series of recorders connected over an RS-485 link to a PC that receives data acquired by each recorder. The manufacturer sells a plug-in card that installs in each recorder, with wiring instructions. Each network card is daisy-chained to the others over a series of shielded twisted pair cables that ultimately terminate on a network interface card in the PC. There is no real need to know and understand the network layers in this arrangement, except to understand the limitations on RS-485 (distance, shielding, data rate, etc.)

By title, the RS-422 standard is TIA/ EIA 422 B, "Electrical Characteristics of Balanced Voltage Digital Interface Circuits" by the Telecommunications Industry Association (in association with the EIA). It is similar to RS-485; the main differences being the rise times and voltage

characteristics of the waveform. RS-422 generally allows cable lengths up to 1.2 kilometres at up to 100 thousand bits per second (kbps). At 10 million bps (Mbps), cable lengths are limited to around 10 meters (Figure 4-3). In the presence of cable imbalance or high common mode noise levels, cable lengths may be further reduced in order to maintain a desired signalling rate.



RS-232C is perhaps the most common form of serial data exchange. It is officially known as EIA/TIA 232 E, "Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Binary Data Interchange," again by TIA in association with the EIA. The "E" suffix denotes a later version than the common "C" version. What makes this standard different from RS-422 and RS-485 is that it defines the mechanical as well as the electrical interfaces.

RS-232 is good for signal rates up to 20 kbps, at distances up to 50 feet. A zero (space) and a one (mark) are measured in terms of a voltage difference from signal common (+3 V dc = 0, -3 V dc = 1). The most common mechanical interfaces are the D-sub 9 and D-sub 25 connectors. Interchange circuits (pins) in RS-232 devices fall into four categories: signal common, data circuits (transmitted data, received data), control circuits (i.e., request to send, clear to send, DCE ready, DTE ready), and timing circuits.

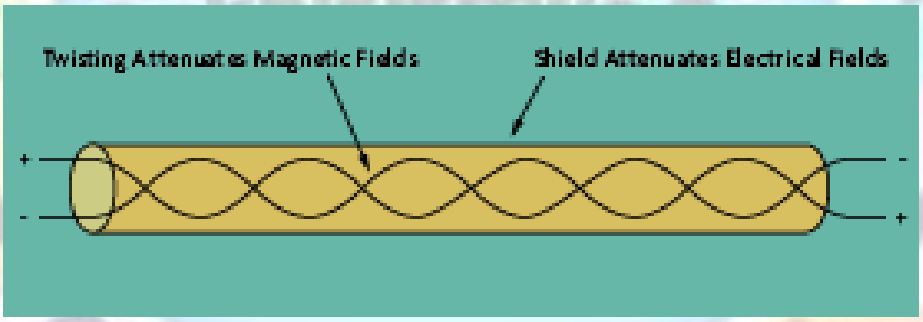
The standards described above all are used in serial communications schemes designed for longer distances. There is one common parallel interface, known as the General Purpose Interface Bus (GPIB), or IEEE- 488. Up to 15 devices can be interconnected, usually personal computers and scientific equipment or instruments. It provides a high data signalling rate, up

to 1 Mbps, but it is limited in length. The total bus length permitted is 20 meters, with no more than 4 meters between devices.

The IEEE-488 bus is a multi-drop, parallel interface with 24 lines accessed by all devices. The lines are grouped into data lines, handshake lines, bus management lines, and ground lines. Communication is digital, and messages are sent one byte at a time. The connector is a 24-pin connector; devices on the bus use female receptacles while interconnecting cables have mating male plugs. A typical cable will have male and female connectors to allow daisy-chaining between devices.

An example of an IEEE-488 implementation is a measurement system designed to assess the performance of a chemistry sample sink. The sink performs sample conditioning (pressure, flow, and temperature control) and chemical analysis (pH, dissolved oxygen, and conductivity) on water samples. The sink is instrumented with pressure sensors, resistance temperature detectors (RTDs), thermocouples, and reference junctions. A 30-point scanner is used to multiplex data from all of the sensors. The scanner is connected to a desktop or laptop PC using the GPIB interface. Data is acquired, stored, displayed, and reduced using application programs on the PC, efficiently and reliably under IEEE-488.

The media used to implement the physical layer is usually a set of copper wires. Unshielded twisted pair (UTP) cable is the most affordable. It is lightweight, easy to pull, easy to terminate, and uses less cable tray space than shielded twisted pair (STP). However, it is more susceptible to electromagnetic interference (EMI).



STP is heavier and more difficult to manufacture, but it can greatly improve the signalling rate in a given transmission scheme (Figure 4-4.). Twisting provides cancellation of magnetically induced fields and currents on a pair of conductors. Magnetic fields arise around other heavy current-carrying conductors and around large electric motors. Various grades of copper cables are available, with Grade 5 being the best and most expensive. Grade 5 copper, appropriate for use in 100-Mbps applications, has more twists per inch than lower grades. More twists per inch means more linear feet of copper wire used to make up a cable run, and more copper means more money.

Shielding provides a means to reflect or absorb electric fields that are present around cables. Shielding comes in a variety of forms from copper braiding or copper meshes to aluminized Mylar tape wrapped around each conductor and again around the twisted pair.

Fiber optics are being used more often as user applications demand higher and higher bandwidths. The term "bandwidth" technically means the difference between the highest and lowest frequencies of a transmission channel, in hertz (Hz).

More commonly, it means the capacity or amount of data that can be sent through a given circuit.

A bandwidth of 100 Mbps is standard using fiber optic cables. When first introduced, fiber was considered only for special applications because it was expensive and difficult to work with. In recent years, the quest for greater bandwidth combined with easier-to-use fiber have made it more common. Tools and training for installing and troubleshooting fiber are readily available.

There are three basic fiber optic cables available: multimode step index, multimode graded index, and single mode. Multimode fibers usually are driven by LEDs at each end of the cable, while single mode fibers usually are driven by lasers. Single mode fibers can achieve much higher bandwidths than multimode fibers, but are thinner (10 microns) and physically weaker than multimode. Equipment costs for transmitting and receiving single mode fiber signals are much higher (at least four times) than for multimode signals.

One distinct advantage of fiber optic cables is noise immunity. Fiber optic cables can be routed indiscriminately through high noise areas with impunity, although fire ratings should be observed. Cables that pass through multiple spaces in a plant should be rated for heating/ ventilation/air conditioning (HVAC) plenums where they can withstand fires per National Fire Protection Association (NFPA) requirements.

Application And Operation Of Protocols

A protocol is a set of rules enabling systems to communicate (exchange data). A single network will involve the use of many different protocols. A protocol generally defines the format in which data can be exchanged.

In any communication session between devices, control codes are used to control another device or provide information about the status of the session. Byte- or character-oriented protocols use full bytes (8 bits) to represent established control codes such as those defined by ASCII (American Standard Code for Information Interchange). Thus, a character-oriented protocol can only be used with its native character set because that character set has the specific control characters. In contrast, bit-oriented protocols rely on individual bits for control information and are the preferred method for transmitting data. Most data link protocols like those used for local area networks are bit oriented.

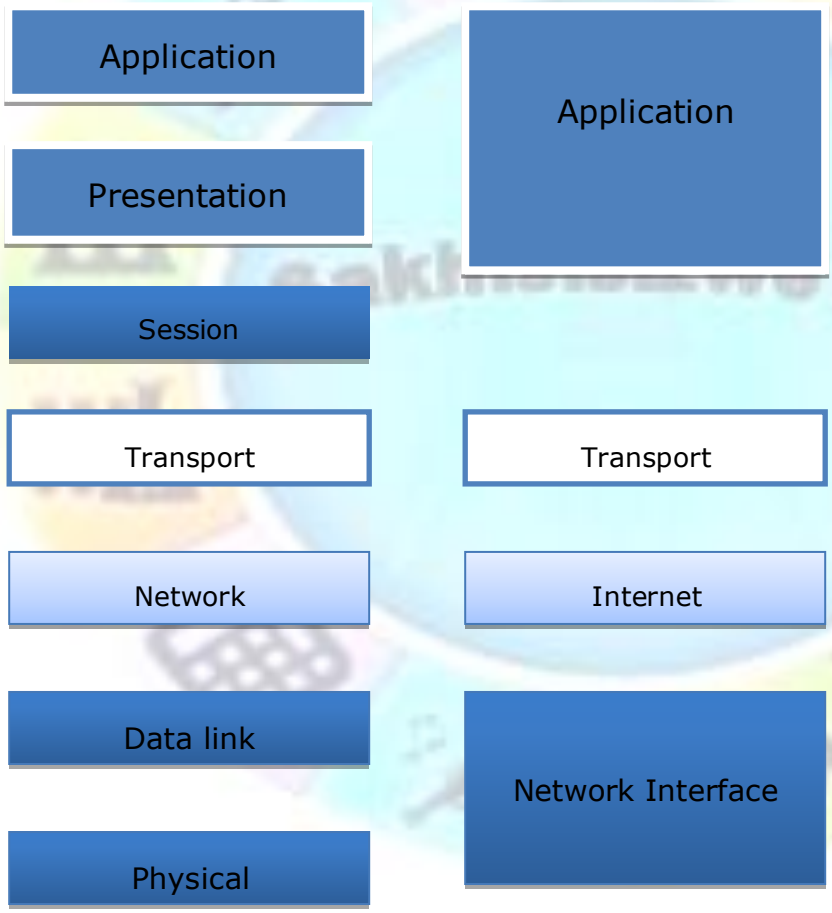
In a bit-oriented transmission, data is transmitted as a steady stream of bits. Before actual data transmission begins, special *sync* characters are transmitted by the sender so the receiver can synchronize itself with the bit stream. This bit pattern is usually in the form of a specially coded 8-bit string. IBM's SDLC (Synchronous Data Link Control) protocol is bit oriented. The sync character is the bit string 01111110, and this is followed by an 8-bit address, an 8-bit control field, and the data. Once the receiving system receives these start frames, it begins reading eight bits at a time (a byte) from the bit stream until an error check and an ending flag appear.

IBM's SDLC and HDLC (High-level Data Link Control) are bit-oriented protocols that control synchronous communication. HDLC is used in X.25 packet-switching networks; SDLC is a subset of HDLC.

The OSI Model and 'Real System' Networking

The OSI model is only intended to be a conceptual framework for discussing and designing protocols. As a result, the computer industry often struggles to categorise various protocols and networking technologies in the model.

This example demonstrates how the OSI model (a theoretical model) compares with the TCP/IP protocol stack (a real system). The TCP/IP and OSI models were developed concurrently and, therefore, show limited agreement. It should be noted that some of the OSI layers are performed by a single protocol, and some protocols cover many layers.



The table will help identify the network components and protocols that operate at the respective layers in the OSI reference model.

Component or Description	***Layer***
Bit transmission and encoding	1
Cable/media	1
Connector and pin-out details	1
Mechanical and electrical specifications for using the media	1
Network interface hardware	1
Physical network topologies	1
Transmitting and receiving signals from the network medium	1
Bridges	2
Converts Incoming 1s and 0s from the physical layer to frames	2
Converts outgoing packets from the network layer to frames	2
Identifies network cards	2
Network adapters, hubs, and Wireless Access Points (MAC)	2
Intelligent hubs (switches)	2
Logical topology	2
Brouters	2 and 3
Fragmenting packets	3
Layer 3 switches	3
Route selection and discover (moving data from one network to another)	3
Routers	3
Network address	3
IPSec	3
Acknowledgement messages and sequence numbers	4
Breaks messages from the session layer into packet format	4
Ensuring reliable data delivery (TCP/UDP)	4
Synchronization/dialog control (NFS/RPC)	5
Connection security (SSL)	5

Overview of Transport Protocols

For communication to take place, the two computers must have a protocol in common. All protocols require that certain actions are performed in a distinct order when computers communicate.

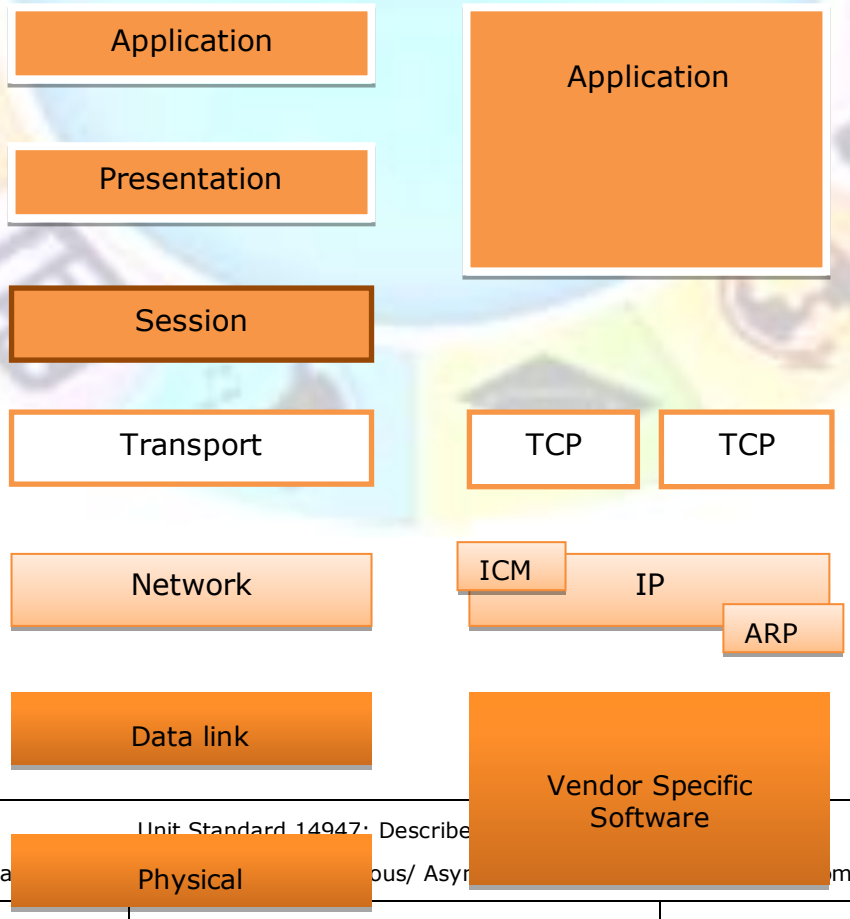
There are many different protocols in day-to-day user and each of these has advantages and disadvantages. Typically, standards organizations or vendors with the intention of accomplishing a particular task or tasks create protocols.

It is common for several protocols to be designed to work together. This collection of protocols is known as a protocol suite. The most widely used protocols suites are:

- ✓ ***TCP/IP*** – Transmission Control Protocol/Internet Protocol.
- ✓ ***IPX/SPX*** – Internetwork Packet Exchange/Sequenced Packet Exchange.
- ✓ ***NetBEUI*** – NetBIOS (Network Basic Input Output System) Extended User Interface.

Another commonly used term is ***protocol stack.*** This term describes a collection of protocols and the logical order in which they work together.

TCP/IP



THE TCP/IP SUITE COMPARED WITH THE OSI REFERENCE MODEL

TCP/IP is the 'de facto' communications standard used by the Internet. Is was originally developed by the US Department of Defence (DOD) in the 1970s to provide a robust network that could support the military networks in the event of nuclear war.

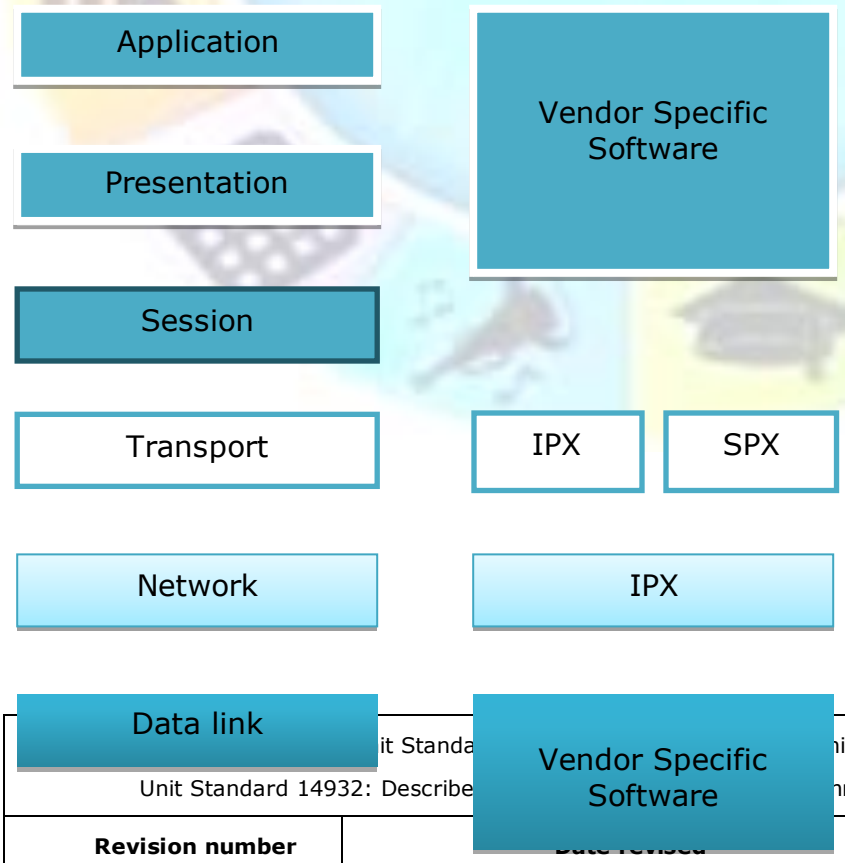
Although TCP/IP was originally devised for the interconnection of military network, it was given to government agencies and universities without charge. The universities incorporated the suite into the UNIX network operating systems on their computers and developed higher level protocols fro file transfer (FTP), mail transfer (SMTP), and document browsing (HTTP). These applications use the ***Sockets Application Programming Interface*** (API).

The TCP/IP protocol suite is increasingly being used on LANs and WANs mainly because of its robust nature and the desire to use Internet technologies. The major network software vendors now include TCP/IP within their products, but it remains an 'open standard'. No one 'owns' TCP/IP and anyone can contribute to its future development.

TCP/IP networks require careful and complex configuration. Each node is assigned and IP address and subnet mask, which identifies the device on its own network and identifies the device's network to other networks. To avoid manually configuring all devices, a DHCP (Dynamic Host Configuration Protocol) Server may be used.

IPX/SPX (or NWLink)

Novell developed the IPX/SPX protocol suite for use on its NetWare network operating system. The protocol is a derivation from the Xerox Network Systems (XNS) developed by Xerox in the late 1970s. Microsoft supply a version of this protocol called NWLink, which is fully interoperable with Novell IPX/SPX.



Physical

IPX/SPX COMPARED WITH THE OSI REFERENCE MODEL

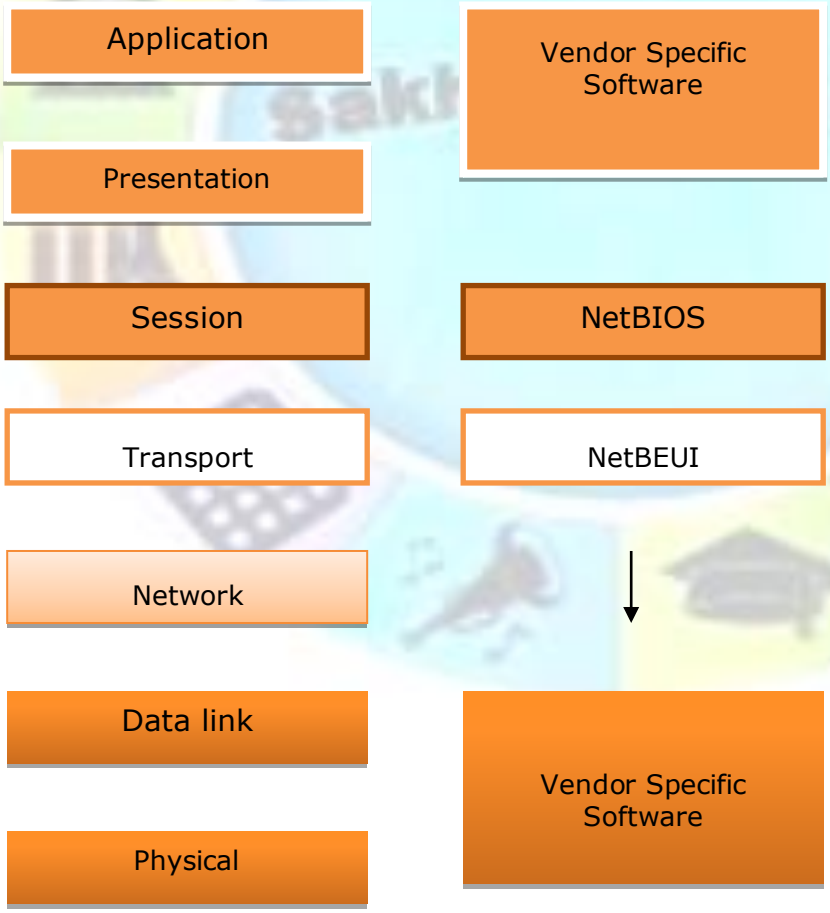
The IPX/SPX protocol is routable, and easier to configure then TCP/IP. However, recently most vendors (including Novell) have been moving to TCP/IP. IPX provides both unreliable transport layer services and unreliable network layer services – including addressing and routing. SPX provides reliable transport services.

NetBEUI

IBM first introduced the NETBEUI protocol suit en 1985 for its PC networks. NETBEUI was, for some years, Microsoft's preferred protocol for its LAN Manager and early NT products. Later versions of NT (3.5x and onwards) switched to Microsoft's own implementation of TCP/IP.

Originally, NetBEUI were considered one protocol but the NetBIOS component was separated for use with other protocols (such as TCP/IP and IPX/SPX).

The popularity of the NetBIOS API arises form its ability to provide software programmers with an easy means of accessing and utilizing network resources.



Characteristics of Transport Protocols

Choosing the correct transport protocol for a network requires an understanding of the advantages and disadvantages of each protocol. The following information evaluates the features and capabilities of the three main transport protocols:

Interoperability

- ✓ NetBEUI is limited to Microsoft and IBM networks
- ✓ TCP/IP is widely accepted within both PC and non-PC networks. It is available for most operating systems including NT, UNIX, NetWare, VMS, DOS, Mac OS, and OS/2.
- ✓ Originally the native protocol for Novell NetWare, IPX/SPX was widely used in PC networks. More recently Novell have shifted towards a TCP/IP-based network operating system. However, IPX/SPX can also be found in the following operating systems: NT (as NWLink), VMS, and UNIX>
- ✓ NetBIOS runs over NetBEUI, TCP/IP, and IPX/SPX.

Open or Proprietary Specification

- ✓ ***NetBEUI*** is a ***proprietary*** specification owned by IBM. However, the specification is made available to developers.
- ✓ ***TCP/IP*** is an ***open*** specification for which anyone can suggest modifications and enancements. Documents called ***Requests For Comment*** (RFC) are used to detail current and proposed specifications.
- ✓ ***IPX/SPX*** is a ***proprietary*** specification owned by Novell. Typically, it has been difficult to obtain information on the protocol but Novell is becoming more willing to publish details.

Configuration and Administration

- ✓ ***NetBEUI*** requires very little configuration or administration
- ✓ ***TCP/IP*** is potentially difficult to administer as each workstation must be allocated a unique IP address and must also have other parameters correctly configured to allow network communication. This task has been much simplified by facilities such as DHCP and DNS.
- ✓ ***IPX/SPX*** is very simple to configure for small networks; however, larger internetworks would require the allocation of unique network numbers.

IPX/SPX Frame Types

Novell has used several frame structures in its networking systems – these are referred to as ***frame types***. Normally, the frame structure is not important as long as the same frame type

is used throughout the network; machines using different frame types will be unable to communicate. The most common frame types used in NetWar networks are:

- ✓ Ethernet_802.3 – is used in earlier versions of NetWare up to 3.11
- ✓ Ethernet_802.2 – is used as the default frame type in NetWare version 3.12 and later. This frame type is required if more than one protocol is to be loaded simultaneously.

Segmentation of Networks and Routing

- ✓ ***NetBEUI*** does not support routing. It uses a single-part naming scheme addresses, and therefore has no ability to cope with multiple networks (that is, the address used cannot be divided into a network and host portion).
- ✓ ***TCP/IP*** divides its IP address into a network and host portion. This allows for a series of subnets to exist within the internetwork environment. TCP/IP provides full support for routing between networks. Dynamic routing, in which routers learn possible paths from each other, is supported by protocols such as ***Routing Information Protocol*** (RIP) and ***Open Shortest Path First*** (OSPF).
- ✓ ***IPX/SPX*** provides a network address and a node address to allow support for multiple subnets. However, the system is not as flexible as TCP/IP. IPX/SPX provides full support for internetwork routing and dynamic routing is supported by RIP over ***IPX*** and ***NLSP*** (NetWare Link State Protocol). Unfortunately, until recently there has been no central body to distribute IPX/SPX network numbers, and therefore if an internetwork like the Internet were to be established using IPX/SPX, there would be considerable network address duplication.

Performance

The performance of a protocol may depend on the choice of certain configuration parameters. The information below provides a general indication:

- ✓ ***NetBEUI*** is tuned for communication on small LANs, and is therefore very fast under these circumstances. Its performance across WANs is poor. NetBEUI has the ability to self-tune performance related parameters.
- ✓ ***TCP/IP*** is not as fast as NetBEUI on small LANs. However, it provides better performance than both NetBEUI and IPX/SPX over WANs.
- ✓ ***IPX/SPX*** is not as fast as NetBEUI on small LANs but does provide some self-tuning features. IPX/SPX is less efficient than TCP/IP on large routed WANs. IPX/SPX is, however, faster than TCP/IP for file and print operations while TCP/IP is faster for application services.

Choosing a Protocol

The choice of protocol will depend upon some or all of the following factors:

- ✓ Size of the network
- ✓ The need to route.
- ✓ The client and server operating systems in use.

- ✓ Interoperability with other systems and the Internet.

However, the choice for a new or upgraded network will almost always be TCP/IP, unless there are very good reasons not to choose it.

Remote Connection Protocols

Modems use serial (asynchronous) communications. Serial links are among the oldest methods of data communication and are supported by most hosts (serial interfaces are widespread I the computer world for instance).

Serial ports communicate using byte streams instead of frames. A number of protocols exist to organise serial information into the frames required by the network. In network communication, frames are defined by the network technology in use (for example, Ethernet).

The two protocols that are commonly used for serial communications are explained below:

Serial Line Internet Protocol (SLIP)/Compressed SLIP (CSLIP)

SLIP is a very simple protocol based on TCP/IP. Compressed SLIP increases the data frol by removing repeated header information.

SLIP is generally regarded as obsolete. It provides no error detection or correction (higher lever protocols must perform this function). It only supports IP and only provides support for static IP addressing (that is, IPs have to allocate and individual IP address to each subscriber).

Point-to-Point Protocol (PPP)

The PPP protocol was devised to replace SLIP. It is easier to use and configure and addresses the deficiencies in SLIP:

- PPP allows the user to specify a means of ***authentication*** (for example, Challenge ***Handshake Authentication Protocol*** [CHAP] or ***Password Authentication Protocol*** [PAP]).
- It provides ***data compression*** negotiation.
- It handles ***error detection*** and correction.
- It provides support for assigning and managing the IP addresses used at connection time (***dynamic IP allocation***).
- It supports ***multiple*** protocols (IP, IPX and NetBEUI).
- It defines a standard ***frame format*** (see table)

PPP is known as an encapsulation protocol. This means that the protocol sits around other protocol data which allows a virtual tunnel to be created.

Flag	Beginning of frame
Address	Broadcast address.
Control	

Protocol	Assigned number for protocol.
Data	The packet (1,500 bytes maximum size).
Frame Check	Checksum calculated from the contents of the other fields.
Flag	End of frame.

Glossary

Conduit: Pipe used to route and protect cable runs.

Final formative assessment

Specific Outcome 1: Describe past, present and emerging developments in data communication.

Assessment Criteria

- **The description explains the origin of current data communications with an outline of past developments.**
- **The description provides taxonomy for current systems.**
- ***The description identifies and projects trends from emerging developments in data communications.***

1. What happened in the computer world in the 1970's?	1
2. During which decade were portable PC's introduced?	1
3. Explain a workgroup	6
4. Explain a client/server network	2
5. Explain a domain-based network	2
6. Explain how data moves during data communication and how data communication is managed and controlled with the OSI model.	4
7. Explain full duplex data transmission	1
8. Explain half-duplex data transmission	1
9. What must two PC's have in order to communicate?	3
10. List five common wire media types used in network communications	5
11. List three types of wireless media	3
12. Explain terrestrial microwave	2
13. Explain a satellite system	3
14. Answer the following questions out of the article from .Net: what is the simplest way to set up a wireless network	1
15. What is a base station also known as?	1
16. What is homerf designed for?	1

17. What is Wi-Fi designed for?	1
18. What is Bluetooth designed for?	1
Specific Outcome 2: Describe synchronous and asynchronous data communications **Assessment criteria** • **The description outlines the characteristics of each form of data communication.** • ***The description explains the features of data communication equipment with respect to synchronous and asynchronous data communication.***	
1. How does a parallel port send and receive data?	2
2. How does synchronous communications work?	2
3. Are serial ports synchronous or asynchronous devices?	1
4. Explain Asynchronous communication	3
U/S 14932Specific Outcome 3: Describe communication with computers using telephone networks. ***Assessment Criteria*** • The description distinguishes types of telephone network services and outlines their features and costs. • The description outlines the functions of telephone network components. • The description outlines the types of problems encountered in digital transmission. • The description outlines the options available as distance increases. .	
5. Explain a dial up line	3
6. List the two types of dedicated or leased lines	2
7. List the two types of switched networks	2
8. Explain circuit switching	6
9. Explain packet switching	3
10. List the two categories of packet switching	2
11. Explain attenuation	1
12. Explain EMI	1
13. What does ISDN stand for	1

Specific Outcome 4: Describe asynchronous and synchronous communication with computers.

Assessment Criteria

- The description outlines the interface of the physical layer for synchronous and asynchronous communication.
- The description outlines the application and operation of protocols.
- The description outlines the delays incurred in transmissions.
- The description outlines the operation of link control protocols.

1. What is a protocol?	1
2. What do the following stand for? TCP/IP, IPX/SPX, NetBEUI	3
3. List the four factors to consider when choosing a protocol	4
Total	***77***