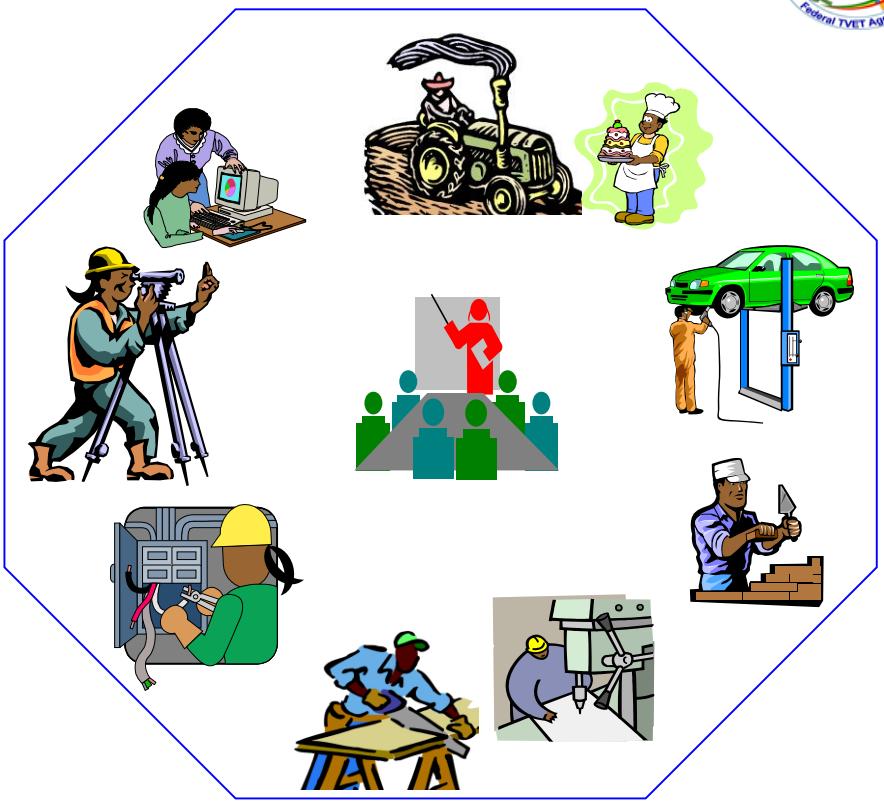


Hardware and Networking Servicing Level III

Based on August, 2011 Version 3 Occupational standards

Module Title: **Determining Best Fit Topology**

LG Code: **EIS HNS3 M05 LO (1-3) LG (17-19)**

TTLM Code: **EIS HNS3 TTLM 1220v1**

December 2020

Bishoftu, Ethiopia

Table of Contents page

LG#17	LO #1- Identify key information sources

Instruction sheet

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics:

- Identifying information repositories
- Reviewing current organizational documentation
- Developing critical questions
- Ensuring information gathering techniques

This guide will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Identify information repositories
- Review current organizational documentation
- Develop critical questions
- Ensure information gathering techniques

Learning Instructions:

Read the specific objectives of this Learning Guide.

1. Follow the instructions described below.
2. Read the information written in the “Information Sheets”. Try to understand what are being discussed. Ask your trainer for assistance if you have hard time understanding them.
3. Accomplish the “Self-checks” which are placed following all information sheets.
4. Ask from your trainer the key to correction (key answers) or you can request your trainer to correct your work. (You are to get the key answer only after you finished answering the Self-checks).
5. If you earned a satisfactory evaluation proceed to the next information sheet
6. If your self-check test is satisfactory proceed to the next learning guide,
7. If your self-check test is unsatisfactory, see your trainer for further instructions or go back to “information sheets”.

Information Sheet 1.1 Identifying information repositories

1.1. Identify information repositories across the business

Defining information

So what is information? What is the relationship between information, data and knowledge?

When information is entered and stored in a computer, it is generally referred to as "**data**." After processing (such as formatting and printing), output data can again be perceived as "**information**." When information is packaged or used for understanding or doing something, it is known as "**knowledge**".

An information repository is a collection of interrelated information maintained across a network on multiple servers. It creates a unified resource for anyone connected with the system to access when they need information. In general, there are three types of resources or sources of information: primary, secondary, and tertiary. It is important to understand these types and to know what type is appropriate for your coursework prior to searching for information.

In **information** technology, a **repository** is "a central place in which an aggregation of data is kept and maintained in an organized way, usually in computer storage. It "may be just the aggregation of data itself into some accessible place of storage or it may also imply some ability to selectively extract data.

The **repositories** constitute **information** systems that aim to organize, preserve and disseminate in the Open Access mode scientific and academic resources of the institutions.

A Business Process Repository is a central location for storing information about how an enterprise operates. This information may be contained in various media including paper, film or electronic form with a storage mechanism appropriate to the medium. Electronic repositories range from passive containers which store process artifacts (also referred to as process objects) to sophisticated tools that serve as active participants in monitoring, executing, managing and reporting on business processes. They come in the form of Document Management Systems, Process Modeling Tools and Business Process Management Systems. Administration of a

Business Process Repository includes activities such as storing, managing and changing process knowledge (objects, relationships.

Data or information may be collected from within the organisation (internal) or it may be sourced from external organisations. In order to collect the right information, you may need to read many documents and interview many people.

Types and sources of information

1. **Primary sources** are original materials on which other research is based, including:
    - original written works – poems, diaries, court records, interviews, surveys, and original research/fieldwork, and
    - research published in scholarly/academic journals.
2. **Secondary sources** are those that describe or analyze primary sources, including:
    - reference materials – dictionaries, encyclopedias, textbooks, and
    - books and articles that interpret, review, or synthesize original research/fieldwork.
3. **Tertiary sources** are those used to organize and locate secondary and primary sources.
    - Indexes – provide citations that fully identify a work with information such as author, titles of a book, article, and/or journal, publisher and publication date, volume and issue number and page numbers.
    - Abstracts – summarize the primary or secondary sources,
    - Databases – are online indexes that usually include abstracts for each primary or secondary resource, and may also include a digital copy of the resource.

Self-Check 1	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives. (Each 2 point)

1. Understanding of an information could be:
   A. Data C. Repository
   B. Wisdom D. Knowledge
2. _____is a central place in which an aggregation of data is kept and maintained in an organized way, usually in computer storage.
   A. Wisdom B. Knowledge C. Data D. Repository
3. Reference material is the best examples of _____sources of information.
   A. Tertiary Primary C. Secondary D. All of the above

Part II: Fill the blank spaces

1. When information is entered and stored in a computer, it is generally referred to as _____(1%).

2. List sources of information (3%)

_____

_____

_____

3. Write down at least 4 examples of primary sources of information. (4%).

_____

_____

_____

Note: Satisfactory rating 100%

You can ask you teacher for the copy of the correct answers.

Score = _____

Information Sheet 1.2 Review current organizational documentation

1.2 Reviewing the current organizational documentation

Documents and information

Documentation is any communicable material that is used to describe, explain or instruct regarding some attributes of an object, system or procedure, such as its parts, assembly, installation, maintenance and use. Documentation can be provided on paper, online, or on digital or analog media, such as audio tape or CDs.

Nearly everyone agrees that good documentation is important to the success of software projects, and yet very few projects actually have good documentation. Even successful projects often have barely adequate documentation.

Organizational documentation is the practical and formal reflection of the organizational structure. Described in the documentation are relationships between system and elements, which constitute the formal organizational structure of the company.

Organizational documentation is the practical and formal reflection of the organizational structure. Described in the documentation are relationships between system and elements, which constitute the formal organizational structure of the company.

For the proper functioning of any organization it is necessary to develop the documentation containing the overall description of the system. Documentation should facilitate the work of the personnel, as well as assist the leadership in the efficient management of the company.

The good news is that both these problems can be solved by understanding how documentation works, and that there are four distinct kinds of documentation - with four distinct functions.

The four kinds of documentation are:

- Learning-oriented tutorials
- goal-oriented how-to guides
- understanding-oriented discussions
- information-oriented reference material

An organisation stores a large number of documents such as policy documents, finance statements, annual reports and mission statements. These documents can provide valuable information when analysing user requirements. For example, mission statements may provide information regarding organisational goals. You may be required to review these documents to identify the kind of information they contain. The contents may be useful in the business requirements analysis.

Organizational Documentation may include the following tips.

1. The organizational documents of a business generally include the documents used to form or organize the business (registration documents) and the operational documents used to control activity within the business (operational documents)
2. The basic financial statements of an enterprise include the 1) balance sheet (or statement of financial position), 2) income statement, 3) cash flow statement, and 4) statement of changes in owners' equity or stockholders' equity. The balance sheet provides a snapshot of an entity as of a particular date.
3. Performance reports show the stakeholders the status of the project and its performance against the planned baselines. Examples of work performance reports include status reports, progress reports, trends report, earned value report, forecasting report, variance report, etc.
4. An organizational security policy is a set of rules or procedures that is imposed by an organization on its operations to protect its sensitive data.

Sources of information

When conducting a business user-requirements analysis, it is important to identify the sources of information. You will need to select different sources of information in order to gather complete and accurate information.

Table 1: Information sources

Repository/source	Information required
Management	To establish objectives, boundaries, constraints, policies, information requirements, involvement in the project, potential problems.
Clerical/operational staff	To establish actual procedures carried out, documents used, volume of work, job satisfaction, morale.
Statements of company policy including	These will provide information on overall objectives and likely changes.
Organization charts	Identify reporting responsibilities and staff names/positions.
Administrative procedure manuals	QA documents, instruction and procedure manuals which provide a statement of the way in which tasks are supposed to be performed.
Document blanks or data entry forms	These are forms that are filled in and passed between departments or stored for reference. This gives the analyst an indication of the formal data flows and data stores.
Completed documents or data entry forms	These are forms that have been filled in and passed between departments or stored for reference. These give the analyst an indication of the 'actual' data that is currently required.
Training manuals	To identify processes and procedures.
Sales and promotional literature	To identify products; company image; marketing style; target market.
Job descriptions and specifications	These should define the responsibilities of personnel.
Reports for decision making	Reports may include: sales; inventory; production; costing.
Performance reports	Identify gaps between actual performance and intended performance.
Intranet and website	Examine for metaphors, design features (such as colour). The intranet will be a valuable resource that can be searched for electronic copies of documents.
Memos and letters	May provide background for your problem statement and ultimate solution.

Organisational documents provide invaluable sources of information for analysing business needs. When gathering data for business needs, it is common to review organisational documents and categorise them according to the type of information they provide.

Self-Check 2	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives.(1 point each).

1. Documentation can be provided on:

A. Paper B. Audio C. CD D. DVD E. All are correct

2. Organizational Documentation may include the following tips.

A. Financial statement

B. An organizational security policy

C. Performance reports

D. All of the above

Part II: fill in the blank spaces.

- The four kinds of documentation are:- (4 point).

_____

_____

_____

_____

- What is documentation?(1 point).

_____

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Score = _____

Information Sheet 1.3 Developing critical questions

1.3 Developing critical questions

Introduction

When conducting usability studies or field studies, it's a great idea to ask lots of open-ended questions. Typically, researchers ask questions before, during, and after research sessions. It's easy to focus on what you want to know rather than on how you ask, but the way you ask questions matters a lot in terms of what and how much you can discover. You can learn unexpected and important things with this easy technique.

Definition

Open-ended questions are questions that allow someone to give a free-form answer.

Closed-ended questions can be answered with "Yes" or "No," or they have a limited set of possible answers (such as: A, B, C, or All of the above).

Closed-ended questions are often good for **surveys**, because you get higher response rates when users don't have to type so much. Also, answers to closed-ended questions can easily be analyzed statistically, which is what you usually want to do with survey data.

However, in **one-on-one usability testing**, you want to get richer data than what's provided from simple yes/no answers. If you test with 5 users, it's not interesting to report that, say, 60% of users answered "yes" to a certain question. No statistical significance, whatsoever. If you can get users to talk in depth about a question, however, you can absolutely derive valid information from 5 users. Not ***statistical*** insights, but ***qualitative*** insights.

Critical Questions

Steps to developing a research question:

Choose an interesting general topic. Most professional researchers focus on topics they are genuinely interested in studying

- Do some preliminary research on your general topic
- Consider your audience
- Start asking questions
- Evaluate your question
- Begin your research.

Here are some questions to guide you through the process of critical evaluation of information sources:

Authority: Who created the information?

- Who is the creator/author/source/publisher of the information? What are the author's credentials or affiliations?
- Is the author's expertise related to the subject? Are they an authority on the topic through education, experience, or expertise in the field?
- Whose voices/viewpoints are not being heard?

Accuracy: How accurate is the information?

- Was the information reviewed by others before being published? Does it contain spelling mistakes and grammatical errors?
- What citations or references support the author's claims?
- Is it fact or opinion? Do the authors leave out important facts or alternative perspectives?

Argument: What are the author's claims?

- What is the author's position?
- What reasons does the author give to support their position?
- Are there any flaws in the author's logic?
- Do you agree or disagree with the author's argument or perspective? Why?
- What is your position on this topic?

- What evidence (i.e. research) can you provide to support your position?

Self-Awareness: Check yourself

- Examine your own perspective and ensure you are seeking out information that represents alternative perspectives and worldviews.
- Ensure you are not seeking or favoring sources that only confirm your existing beliefs (avoid confirmation bias).
- Get uncomfortable. Read from sources across the spectrum (even if you do not agree with such sources); this will help ensure you are aware of the various sides of a debate/issue.

Relevance: Does the source satisfy your information need?

- Is the information related to your topic? Does it help you better understand your topic?
- Is the information at an appropriate depth or level for your assignment?

Timeliness: How current is the information?

- When the information was created, published or updated?
- Is it recent enough to be relevant to your topic or discipline? Sometimes you are required to use recently published material; sometimes you must use historical documents.

Self-Check 3	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives. (Each 1 point)

1. _____questions are questions that allow someone to give a free-form answer.

   A. Close-ended B. Open-ended

2. _____ Questions are often good for surveys**.**

   A. Close-ended B. open-ended

Part II: Fill the blank spaces

1. Write down at least 3 examples of closed ended questions. (4%)

_____

_____

_____

3. Write down at least 3 examples of open-ended questions. (3%).

_____

_____

_____

_____

_____

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Score = _____

Information Sheet 1.4 Ensuring information gathering techniques

Assess methods

Data gathering methods and budget constraints

There are a variety of different data gathering methods, and each have their own advantages and disadvantages. You will need to research the advantages and disadvantages of these methods. While you are undertaking your research, take notice of the relative costs associated with each method.

Your research should highlight that questionnaires are an effective method of capturing data from a large group of people at a relatively low cost; however, if the sample group is small, sometimes the questionnaire development costs outweigh the benefits. In the past, questionnaires have often been paper-based. A cost associated with paper-based surveys is the coding and transcribing of the responses into a computer for analysis. Using computer-based questionnaires reduces costs associated with coding and transcribing data.

You may find through your research that some authors refer to workshops as activities that last several days, involve high-level management and are conducted at remote locations using high-tech equipment. But this need not be the case. Given this insight, workshops are sometimes classified as an expensive method. This is due to costs associated with the venue, computing infrastructure, facilitator and management wages. However, if done correctly, workshops can return significant results in a short period of time because issues can be explored from a variety of perspectives, and resolutions can be arranged from a team perspective.

When determining requirements, the most common method of gathering data is the interview. The interview is usually a cost-effective method of gathering goal-focused information associated with the business requirements.

Reviewing documents

Reviewing documents is the process of searching, finding and extracting information from documents which have been created by authors. A listing of documents can be found in Table 1: Information sources.

If you are developing a website with e-commerce facilities, it may be worthwhile reviewing customer order forms and documents identifying sales processes and procedures. If you are interested in identifying the number of items per order or the number of incorrect orders received from customers, you may need to sample records kept by the organisation.

b. Interviews

An **interview** is a planned meeting during which you obtain information from another person. The personal interview is often the preferred information gathering technique when developing business and user requirements.

The interviewer can contextualise the response by observing body language. Body language is all of the non-verbal information being communicated by an individual. Part of body language is facial disclosure. Facial disclosure can sometimes enable you to understand how people feel by watching the expressions on their faces. Many common emotions have easily recognizable facial expressions.

Now let's look at the most common steps that take place during the interviewing process.

1. Determining the people to interview

You need to determine the people that can best satisfy the answers to your questions. Organisational charts and job specifications can help to identify appropriate people to interview. Table 1: Information sources, provides a list of information sources that may be useful in determining the right people with which to speak.

2. Establishing objectives for the interview

You need to be clear about what your objectives are for the interview. To do this, you should determine the general areas to be discussed, then list the facts that you want to gather. The

objectives of the interview will depend on the role of the person being interviewed. Upper management provides a "big picture" or overview which will help you understand the system as a whole. Specific details about operations and business processes are best learned from people who actually work with the system on a daily basis. Examples of goals can be found in the topic “Gather data through formal processes.”

3. Developing the interview questions

Creating a list of questions helps you keep on track during the interview. It is appropriate to include open and closed questions during the body of the interview. Extended discussion on questions can be found in the topic “Gather data through formal processes.”

4. Preparing for the interview

Preparation is the key to a successful interview. It is often easy to detect an unprepared interviewer. The interviewee is providing their valuable time, so you, as the interviewer, must be prepared. The interviewer should book and confirm their appointment times and venue. In addition, the goals or subject matter of the interview should be communicated to the interviewee.

5. Conducting the interview

An interview can be characterised as having three phases: the opening, the body and the conclusion.

During the interview opening, the interviewer should explain the reason for the interview, what the interviewer expects to get out of the interview, and motivate the interviewee to contribute to the interview.

The interview body represents the most time-consuming phase where you obtain the interviewee's responses to your questions and focus on your well-defined objectives.

Most interviewees will expect or at least permit you to take notes. Some interviewers use audio note-takers. While this can capture the entire interview, some interviewees may be hesitant to

express their opinions if they know that they have been recorded on tape. Typing on laptop computers can also be distracting during the interview process.

The interview conclusion allows you to summarise your understanding of the data gathered during the interview. You should express your appreciation for the interviewee's valuable time and instil a sense of value for the interviewee. You may need to follow-up with more questions, so the conclusion is an important time to develop rapport and trust with the interviewee.

6. Documenting the interview

It is important that you transcribe your notes into a format that allows you to understand the information gained at the interview. Sometimes, inexperienced interviewers do not capture the interview in writing until sometime after the interview. In these cases, the interviewer may lose many of the valuable facts gained in the interview. Some interviewees request copies of the interview transcript. This can be helpful in prompting the interviewee to volunteer information inadvertently omitted in the interview.

7. Evaluating the interview

It is important to review your notes and transcript to identify any areas of problem, bias or errors. The review may prompt further questions that need to be answered.

c. Questionnaires

Questionnaires are sometimes called surveys. A questionnaire involves questions written onto a form. The respondent provides their response in the form.

Two common formats for questionnaires are free-format and fixed-format. A single questionnaire often includes both formats.

- **Free-format questionnaires** offer the respondent greater latitude in their answer. A question is asked, and the respondent records the answer in the space provided after the question.

- **Fixed-format questionnaires** contain questions that quire the selection of predefined responses from individuals.

A typical questionnaire starts with a heading or title. This is usually followed by a brief statement of purpose and contact details for the person distributing the questionnaire. Often an introductory paragraph includes the deadline date for completion, as well as how and where to return the form. Instructions should be provided to give clear guidance on how to complete the form. Headings can be used to separate sections of the questionnaire. Your questionnaire may request the name and/or job role of the respondent; however, it has been found that anonymous responses often provide better information.

Questionnaires do not have to be paper-based. You may choose to distribute electronic questionnaires via e-mail, or you may request that respondents access a website and complete a questionnaire online.

d. Observation

Observation is a technique that enables the analyst to view how processes and activities are being done in the context of the business. This additional perspective can give a better understanding of system procedures. It is sometimes worthwhile to read procedure manuals to find out how things should be done. Then interview people to find out how they believe it is being done. Finally, observe processes to find out how it is actually being done.

e. Brainstorming

Brainstorming is a workshop or meeting where ideas are expressed and captured for later consideration. The three common rules of brainstorming are:

- Be spontaneous. Call out ideas as they occur.
- No criticism, analysis, or evaluation is permitted while the ideas are being generated. Any idea may be useful, if only to generate another idea.
- Focus on the quantity of ideas, rather than the quality of the ideas.

Categories of data

Quantitative vs. qualitative data

You may need to source quantitative data or qualitative data**.** Quantitative data can be measured. Sources include reports for decision making, performance reports, data capture forms, and numeric results from surveys and statistical research. Quantitative data can be analysed using mathematical equations and computation. Care needs to be taken to ensure that quantitative data is current and reliable - you may want to investigate the method of data capture and processing.

Qualitative data is a record of thoughts, observations, opinions or words. Qualitative data often comes from asking open-ended questions to which the answers are not limited by a set of choices or a scale. Qualitative data is important to capture; it may be in the form of memos, procedure manuals, survey responses, workshop results or policy guidelines. Care needs to be taken when analysing qualitative data to ensure that the information or data has not been authored in a way to bias or politically motivate receivers of information.

Sampling

When determining requirements, it is likely that you will have to collect information from a number of people. If the organisation is small, you may choose to collect information from all people - this is called a census. Alternatively, you may choose to collect information from only nominated specialists. This is known as judgement sampling or convenience sampling. Not all organisations are small and localised: consider determining requirements for an organisation with over 2000 computer users spread across 4 continents. In this situation, it is prudent to survey a sample of users. Two commonly used sampling techniques are **r**andomisation and systematic sampling.

- **Randomisation** is a sampling technique characterised as having no predetermined pattern or plan for selecting sample data.
- **Systematic sampling** is a technique that attempts to reduce the variance of the estimates by spreading out the sampling. One example would be choosing documents or records by formula which avoids very high or low estimates.

The use of sampling is much more time efficient, and that is why sampling is so commonly used. Unfortunately, the improper use of sampling can lead to methodological disaster.

Summary

In this resource you have identified the difference between data, information and knowledge. You are aware that there are different sources of information. These include internal or external, documents or people and the data you collect may be qualitative or quantitative data. When selecting samples, you may choose a census, a judgment sample/convenience sample, randomised sample or a systematic sample. From each of the nominated information sources you can expect to get a variety of information.

Self-Check 4	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives. (Each 1 point)

1. According to your readings, qualitative data can be defined as follows: “Qualitative data is a record of thoughts, observations, opinions or words.”
   A. True B. False
2. Collecting information from only nominated specialists is called:
   A. convenience sampling
   B. judgment sampling
   C. All of the above.
3. Which of the following is NOT usually regarded as a step of the interview process?
   A. determine the people to interview
   B. develop interview questions
   C. close the interview
   D. conduct the interview
   E. None of the above
4. Which of the following is can NOT be a data gathering method?
   A. Observation
   B. Interview
   C. Questionnaires
   D. None of the above

Part II: Fill the blank spaces

1. _____is a technique that enables the analyst to view how processes and activities are being done in the context of the business. (1%)
2. An_____ is a planned meeting during which you obtain information from another person. (1%).

3. The most common steps that take place during the interviewing process are: (7%).

_____

_____

_____

_____

_____

_____

_____

_____

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Score = _____

LG #18	LO #2- Determine user needs

Instruction sheet

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics:

- Identifying different segments of network based on business requirements
- Determining segment needs using network functional analysis
- Estimating traffic content and volumes

This guide will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Identify different segments of network based on business requirements
- Determine segment needs using network functional analysis
- Estimate traffic content and volumes

Learning Instructions:

Read the specific objectives of this Learning Guide.

1. Follow the instructions described below.
2. Read the information written in the “Information Sheets”. Try to understand what are being discussed. Ask your trainer for assistance if you have hard time understanding them.
3. Accomplish the “Self-checks” which are placed following all information sheets.
4. Ask from your trainer the key to correction (key answers) or you can request your trainer to correct your work. (You are to get the key answer only after you finished answering the Self-checks).
5. If you earned a satisfactory evaluation proceed to the next information sheet
6. If your self-check test is satisfactory proceed to the next learning guide,
7. If your self-check test is unsatisfactory, see your trainer for further instructions or go back to “information sheets”.

Information Sheet 2.1 Identifying different segments of network based on business requirements

2.1. Identifying different segments of network based on business requirements

A computer network or data network is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices exchange data with each other using a data link. The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

Network computer devices that originate, route and terminate the data are called network nodes.[1]Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices can be said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

Computer networks differ in the transmission medium used to carry their signals, the communications protocols to organize network traffic, the network's size, topology and organizational intent.

Computer networks support an enormous number of applications and services such as access to the World Wide Web, digital video, digital audio, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications as well as many others. In most cases, application-specific communications protocols are layered (i.e. carried as payload) over other more general communications protocols.

User Requirements

From the model of system components in our generic system, the user component is at the highest layer. The term user represents primarily the end users of the system, but it can be expanded to include everyone involved in the system, such as network and system administrators and management. User requirements is the set of requirements gathered or derived from user input and is what is needed by users to successfully accomplish their tasks on the system. Typically,

When gathering requirements, everyone involved with that network is considered a potential user.

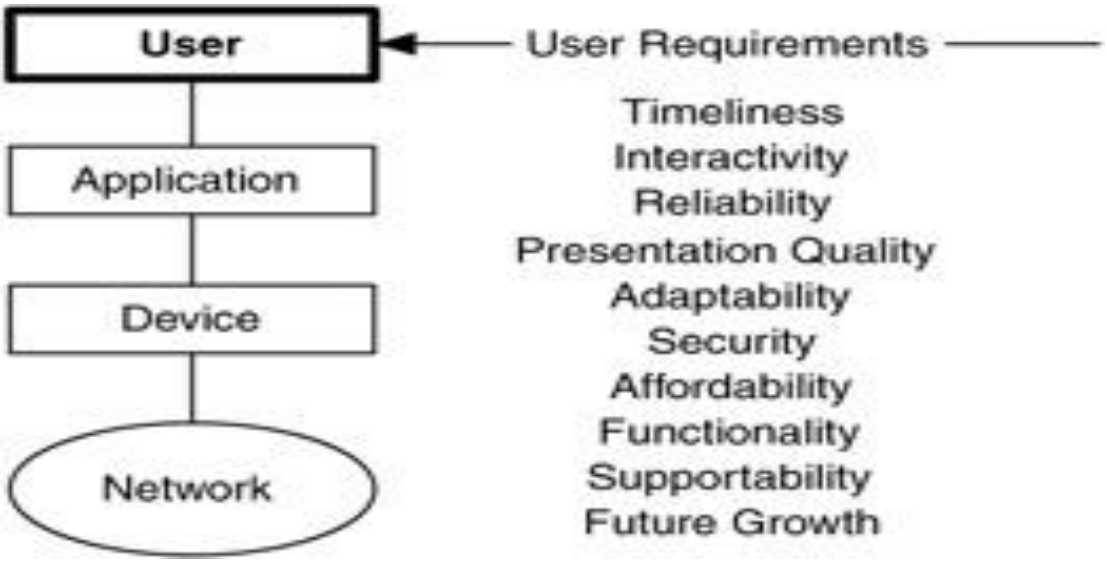


Figure 1. Types of user requirements.

We begin describing requirements at this layer, which will lead to the development of more specific requirements as we work through each of the components.

From the user perspective, we can ask, "What does it take to get the job done?" This will usually result in a set of qualitative, not quantitative, requirements. Part of our job in gathering and deriving user requirements is to make them quantitative whenever possible.

In general, the system should adapt to users and their environments, provide quick and reliable information access and transfer, and offer quality service to the user. This indicates the following general requirements:

- Timeliness
- Interactivity
- Reliability
- Presentation quality
- Adaptability
- Security

- Affordability
- Functionality
- Supportability
- Future growth

User requirements are the least technical and are also the most subjective. As shown in Figure 2.3, requirements become more technical as they move from users to the network. All of these requirements will be developed in more detail as we proceed through the application, device, and network components.

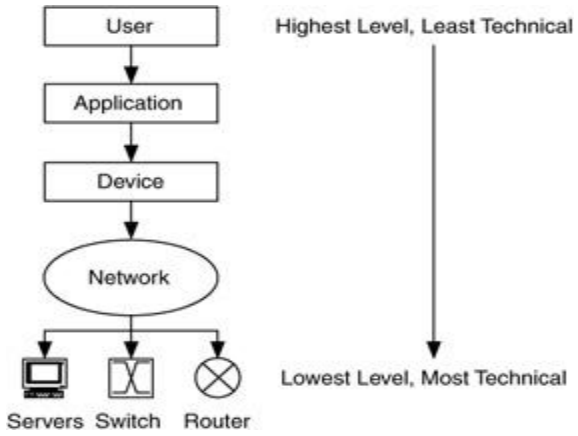


Figure 2. User requirements

Requirements are presented as a guide for you to use in developing requirements for your network, and they may change depending on the user's environment.

Timeliness is a requirement that the user is able to access, transfer, or modify information within a tolerable time frame. What a "tolerable" time frame is, of course, depends on the user's perception of delay in the system. It is this perception that we want to quantify. For example, a user may want to download files from a server and complete each transfer within 10 minutes. Or the user may need to receive video frames every 30 ms. Each one of these times indicates a delay that the network will need to provide. For timeliness, end-to-end or round-trip delay can be a useful measurement.

Interactivity is similar to timeliness but focuses on a response time from the system (as well as the network) that is on the order of the response times of users. In the preceding example, we could consider the 10 minutes needed to download a file as the response time for the system.

We further say that the file transfer is interacting with the user (which it is), but the degree of interactivity in this example is very low and not of much interest from an architectural or design perspective. What is interesting is when the system and network response times are close to the response times of users, for then changes that are made in the network architecture and design to optimize response times can have a direct impact on users' perception of interactivity. Therefore, interactivity is a measure of the response times of the system and network when they are required to actively interact with users. Delay, here the round-trip delay, is a measure of interactivity. Using these descriptions of timeliness and interactivity, timeliness is more likely to be associated with bulk file or image transfer, whereas interactivity is likely to be associated with remote device access (e.g., telnet), Web use, or visualization.

Reliability, that is, availability from the user's perspective, is a requirement for consistently available service. Not only must the user be able to have access to system resources a very high percentage of the time, but the level of service to the user (in terms of application usage or information delivery) must be consistent. Thus, reliability is closely related to the performance characteristic reliability (discussed in Chapter 1 as part of RMA), but delay and capacity are also important. It is likely that a combination of all performance characteristics would be used to describe reliability.

Presentation quality refers to the quality of the presentation to the user. This may be the user's perception of audio, video, and/or data displays. As examples, consider the current Internet capabilities of video conferencing, video feeds (live or delayed), and telephony. Although it is possible to do all of these on the Internet, there are other mechanisms that currently provide much better presentation quality. It is often not sufficient to provide a capability over a network—that capability must be *as* good *as or* better than other mechanisms, or the user will be disappointed. Network architects and designers often miss this concept. Measures of quality include all of the performance characteristics.

Adaptability is the ability of the system to adapt to users' changing needs. Some examples of this are in distance-independence and mobility. As users rely more and more on the network, they are becoming coupled to logical services and decoupled from physical servers.

This decoupling means that users do not have to care where servers are located, as long as they can get the services they need. A result of this is distance-independent computing, where the user loses all knowledge of where jobs are being executed, or where data are sourced, stored, or migrated through the network. Mobility refers to mobile or nomadic computing, where the user can access services and resources from any location, using portable devices and wireless access to the network. Adaptability to such user needs forces requirements on the system architecture and design.

Security from the user perspective is a requirement to guarantee the confidentiality, integrity, and authenticity of a user's information and physical resources, as well as access to user and system resources. Security is probably closest to the performance characteristic reliability, but it will affect capacity and delay as well.

Affordability is the requirement that purchases fit within a budget. Although this requirement is not technical, it will affect the architecture and design. Our goal in this requirement is to determine what users or management can afford to purchase for the network so that our architecture and design do not cost too much to implement. As a user requirement, we are looking for how costs and funding are tied to users, groups of users, and management. We will also discuss funding as a system-wide requirement, from an overall budget perspective.

Functionality encompasses any functional requirement that the user will have for the system. Functions that the system will perform are often tied to applications that are used on the system. Understanding functionality is important in that it will lead into application requirements (covered in the next section). Part of understanding functionality is determining which applications users actually want or apply in their daily work. We do not want to analyze applications that no one is planning to use.

Supportability is a set of characteristics that describe how well the customer can keep the network operating at designed performance through the full range of mission scenarios described by the customer during the requirements analysis process. This includes how users want or need to be supported by their network operations staff and any interfaces they will have with a network operations center (NOC).

For example, will the network need to be reconfigured to meet different or changing user needs? What applications will the network operations staff and/or NOC need to provide support to users and to identify and troubleshoot problems on the network? Information such as this will be used later as input to the network management architecture.

Types of Computer Network

Based on the area coverage of the network, computer networks can be divides into two

1. Local Area Network (LAN)
2. Wide area Network (WAN)
3. Metropolitan area Network (MAN)

LANs

- Local area networks are used to interconnect distributed communities of computers located within a single building or localized group of buildings.
- Since all equipment is located within a single establishment, LAN's are normally installed and maintained by the organization. Hence, they are also referred to as private data networks.
- Example: network in your class

MAN:

- Is a larger network that usually spans several buildings in the same city or town.
- Example: networks among Addis Ababa sub city administrations (Kifle Ketemas)

WANs

- When data communication is necessary or desired beyond the reach of a MAN, a wide area network (WAN) over public carrier networks is established.
- Institutions transferring large amounts of data between offices often decide to lease dedicated transmission lines from public carriers, in what is termed an enterprise-wide private network.
- Example: network among news agency offices in different region of Ethiopia.

VPN (Virtual Private Network: is an encrypted connection over the Internet from a device to a **network**. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

Explanation: A Virtual Private Network i.e. VPN is a technique used in networking or other intermediate networks for connecting computers and making them isolated remote computer networks, maintaining a tunnel of security and privacy.

A **virtual LAN** (**VLAN**) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). LAN is the abbreviation for local area network and in this context virtual refers to a physical object recreated and altered by additional logic. A Virtual Local Area Network (VLAN) is a logical division of computer systems in a LAN (Local Area Network) that are connected to a switch, based on their functionalities. VLANs are implemented for enhancing security between various departments and also for easy configuration.

Wireless Local Area Network (WLAN) – a network that connects two or more devices using a wireless distribution method and provides access to the public Internet. Most WLANs are based on Institute of Electrical and Electronic Engineers (IEEE) 802.11 standards, otherwise known as Wi-Fi. PSTN (public standard telephone network) uses an old technology whereby circuit-switched copper phone lines are used to transmit analogue voice data. It is the basic service that you have at home and in a small business. As a dedicated service, a PSTN line cannot be used for any other purpose while a call is being made.

Types of networks based on configuration (Node Relationship)

Terms to be familiar

- Servers—Computers that provide shared resources to network users.
- Clients—Computers that access shared network resources provided by a server.
- Media—the wires that make the physical connections.
- Shared data—Files provided to clients by servers across the network.
- Shared printers and other peripherals—Additional resources provided by servers.
- Resources—any service or device, such as files, printers, or other items, made available for use by members of the network.

Based on the computers relationship on the network, computer networks can be categorized as Peer to Peer and Server based network

Peer-to-Peer Networks

In a peer-to-peer network, there are no dedicated servers, and there is no hierarchy among the computers. All the computers are equal and therefore are known as peers. Each computer functions as both a client and a server, and there is no administrator responsible for the entire network. The user at each computer determines what data on that computer is shared on the network. Peer to peer network are also called Workgroup

Where a Peer-to-Peer Network Is Appropriate

Peer-to-peer networks are good choices for environments where:

- There are 10 users or fewer.
- Users share resources, such as files and printers, but no specialized servers exist.
- Security is not an issue.
- The organization and the network will experience only limited growth within the foreseeable future.

Where these factors apply, a peer-to-peer network will probably be a better choice than a server-based network.

Advantages of peer to peer network

- Easy to install and configure
- The cost of installation and operation is less
- A full time network administrator is not required

Disadvantages of peer to peer network

- Shared resources can be accessed by everyone
- Backup has to be performed on each computer separately
- No centralized security

Server Based network (client/server network)

In an environment with more than 10 users, a peer-to-peer network—with computers acting as both servers and clients—will probably not be adequate. Therefore, most networks have dedicated servers. A dedicated server is one that functions only as a server and is not used as a client or workstation.

Servers are described as "dedicated" because they are not themselves clients, and because they are optimized to service requests from network clients quickly and to ensure the security of files and directories. Server based network is also known as Domain.

Advantages of server based network

- Centralized resources
  - ✓ Easier to backup files
  - ✓ Easier to find files
- Efficient
- Security
  - ✓ One machine can secure entire network
  - ✓ One central login
- Scalability

Disadvantage of client server

- If the server goes down, it takes part or the whole network with it
- It is more expensive to install
- Needs to be maintained by staff with high IT skills

Specialized servers

Servers must perform varied and complex tasks. Servers for large networks have become specialized to accommodate the expanding needs of users. Following are examples of different types of servers included on many large networks

File and Print Servers

File and print servers manage user access and use of file and printer resources.

Application Servers

Application servers make the server side of client/server applications, as well as the data, available to clients.

Mail Servers

Mail servers operate like application servers in that there are separate server and client applications, with data selectively downloaded from the server to the client.

Fax Servers

Fax servers manage fax traffic into and out of the network by sharing one or more fax modem boards.

Communications Servers

Communications servers handle data flow and e-mail messages between the servers' own networks and other networks, mainframe computers, or remote users who dial in to the servers over modems and telephone lines.

Directory Services Servers

Directory services servers enable users to locate, store, and secure information on the network

Business requirements for network system

Identifying Business Requirements

Business requirements describe why the organization is undertaking the project. They state some benefits that the developing organization or its customers expect to receive from the product. Business requirements may be delineated in several documents such as a project charter, business case, or in a project vision and scope statements. Business requirements bring the project owner, stakeholders and the project team on the same song sheet. But you can't build software from such high-level information. In the Enforces Requirement Suite, ™ we consider the following business requirements.

- Problem Statement
- Project Vision
- Project Constraints (Budget, Schedule, and Resources)
- Project Objectives
- Project Scope Statements
- Business Process Analysis
- Stakeholder Analysis

The results from the business process analysis and stakeholder analysis activities are also considered business requirements. The purpose of the business process analysis is to determine how the business process will work. It is often necessary to resolve deficiencies in the business process before trying to automate it. Not dealing with the business process design first is like trying to pave a cow path; it might get you there, but it certainly won't be the straightest most direct path. The stakeholder analysis is needed to determine who will be impacted by the system and how to engage the impacted people to get their user requirements.

As the organization's network grows, so does the organization's dependency on the network and the applications that use it. Network-accessible organizational data and mission-critical applications that are essential to the organization's operations depend on network availability.

To design a network that meets customers' needs, the organizational goals, organizational constraints, technical goals, and technical constraints must be identified. This section describes the process of determining which applications and network services already exist and which ones are planned, along with associated organizational and technical goals and constraints. We begin by explaining how to assess the scope of the design project. After gathering all customer requirements, the designer must identify and obtain any missing information and reassess the scope of the design project to develop a comprehensive understanding of the customer's needs.

4 Key Factors to Consider When Creating an IT Network

- Understand your network goals. Surprisingly, not all businesses consider what the actual goal of their IT network is.
- Create a budget and acquire components.
- Training, security, and scalability.
- IT maintenance.

Self-Check 1	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives. (Each 1 point)

1. If Ambo University main Campus wants to develop a network for main branch that linked with Woliso FBE Campus, what network type is applicable for this situation in order to share information between the two Campuses?
   A. MAN
   B. WAN
   C. LAN
   D. All of the above
2. One of the following is not the main advantages of computer networking?
   A. Sharing of hardware
   B. Sharing of software
   C. Sharing of hardware and software
   D. Sharing of powers
3. **Which of the following is the Disadvantages of peer to peer network**
   A. Shared resources can be accessed by everyone
   B. Backup has to be performed on each computer separately
   C. No centralized security
   D. All of the above
4. _____is the wire that make the physical connections.
   A. Media B. Resource C. Client D. Server
5. VPN stands for _____.
   A. Very poor network
   B. Virtual private network
   C. Virtual local area network
   D. None of the above

Part II: Fill the blank spaces

1. What is the main difference between LAN, MAN and WAN? (3%)

   _____

   _____

   _____

   _____

2. Write down the advantages of server based network (4%).

   _____

   _____

   _____

   _____

   _____

Note: **Satisfactory rating 6 and 12 points**

You can ask you teacher for the copy of the correct answers.

Score = _____

Information Sheet 2.2. Determining segment needs using network functional analysis

2.2. Determining segment needs using network functional analysis

Network segmentation, which involves splitting the larger network into smaller network segments, can be accomplished through firewalls, virtual local area networks, and other separation techniques.

Determine best-fit topology for a local network

What evidence can you provide to prove your understanding of each of the following citeria?

Determine user needs

1. Identify the different segments of the proposed network based on business requirements
2. Determine segment needs, using network functional analysis
3. Estimate traffic content and volumes based on business requirements
4. Develop a prioritized organizational network functional matrix

Determine the resource requirements for each network segment on the basis of functional analysis

Develop local area network specification

1. Determine the resource requirements for each network segment on the basis of functional analysis
2. Analyse features of the physical environment for the effect on network design
3. Conduct a costing process for possible topology options
4. Consider topology options with reference to available resources and network functional matrix
5. Select and document appropriate network topology based on business requirements and functional analysis

Introducing Network Analysis

A network analyzer is a combination of hardware and software. Although there are differences in each product, a network analyzer is composed of five basic parts:

Hardware Most network analyzers are software-based and work with standard operating systems and network interface cards (NICs). However, some hardware network analyzers offer additional benefits such as analyzing hardware faults (e.g., cyclic redundancy check (CRC) errors, voltage problems, cable problems, jitter, jabber, negotiation errors, and so on). Some network analyzers only support Ethernet or wireless adapters, while others support multiple adapters and allow users to customize their configurations. Depending on the situation, you may also need a hub or a cable tap to connect to the existing cable.

Capture Driver This is the part of the network analyzer that is responsible for capturing raw network traffic from the cable. It filters out the traffic that you want to keep and stores the captured data in a buffer. This is the core of a network analyzer—you cannot capture data without it.

Buffer This component stores the captured data. Data can be stored in a buffer until it is full or in a rotation method (e.g., a round robin") where the newest data replaces the oldest data. Buffers can be disk-based or memory-based.

Real-time Analysis This feature analyzes the data as it comes off the cable. Some network analyzers use it to find network performance issues, and network intrusion detection systems use it to look for signs of intruder activity.

Decode This component displays the contents (with descriptions) of the network traffic so that it is readable. Decodes are specific to each protocol, thus network analyzers vary in the number of decodes they currently support. However, new decodes are constantly being added to network analyzers.

Notice: Jitter is the term that is used to describe the random variation of signal timing (e.g., electromagnetic interference and crosstalk with other signals can cause jitter).

Jabber is the term that is used to describe when a device is improperly handling electrical signals, thus affecting the rest of the network (e.g., faulty NICs can cause jabber).

Who Uses Network Analysis

System administrators, network engineers, security engineers, system operators, and programmers all use network analyzers, which are invaluable tools for diagnosing and troubleshooting network problems, system configuration issues, and application difficulties. Historically, network analyzers were dedicated hardware devices that were expensive and difficult to use. However, new advances in technology have allowed for the development of software-based network analyzers, which make it more convenient and affordable for administrators to effectively troubleshoot a network. It also brings the capability of network analysis.

The art of network analysis is a double-edged sword. While network, system, and security professionals use it for troubleshooting and monitoring the network, intruders use network analysis for harmful purposes. A network analyzer is a tool, and like all tools, it can be used for both good and bad purposes.

A network analyzer is used for:

- converting the binary data in packets to readable format
- Troubleshooting problems on the network
- analyzing the performance of a network to discover bottlenecks
- Network intrusion detection
- Logging network traffic for forensics and evidence
- analyzing the operations of applications
- discovering faulty network cards
- discovering the origin of virus outbreaks or Denial of Service (DoS) attacks
- Detecting spyware
- Network programming to debug in the development stage
- detecting a compromised computer
- Validating compliance with company policy
- As an educational resource when learning about protocols

Common Network Analyzers

A simple search on Security Focus (www.securityfocus.org/tools/category/4) shows the diversity and number of sniffers available. Some of the most prominent are:

Wireshark is one of the best sniffers available and is being developed as a free, commercial-quality sniffer. It has numerous features, a nice graphical user interface (GUI), decodes over 400 protocols, and is actively being developed and maintained. It runs on UNIX-based systems, Mac OS X, and Windows.This is a great sniffer to use in a production environment, and is available at www.wireshark.org.

WinDump is the Windows version of tcpdump, and is available at www.winpcap.org/windump. It uses the WinPcap library and runs on Windows 95, 98, ME, NT, 2000, and XP.

Network General Sniffer A Network General Sniffer is one of the most popular commercial sniffers available. Now a suite of enterprise network capture tools, there is an entire Sniffer product line at www.networkgeneral.com.

Windows 2000 and 2003 Server Network Monitor Both the Windows 2000 Server and the Windows 2003 Server have a built-in program to perform network analysis. It is located in the "Administrative Tools" folder, but is not installed by default; therefore, you have to add it from the installation CD.

Ether Peek is a commercial network analyzer developed by WildPackets.Versions for both Windows and Mac, and other network analysis products can be found at www.wildpackets.com.

Tcpdump is the oldest and most commonly used network sniffer, and was developed by the Network Research Group (NRG) of the Information and Computing Sciences Division (ICSD) at Lawrence Berkeley National Laboratory (LBNL). It is command line-based and runs on UNIX-based systems, including Mac OS X. It is actively developed and maintained at www.tcpdump.org.

Snoop Snoop is a command-line network sniffer that is included with the Sun Solaris OS.

Snort Snort is a network IDS that uses network sniffing, and is actively developed and maintained at www.snort.org. For more information, refer to Nessus, Snort, & Ethereal Power Tools: Customizing Open Source Security Applications (Syngress Publishing: 1597490202) and Snort Intrusion Detection and Prevention Toolkit (Syngress, ISBN: 1597490997).

Dsniff Dsniff is a very popular network-sniffing package. It is a collection of programs that are used to specifically sniff for interesting data (e.g., passwords) and to facilitate the sniffing process (e.g., evading switches). It is actively maintained at www.monkey.org/~dugsong/dsniff.

Ettercap was specifically designed to sniff a switched network. It has built-in features such as password collecting, OS fingerprinting, and character injection, and runs on several platforms including Linux, Windows, and Solaris. It is actively maintained at ettercap.sourceforge.net.

Analyzer is a free sniffer that is used for the Windows OS. It is being actively developed by the makers of WinPcap and WinDump at Politecnico di Torino, and can be downloaded from analyzer.polito.it.

Packetyzer is a free sniffer (used for the Windows OS) that uses Wireshark's core logic. It tends to run a version or two behind the current release of Wireshark. It is actively maintained by Network Chemistry at www.networkchemistry.com/products/packetyzer.php.

MacSniffer MacSniffer is specifically designed for the Mac OS environment. It is built as a front-end for tcpdump.The software is shareware and can be downloaded from personalpages.tds.net/~brian_hill/macsniffer.html.

Network Standards

Ethernet

This lesson introduces the Ethernet network architecture. Over the years, Ethernet has become the most popular media access method to the desktop computer and is used in both small and large network environments. Ethernet is a nonproprietary industry standard that has found wide acceptance by network hardware manufacturers. Problems related to using Ethernet hardware products from different hardware manufacturers in a single network are nearly nonexistent. This lesson presents an overview of the major Ethernet components, features, and functions.

Ethernet Features

Ethernet is currently the most popular network architecture. Notice that the cable is terminated at both ends. This baseband architecture uses a bus topology, usually transmits at 10 Mbps, and relies on CSMA/CD to regulate traffic on the main cable segment. The Ethernet media is passive, which means it requires no power source of its own and thus will not fail unless the media is physically cut or improperly terminated.

The Ethernet Frame Format

Ethernet breaks data down into packages in a format that is different from the packets used in other networks:

Ethernet breaks data down into frames. (Remember that the terms "packet" and "frame" can be used interchangeably; in the context of Ethernet, the term "frame" is used.) A *frame* is a package of information transmitted as a single unit. An Ethernet frame can be between 64 and 1518 bytes long, but the Ethernet frame itself uses at least 18 bytes; therefore, the data in an Ethernet frame can be between 46 and 1500 bytes long. Every frame contains control information and follows the same basic organization.

Ethernet specifications

The 10-Mbps IEEE Standards

This section looks at four 10 Mbps Ethernet topologies:

- 10BaseT
- 10Base2
- 10Base5
- 10BaseFL

10BaseT Standard

- 10 Mbps, baseband, over twisted-pair cable
- Mostly uses UTP but can also use STP
- Has a physical star and logical bus topology
- The maximum length of a 10BaseT segment is 100 meters (328 feet). Repeaters can be used to extend this maximum cable length. The minimum cable length between computers is 2.5 meters (about 8 feet). A 10BaseT LAN will serve 1024 computers

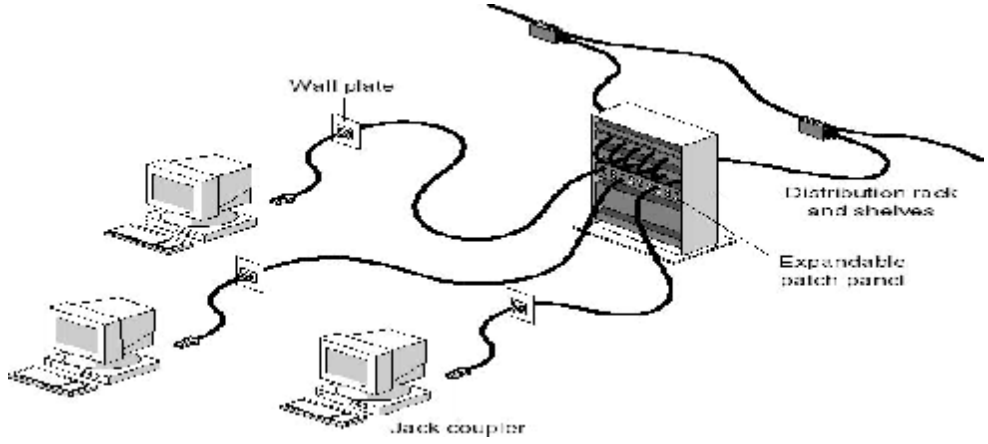


Figure 3. A patch panel makes moving computers easy

Table 3.10 BaseT Specifications Summary

Category	Notes
Cable	Category 3, 4, or 5 UTP.
Connectors	RJ-45 at cable ends.
Transceiver	Each computer needs one; some cards have built in transceivers.
Transceiver to hub distance	100 meters (328 feet) maximum.
Backbones for hubs	Coaxial or fiber-optic cable to join a larger LAN or to carry major traffic between smaller networks.
Total number of computers per LAN without connectivity components	1024 by specification.

10Base2 Standard

Another topology is *10Base2,* given this name in the IEEE 802.3 specification because it transmits at 10

Mbps over a baseband wire and can carry a signal about two times 100 meters (the actual distance is 185 meters, or 607 feet).

This type of network uses thin coaxial cable, or thinnet, which has a maximum segment length of 185 meters (607 feet) and a minimum cable length of at least 0.5 meters (20 inches) between workstations. There is also a 30-computer maximum per 185-meter segment.

A single thinnet network can support a maximum of 30 nodes (computers and repeaters) per cable segment, as per the IEEE 802.3 specification.

Table4: 10Base2 Specifications Summary

Category	**Notes**
Maximum segment length	185 meters (607 feet).
Connection to network interface card	BNC T connector.
Trunk segments and repeaters	Five segments can be joined using four repeaters.
Computers per segment	30 computers per segment by specification.
Segments that can have computers	Three of the five segments can be populated.
Maximum total network length	925 meters (3035 feet).

10Base5 Standard

The IEEE specification for this topology is 10 Mbps, baseband, and 500-meter (five 100-meters) segments. It is also called *standard Ethernet*.

This topology makes use of thick coaxial cable , also known as thicknet. Thicknet generally uses a bus topology and can support as many as 100 nodes (stations, repeaters, and so on) per backbone segment. The distances and tolerances for thicknet are greater than those for thinnet: a thicknet segment can be 500 meters (1640 feet) long for a total network length of 2500 meters (8200 feet).

Figure 4. Thicknet cable composition

The thicknet cabling components include:

- **Transceivers** These are devices that can both transmit and receive, provide communications between the computer and the main LAN cable, and are located in the vampire taps attached to the cable.

- **Transceiver cables** the transceiver cable (drop cable) connects the transceiver to the NIC.
- **DIX (or AUI) connectors** these are the connectors on the transceiver cable.
- **N-series connectors, including N-series barrel connectors, and N-series terminators** The thicknet components work in the same way as the thinnet components. It also shows the DIX or AUI connector on the transceiver cable.

NOTE

"AUI," an acronym for attachment unit interface, is a 15-pin (DB-15) connector commonly used to connect a NIC to an Ethernet cable;

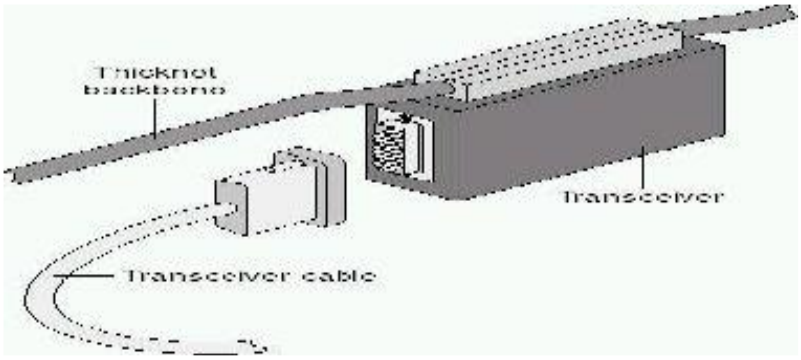


Figure 5. Thicknet backbone with attached transceiver and cable

Table 5. 10Base5 Specifications Summary

Category	**Notes**
Maximum segment length	500 meters (1640 feet).
Transceivers	Connected to the segment (in the tap).
Maximum computer-to-transceiver distance	50 meters (164 feet).
Minimum distance between transceivers	2.5 meters (8 feet).
Trunk segments and repeaters	Five segments can be joined using four repeaters.
Segments that can have computers	Three of the five segments can be populated.
Maximum total length of joined segments	2500 meters (8200 feet).
Maximum number of computers per segment	100 by specification.

10BaseFL Standard

The IEEE committee published a specification for running Ethernet over fiber-optic cable. The result,

10BaseFL (10Mbps, baseband, over fiber-optic cable) is an Ethernet network that typically uses fiber-optic cable to connect computers and repeaters.

The primary reason for using 10BaseFL is to accommodate long cable runs between repeaters, such as between buildings. The maximum distance for a 10BaseFL segment is 2000 meters (about 6500 feet).

The 100-Mbps IEEE Standards

New Ethernet standards are pushing the traditional Ethernet limits beyond the original 10 Mbps. These new capabilities are being developed to handle such high band width applications as:

- Computer-aided design (CAD).
- Computer-aided manufacturing (CAM).
- Video.
- Imaging and document storage. Two Ethernet standards that can meet the increased demands are:
- 100BaseVG-AnyLAN Ethernet.
- 100BaseX Ethernet (Fast Ethernet).

Both 100BaseVG-AnyLAN and Fast Ethernet are about 5 to 10 times faster than standard Ethernet. They are also compatible with existing 10BaseT cabling systems. This means they allow for Plug and Play upgrades from existing 10BaseT installations.

100VG-AnyLAN Standard

The 100VG (Voice Grade) AnyLAN is an emerging networking technology that combines elements of both Ethernet and Token Ring architectures. Originally developed by Hewlett-Packard, it is currently being refined and ratified by the IEEE 802.12 committee. The 802.12 specification is a standard for transmitting 802.3 Ethernet frames and 802.5 Token Ring packets.

This technology goes by any of the following names, all of which refer to the same type of network:

- 100VG-AnyLAN
- 100BaseVG
- VG
- Any LAN

Specifications

Some of the current 100VG-AnyLAN specifications include:

- A minimum data rate of 100 Mbps.
- The ability to support a cascaded star topology over Category 3, 4, and 5 twisted-pair and fiber-optic cable.
- The demand-priority access method that allows for two priority levels (low and high).
- The ability to support an option for filtering individually addressed frames at the hub to enhance privacy.
- Support for both Ethernet frames and Token Ring packets.

100BaseX Ethernet Standard

This standard, sometimes called *Fast Ethernet*, is an extension of the existing Ethernet standard. It runs on UTP Category 5 data-grade cable and uses CSMA/CD in a star-wired bus topology, similar to 10BaseT where all cables are attached to a hub.

Media Specifications

100BaseX incorporates three media specifications:

- 100BaseT4 (4-pair Category 3, 4, or 5 UTP)
- 100BaseTX (2-pair Category 5 UTP or STP)
- 100BaseFX (2-strand fiber-optic cable)

Table 7. 100BaseX Media Specifications

Value	Represents	Actual meaning
100	Transmission speed	100 Mbps
Base	Signal type	Baseband
T4	Cable type	Indicates twisted-pair cable using four telephone-grade pairs
TX	Cable type	Indicates twisted-pair cable using two data-grade pairs
FX	Cable type	Indicates fiber-optic link using two strands of fiber-optic cable

Performance Considerations

Ethernet architecture can use multiple communication protocols and can connect mixed computing environments such as Netware, UNIX, Windows, and Macintosh.

Segmentation

Ethernet performance can be improved by dividing a crowded segment into two less-populated segments and joining them with either a bridge or a router. This reduces traffic on each segment. Because fewer computers are attempting to transmit onto the segment, access time improves.

Network Operating Systems on Ethernet

Ethernet will work with most popular network operating systems including:

- Microsoft Windows XP, Windows Vista, Windows Seven, Windows server 2003/2008
- Unix
- Novell NetWare.
- IBM LAN Server.
- AppleShare.

Table 8. Ethernet Specifications (IEEE 802.3) summary table

	10Base2	**10Base5**	**10BaseT**
Topology	Bus	Bus	Star bus
Cable type	RG-58 (thinnet coaxial cable)	Thicknet; one-centimeter (3/8- inch) shielded transceiver cable	Category 3, 4, or 5 unshielded twisted-pair cable
Connection to NIC	BNC T connector	DIX or AUI connector	RJ-45
Distance	0.5 meters between computers (23 inches)	2.5 meters (8 feet) between taps and maximum of 50 meters (164 feet) between the tap and the computer	100 meters (328 feet) between the transceiver (the computer) and the hub
Maximum cable segment length	185 meters (607 feet)	500 meters (1640 feet)	100 meters (328 feet)
Maximum connected Segments	5 (using 4 repeaters); Only 3 segments can have computers connected.	5 (using 4 repeaters). Only 3 segments can have computers connected.	Not applicable
Maximum total network length	925 meters (3035 feet)	2460 meters (8000 feet)	Not applicable
Maximum computers per segment	30 (There can be a maximum of 1024 Computers per network.)	100	

Self-Check 2	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives. (1 point each).

1. a network analyzer is composed of :
   A. Hardware C. Buffer
   B. Capture Driver D. Real-time Analysis E. All of the above
2. A network analyzer is used for :

   A. converting the binary data in packets to readable format

   B. Troubleshooting problems on the network

   C. analyzing the performance of a network to discover bottlenecks

   D. Network intrusion detection E. All of the above

Part II: fill in the blank spaces.

1. A _____is a combination of hardware and software. (**network analyzer**)
2. _____ is the term that is used to describe the random variation of signal timing (e.g., electromagnetic interference and crosstalk with other signals.(**Jitte**r)
3. _____is a command-line network sniffer that is included with the Sun Solaris OS. (**snoop**).
4. _____involves splitting the larger network into smaller network segments, can be accomplished through firewalls, virtual local area networks, and other separation techniques.(Network segmentation)

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Score = _____

Information Sheet 2.3. Estimating traffic content and volumes

2.3. Estimating traffic content and volumes

Segmenting at its most basic level is the process of separating certain portions of **network** traffic, either for performance, security, or reliability reasons. You can use a bridge, a switch, or a router to separate your **network's** devices into **segments**.

Network traffic or **data traffic** is the amount of data moving across a network at a given point of time. Network data in computer networks is mostly encapsulated in network packets, which provide the load in the network. Network traffic is the main component for network traffic measurement, network traffic control and simulation.

Network traffic refers to the amount of data moving across a network at a given point of time. Network data is mostly encapsulated in network packets, which provide the load in the network. Network traffic is the main component for network traffic measurement, network traffic control and simulation.

The proper organization of network traffic helps in ensuring the quality of service in a given network.

- Network traffic control - managing, prioritizing, controlling or reducing the network traffic
- Network traffic measurement - measuring the amount and type of traffic on a particular network
- Network traffic simulation - to measure the efficiency of a communications network
- Traffic generation model - is a stochastic model of the traffic flows or data sources in a communication computer network.

Proper analysis of network traffic provides the organization with the network security as a benefit - unusual amount of traffic in a network is a possible sign of an attack. Network traffic reports provide valuable insights into preventing such attacks. [2]

Traffic volume is a measure of the total works done by a resource or facility, normally over 24 hours, and is measured in units of-hours. It is defined as the product of the average traffic intensity and the time period of the study.

Network traffic or data traffic is the amount of data moving across a network at a given point of ... Traffic volume is a measure of the total work done by a resource or facility, normally over 24 hours, and is measured in units of ... Main page · Contents ·

The Major difference between voice and data traffic

The major **difference** between **voice** and **data traffic** is the fact that **data** packets can be re-sent if they are dropped, and then applied to the empty spots in **data**, thereby producing complete information. With **voice**, there is no point in resending packets because **voice** only makes sense in a stream of contiguous packets.

Self-Check 3	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page

Fill in the blank spaces.

1. _____refers to the amount of data moving across a network at a given point of time.(**Network traffic or data traffic**)
2. _____is used to measure the efficiency of a communications network(**Network traffic simulation)**
3. _____is the main component for network traffic measurement, network traffic control and simulation. (**Network traffic**).

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Score = _____

LG #19	LO #3- Develop best topology

Instruction sheet

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics:

- Determining resource requirements for each network segment
- Analyzing features of the physical environment on network design
- Conducting costing process for possible topology
- Selecting and documenting appropriate network topology

This guide will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Determine resource requirements for each network segment
- Analyze features of the physical environment on network design
- Conduct costing process for possible topology
- Select and documenting appropriate network topology

Learning Instructions:

Read the specific objectives of this Learning Guide.

1. Follow the instructions described below.
2. Read the information written in the “Information Sheets”. Try to understand what are being discussed. Ask your trainer for assistance if you have hard time understanding them.
3. Accomplish the “Self-checks” which are placed following all information sheets.
4. Ask from your trainer the key to correction (key answers) or you can request your trainer to correct your work. (You are to get the key answer only after you finished answering the Self-checks).
5. If you earned a satisfactory evaluation proceed to the next information sheet
6. If your self-check test is satisfactory proceed to the next learning guide,
7. If your self-check test is unsatisfactory, see your trainer for further instructions or go back to “information sheets”.

Information sheet 3.1 Determining resource requirements for each network segment

3.1. Determining resource requirements for each network segment

Network Topology

The term *topology*, or more specifically, network topology, refers to the arrangement or physical layout of computers, cables, and other components on the network. "Topology" is the standard term that most network professionals use when they refer to the network's basic design. In addition to the term "topology," you will find several other terms that are used to define a network's design:

- Physical layout
- Design
- Diagram
- Map

A network's topology affects its capabilities. The choice of one topology over another will have an impact on the:

- Type of equipment the network needs.
- Capabilities of the equipment.
- Growth of the network.
- Way the network is managed.

Developing a sense of how to use the different topologies is a key to understanding the capabilities of the different types of networks. Before computers can share resources or perform other communication tasks they must be connected. Most networks use cable to connect one computer to another.

Category of Topology

1. Logical: describes the way network data flows through the physical components.
2. Physical: Physical topology describes how the physical components on a network are connected.

Standard Topologies

All network designs stem from four basic topologies:

- Bus
- Star
- Ring
- Mesh

Bus Topology

The bus topology is often referred to as a "linear bus" because the computers are connected in a straight line.

This is the simplest and most common method of networking computers.

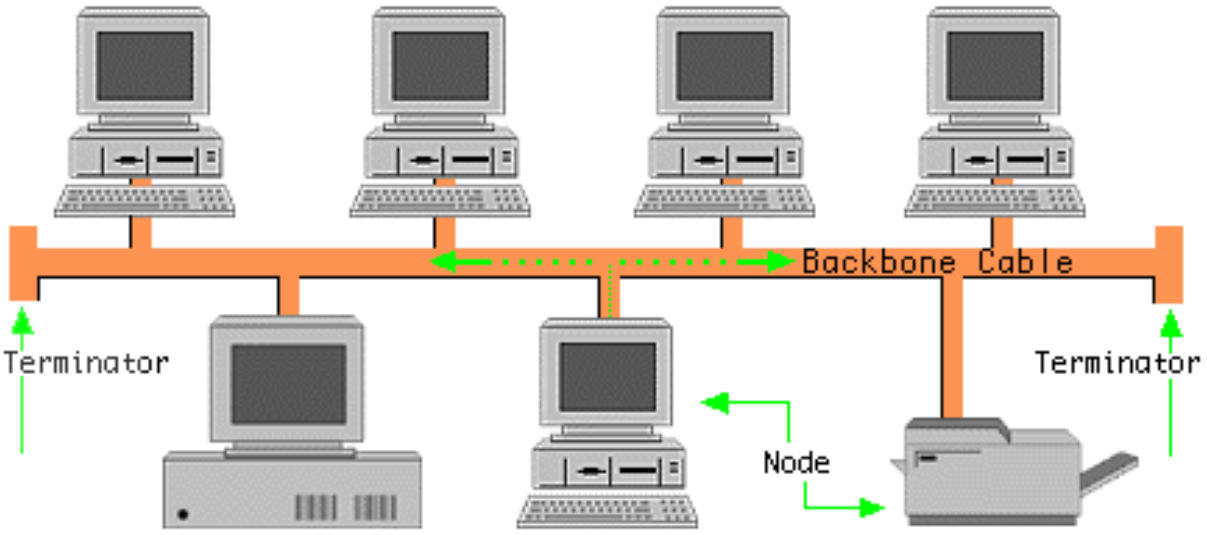


Figure 6. Communication on the Bus

Computers on a bus topology network communicate by addressing data to a particular computer and sending out that data on the cable as electronic signals. To understand how computers communicate on a bus, you need to be familiar with three concepts:

- Sending the signal
- Signal bounce
- Terminator

Sending the Signal Network data in the form of electronic signals is sent to all the computers on the network. Only the computer whose address matches the address encoded in the original signal accepts the information. All other computers reject the data. Only one computer at a time can send messages. Because only one computer at a time can send data on a bus network, the number of computers attached to the bus will affect network performance. The more computers there are on a bus, the more computers will be waiting to put data on the bus and, consequently, the slower the network will be. Computers on a bus either transmit data to other computers on the network or listen for data from other computers on the network. They are not responsible for moving data from one computer to the next. Consequently, if one computer fails, it does not affect the rest of the network.

Signal Bounce Because the data, or electronic signal, is sent to the entire network, it travels from one end of the cable to the other. If the signal is allowed to continue uninterrupted, it will keep bouncing back and forth along the cable and prevent other computers from sending signals. Therefore, the signal must be stopped after it has had a chance to reach the proper destination address.

Terminator To stop the signal from bouncing, a component called a *terminator* is placed at each end of the cable to absorb free signals. Absorbing the signal clears the cable so that other computers can send data. A break in the cable will bounce signal and all network activity will stop. The network will not work because it has unterminated cables

Disadvantages of Bus topology

- If there is a break anywhere in the cable or if an end is not terminated, the signal will travel back and forth across the network and all communication will stop.
- The more computers there are on the bus, the greater the backup of computers waiting to put data on the bus, and consequently, the slower the network.

- In addition, because of the way computers communicate in a bus topology, there may be a lot of noise. Noise is the traffic generated on the network when computers attempt to communicate with each other simultaneously.

Star Topology

In the star topology, cable segments from each computer are connected to a centralized component called a *hub or switch*. Signals are transmitted from the sending computer through the hub to all computers on the network

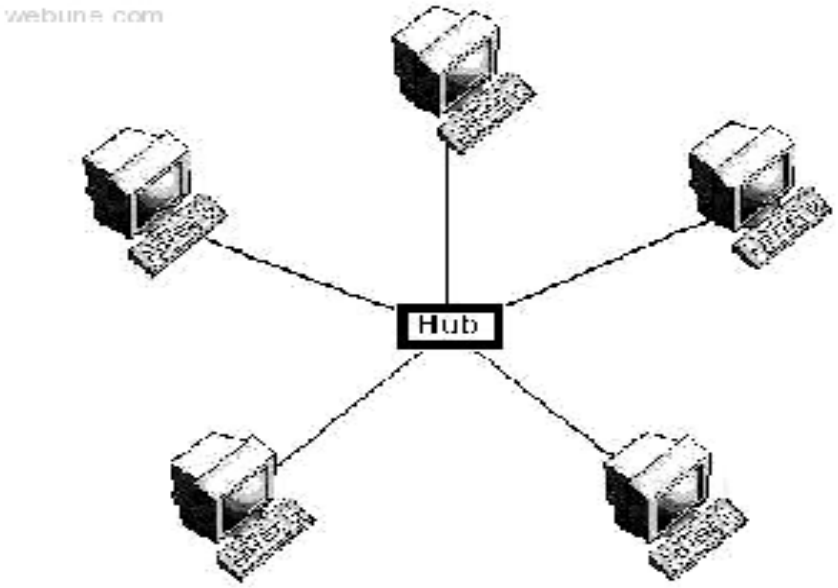


Figure 7. Star topology

Advantage of Star topology

An advantage of the star topology is that if one computer on the star topology fails, only the failed computer is unable to send or receive data. The remainder of the network functions normally.

Disadvantage of star topology

The disadvantage of using this topology is that because each computer is connected to a hub, if the hub fails, the entire network fails. In addition, noise is created on the network in a star topology.

Ring Topology

The ring topology connects computers on a single circle of cable. Unlike the bus topology, there are no terminated ends. The signals travel around the loop in one direction and pass through each computer, which can act as a repeater to boost the signal and send it on to the next computer.

One method of transmitting data around a ring is called *token passing*. (A *token* is a special series of bits that travels around a token-ring network. Each network has only one token.) The token is passed from computer to computer until it gets to a computer that has data to send. The sending computer modifies the token, puts an electronic address on the data, and sends it around the ring. The data passes by each computer until it finds the one with an address that matches the address on the data.

The receiving computer returns a message to the sending computer indicating that the data has been received. After verification, the sending computer creates a new token and releases it on the network. The token circulates within the ring until a workstation needs it to send data.

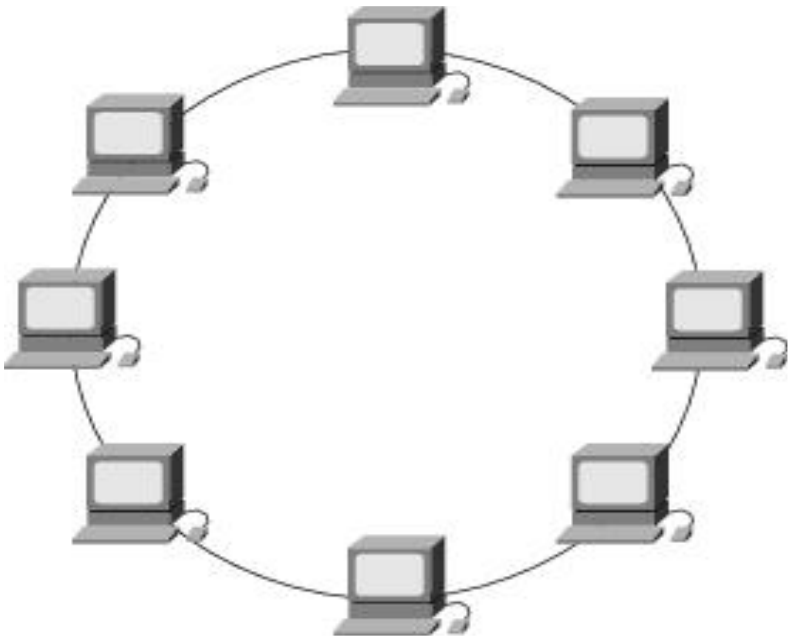


Figure 8. Ring topology

Advantage of Ring topology

- The advantage of a ring topology is that each computer acts as a repeater, regenerating the signal and sending it on to the next computer, thereby preserving signal strength.

Disadvantage of Ring topology

- The disadvantage of a ring topology is that only one computer at a time can send data on a single token ring. Also, ring topologies are usually more expensive than bus technologies.
- If one computer fails, the network will fail

Mesh Topology

A mesh topology network offers superior redundancy and reliability. In a mesh topology, each computer is connected to every other computer by separate cabling. This configuration provides redundant paths throughout the network so that if one cable fails, another will take over the traffic. While ease of troubleshooting and increased reliability is definite pluses, these networks are expensive to install because they use a lot of cabling.

Advantage of Mesh topology

- An advantage of a mesh topology is its back-up capabilities by providing multiple paths through the network.

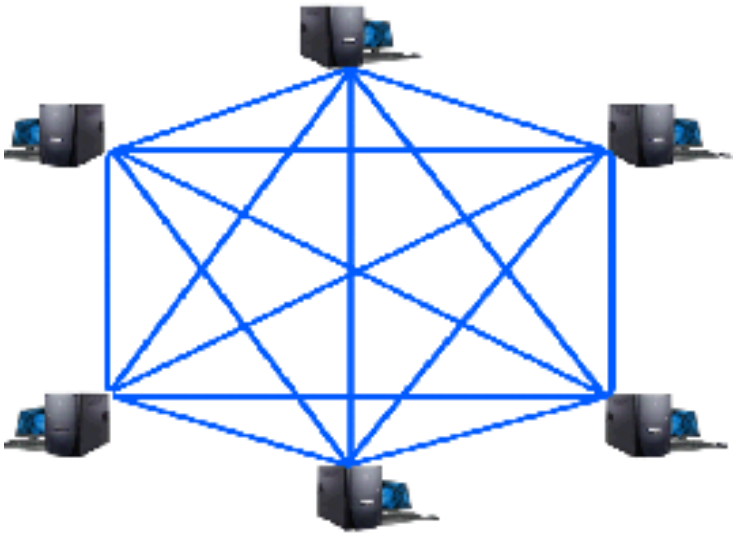


Figure 9. Mesh topology

Disadvantage of Mesh topology

- Because redundant paths require more cable than is needed in other topologies, a mesh topology can be expensive.

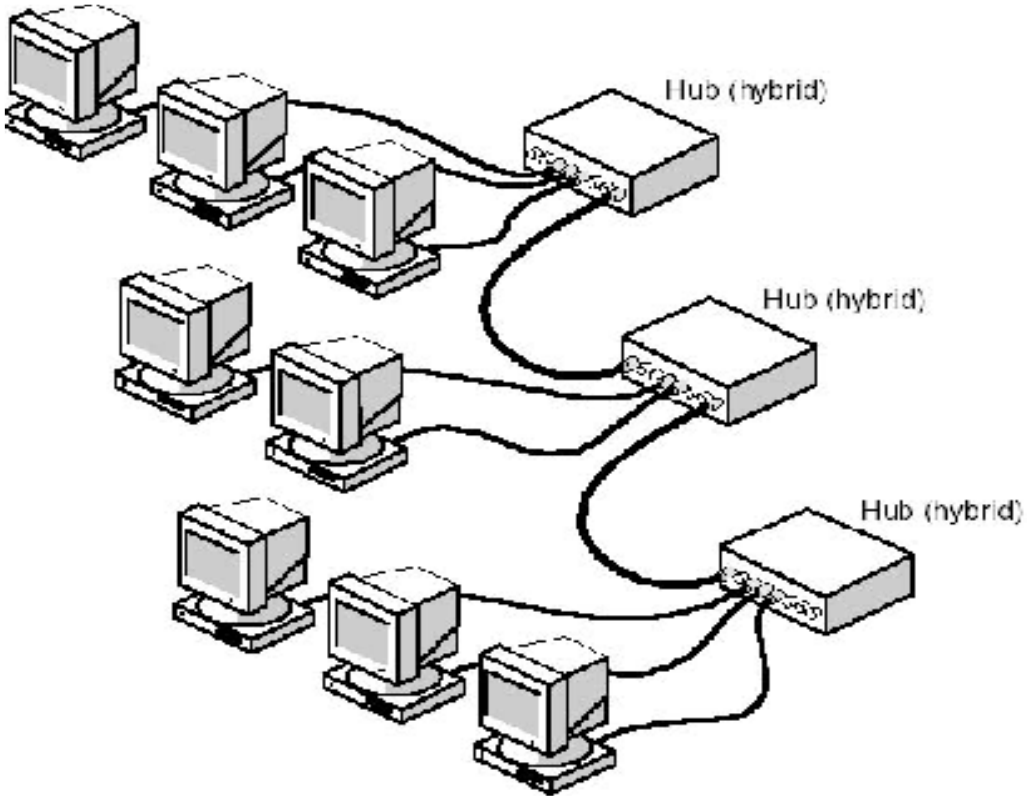


Figure 10 Hybrid Topology

Star Bus

The *star bus* is a combination of the bus and star topologies. In a star-bus topology, several star topology networks are linked together with linear bus trunks.

If one computer goes down, it will not affect the rest of the network. The other computers can continue to communicate. If a hub goes down, all computers on that hub are unable to communicate.

Star Ring

The *star ring* (sometimes called a star-wired ring) appears similar to the star bus. Both the star ring and the star bus are centered in a hub that contains the actual ring or bus. Linear-bus trunks connect the hubs in a star bus, while the hubs in a star ring are connected in a star pattern by the main hub.

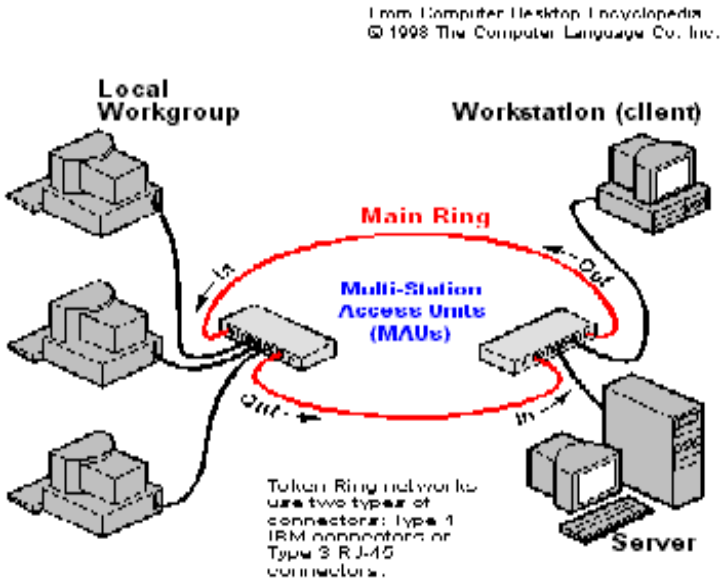


Figure 11. Star ring topology

Selecting a topology

There are many factors to consider when deciding which topology best suits the needs of an organization.

The following table provides some guidelines for selecting a topology.

Table 9. Summary of topology

Topology	Advantages	Disadvantages
Bus	▪ Use of cable is economical. ▪ Media is inexpensive and easy to work with. ▪ System is simple and reliable. ▪ Bus is easy to extend.	▪ Network can slow down in heavy traffic. ▪ Problems are difficult to isolate. ▪ Cable break can affect many users.
Ring	▪ System provides equal access for all computers. ▪ Performance is even despite many users.	▪ Failure of one computer can impact the rest of the network. ▪ Problems are hard to isolate. ▪ Network reconfiguration disrupts operation.
Star	▪ Modifying system and adding new computers is easy. ▪ Centralized monitoring and management are possible. ▪ Failure of one computer does not affect the rest of the network.	▪ If the centralized point fails, the network fails.
Mesh	▪ System provides increased redundancy and reliability as well as ease of troubleshooting.	▪ System is expensive to install because it uses a lot of cabling.

Network connectivity devices

Network Interface Cards (NIC)

- Also called network adapter
- Receive data and convert it into electrical signals
- Receive electrical signals and convert them into data
- Determine if the data received is for a particular computer
- Control the flow of data through the cable

Network adapters constitute the physical interface between the computer and the network cable. Network adapters, also known as network interface cards, are installed into an expansion slot in each computer and server on the network. After the network adapter is installed, the network cable is attached to the adapter's port to physically connect the computer to the network.

Figure 12. Network Interface Cards

As the data passes through the cable to the network adapter, it is formatted into *packets*. A packet is a logical grouping of information that includes a header, which contains location information and user data. The header contains address fields that include information about the data's origin and destination. The network adapter reads the destination address to determine if the packet is to be delivered to this computer. If it is, the network adapter then passes the packet on to the operating system for processing. If not, the network adapter discards the packet.

Each network adapter has a unique address that is incorporated into chips on the card. This address is called the physical, or media access control (MAC), address.

The network adapter performs the following functions:

- Receives data from the computer's operating system and converts it into electrical signals that are transmitted onto the cable

- Receives electrical signals from the cable and translates them into data that the computer's operating system can understand
- Determines whether data received from the cable is intended for the computer
- Controls the flow of data between the computer and the cabling system

To ensure compatibility between the computer and the network, the network adapter must meet the following criteria:

Fit in the computer's expansion slot

- Use the correct type of cable connector for the cabling
- Be supported by the computer's operating system

Repeaters

As signals travel along a cable, they degrade and become distorted in a process called "attenuation." If a cable is long enough, attenuation will finally make a signal unrecognizable. Installing a repeater enables signals to travel farther.

Repeater Considerations

Repeaters afford the least expensive way to expand a network. When the need arises to extend the physical network beyond its distance or node limitations, consider using a repeater to link segments if neither segment is generating much traffic or limiting costs is a major consideration.

No Isolation or Filtering Repeaters send every bit of data from one cable segment to another, even if the data consists of malformed packets or packets not destined for use on the network. This means that a problem with one segment can disrupt every other segment. Repeaters do not act as filters to restrict the flow of problem traffic.

Use a repeater to:

- Connect two segments of similar or dissimilar media.
- Regenerate the signal to increase the distance transmitted.
- Pass all traffic in both directions.
- Connect two segments in the most cost-effective manner.

Do not use a repeater when:

- There is heavy network traffic.
- Segments are using different access methods.
- Data filtering is needed.

Hubs

Hubs are connectivity devices that connect computers in a star topology. Hubs contain multiple ports for connecting to network components. If you use a hub, a break in the network does not affect the entire network; only the segment and the computer attached to that segment fail.

A Hub works at the physical layer of the OSI Reference Model to regenerate the network's signals and resend them out on other segments. Hubs are multiport repeater

A single data packet sent through a hub goes to all connected computers. There are two types of hubs:

Passive Hubs: Send the incoming signal directly through their ports without any signal processing. These hubs are usually wiring panels.

Active Hubs: Sometimes called *multiport repeaters*, receive incoming signals, process the signals, and retransmit them at their original strengths and definitions to the connected computers or components.

Use a hub to:

- Easily change and expand wiring systems.
- Use different ports to accommodate a variety of cable types.
- Enable central monitoring of network activity and traffic.

Bridges

Like a repeater, a bridge can join segments or workgroup LANs. However, a bridge can also divide a network to isolate traffic or problems. For example, if the volume of traffic from one or two computers or a single department is flooding the network with data and slowing down the entire operation, a bridge could isolate those computers or that department.

Bridges can be used to:

- Expand the length of a segment.
- Provide for an increased number of computers on the network.
- Reduce traffic bottlenecks resulting from an excessive number of attached computers.
- Split an overloaded network into two separate networks, reducing the amount of traffic on each segment and making each network more efficient.
- Link unlike physical media such as twisted-pair and coaxial Ethernet.

How Bridges Work

Because bridges work at the data-link layer of the OSI reference model, all information contained in the higher levels of the OSI reference model is unavailable to them. Rather than distinguish between one protocol and another, bridges simply pass all protocols along the network. All protocols pass across bridges, so it is up to the individual computers to determine which protocols they can recognize.

As discussed in previous topics the data-link layer has two sub layers: the Logical Link Control (LLC) sub layer and the Media Access Control (MAC) sub layer. Bridges work at the MAC sub layer and are sometimes referred to as MAC-layer bridges.

A MAC-layer bridge:

- Listens to all traffic.
- Checks the source and destination addresses of each packet.
- Builds a routing table, as information becomes available.
- Forwards packets in the following manner:
  - ✓ If the destination is not listed in the routing table, the bridge forwards the packets to all segments.
  - ✓ If the destination is listed in the routing table, the bridge forwards the packets to that segment (unless it is the same segment as the source).

A bridge works on the principle that each network node has its own address. A bridge forwards packets based on the address of the destination node.

Initially, the bridge's routing table is empty. As nodes transmit packets, the source address is copied to the routing table. With this address information the bridge learns which computers are on which segment of the network.

Switch

Switches are similar to bridges but offer a more direct network connection between the source and destination computers. When a switch receives a data packet, it creates a separate internal connection, or segment, between any two of its ports and forwards the data packet to the appropriate port of the destination computer only, based on information in each packet's header. This insulates the connection from the other ports and gives the source and destination computers access to the full bandwidth of a network. Unlike a hub, switches are comparable to a telephone system with private lines.

In such a system, if one person calls someone, the operator or telephone switch connects them on a dedicated line. This allows more conversations to take place at any one time.

Use a switch to:

- Send a packet directly from the source computer to the destination computer.
- Provide for a greater rate of data transmission.

Routers

In an environment that consists of several network segments with differing protocols and architectures, a bridge might be inadequate for ensuring fast communication among all segments. A network this complex needs a device that not only knows the address of each segment, but can also determine the best path for sending data and filtering broadcast traffic to the local segment. Such a device is called a "router."

Routers work at the network layer of the OSI reference model. This means they can switch and route packets across multiple networks. They do this by exchanging protocol-specific information between separate networks. Routers read complex network addressing information in the packet and, because they function at a higher layer in the OSI reference model than bridges, they have access to additional information.

Routers can provide the following functions of a bridge:

- Filtering and isolating traffic
- Connecting network segments

Types of Routers

The two major types of routers are:

- **Static.**

  Static routers require an administrator to manually set up and configure the routing table and to specify each route.

- **Dynamic.**

  Dynamic routers are designed to discover routes automatically and therefore require a minimal amount of setup and configuration. More sophisticated than static routers, they examine information from other routers and make packet-by-packet decisions about how to send data across the network.

Gateways

Gateways enable communication between different architectures and environments. They repackage and convert data going from one environment to another so that each environment can understand the other environment's data. A gateway repackages information to match the requirements of the destination system.

Gateways can change the format of a message so that it conforms to the application program at the receiving end of the transfer. For example, electronic-mail gateways, such as the X.400 gateway, receive messages in one format, translate it, and forward it in X.400 format used by the receiver, and vice versa.

A gateway links two systems that do not use the same:

- Communication protocols.
- Data-formatting structures.
- Languages.
- Architecture.

Gateways interconnect heterogeneous networks; for example, they can connect Microsoft Windows NT Server to IBM's Systems Network Architecture (SNA). Gateways change the format of the data to make it conform to the application program at the receiving end.

Network addressing

Addressing on a network can take one of three forms:

- **Computer names:** on a typical network, most users prefer to use computer names to communicate; computer names are far easier to remember than IP addresses. A computer name is the logical equivalent of an IP or MAC address
- **IP(Internet protocol):** Although users can use IP addresses, customarily IP addresses are used primirly by applications to communicate with locations on or outside the network
- **MAC(Media Access Control) address:**MAC addresses are the physical addresses of network devices and if users use computer names and application use IP addresses, then computers and other networked devices use MAC addresses to access other devices on the network

With three ways to address elements on a network, there must be ways to resolve each type of address to its equivalents.

MAC addressing

A host's MAC address is based on a 12-digit hexadecimal address. Usually, but not always, the MAC address is burned in the NIC through the use of a programmable Read only memory (PROM) module, or the address can be burned into a special chip called an electronic PROM (EPROM). The MAC address is identified in the second layer of the seven layer OSI model, the Data link layer Although the MAC address is always used in networking. It cannot be routed. The MAC address is not routable because of

- It does not pass through routers (because of its position in the OSI model)
- It has no network address.

Working on peer-to-peer Network (Workgroup)

IP Addressing

An IP address consists of two parts a **network address** that identifies the network and a **host address** that identifies the particular host, or node.

Types of IP address

1. Internet protocol version 4/IPV4
2. Internet protocol Version 6/IPV6

Every computer on a network must have a unique address. If two computers have the same address an address conflict occurs.

IPV4

The IP address identifies and differentiates a given machine from all others on the network. It consists of a 32-bit binary number that is usually displayed as four octets expressed in decimal and separated by periods.

You must have a unique IP address for each machine on the network. In addition, if your machine serves as a router to another network (it contains two or more network adapters and belongs to two or more networks), you must assign each adapter a unique IP address on the appropriate network.

8bit	8bit	8bit	8bit

Table 10. Show 32-bit binary number

Network classes

Internet addresses are allocated by the InterNIC (http://www.internic.net), the organization that administers the Internet. These IP addresses are divided into classes. The most common of these are classes A, B, and C.

Classes D and E exist, but are not generally used by end users. Each of the address classes has a different default subnet mask.

Network classes used to provide an addressing scheme that can accommodate large and small networks. All networks in practical use have different sizes. For example, a company that will have 50 computers, will not need a network of 5000 computers, And on the contrary, a company that needs 5000 computers does not need a network that can only hold 50 computers.

This is the main reason that engineers decided that IP address space should be divided in different classes in order to meet different requirements.

There are five different classes of networks: A, B, C, D and E. classes D and E are reserved. Class D is reserved for multicasting purpose and class E for experimental purpose.

Class A networks

- designed to meet the needs of large networks
- This class will only support 126 networks; but each network can support 16,777,214 hosts.
- The first octet of the IP address is network portion and the rest the node portion

Class B networks

- was designed for medium-sized networks
- This class will support 16,384 networks; and limited to 65,534 hosts per network.
- The first two octet are the nw portion
- Octet 3 and 4 are for nodes
- Used for nw that have b/n 256 and 65,534 nodes

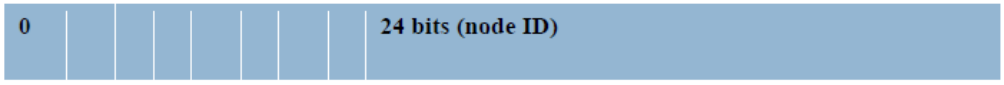
Class C networks

- Was designed for small networks; thus the number of hosts per network will be small, however it will support many more networks total.
- The first three octet are the network portion and the remaining one for node
- A maximum of 2,097,152 (221) networks can be defined with up to 254 (28-2) hosts per network

Class A

- The first bit is 0

Network ID

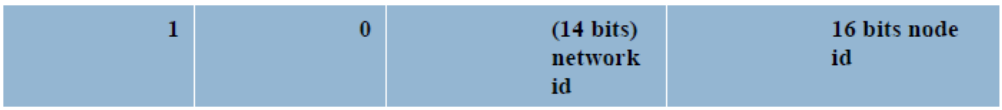


The possible class A IP ranges

1.0.0.0-127.255.255.255

Class B

- The first two bits are 1 and 0

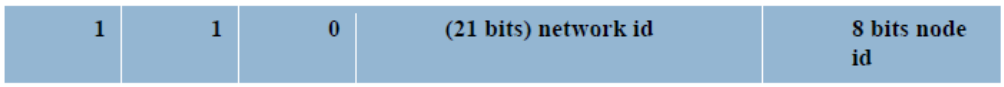


The possible IP range for class B is

128.0.0.0-191.255.255.255

Class C

- The first three bits are 1,1 and 0



The possible IP range for class C is

192.0.0.0- 223.255.255.255

Table 10. IP address class summary

Class	Prefix bits(ntk)	Max. num. of network	Suffix bits(host)	Available Hosts per Network	Valid Address Ranges
A	7	27=128	24	224-2=16777214	1.0.0.1 through 126.255.255.254
B	14	214=16384	16	216-2 =65534	128.0.0.1 through 191.255.255.254
C	21	221=2097152	8	28-2=254	192.0.0.1 through 222.255.255.254
D & E Reserved					224.0.0.0 through 255.255.255.254

If you are connecting your machine to a pre-existing network, the network address (for Class A, the first octet; for Class B, the first two octets; and for Class C, the first three octets) is the same as those of other machines on the network. In this case, you only need to create a unique host address.

If you are creating an entirely new network and you want to connect to the Internet, you need to contact the internet service provider or Network Information Center to have a network address. When you determine the

IP address, **remember:**

- Each logical network must have its own network address.
- All hosts in a network must have the same network address.
- All hosts in a network must have unique host addresses.

IP address type

1. **Private IP addresses**

   Private IP addresses are typically used on local networks including home, school and business LANs. Private networks are non-routable. Devices with private IP addresses cannot connect directly to the Internet.

   Likewise, computers outside the local network cannot connect directly to a device with a private IP. Instead, access to such devices must be brokered by a router.

   Class A 10.0.0.1 through 10.255.255.254

   Class B 172.16.0.1 through 172. 31.255.254

   Class C 192.168.0.1 through 192.168.255.254

2. **Public IP address**

   An IP address can be public - for use on the Internet or other wide area network (WAN).

Static verses Dynamic IP address

IP addresses can be determined statically (assigned to a computer by a system administrator) or dynamically (assigned by another device on the network on demand).

Reserved IP address

Certain host addresses are reserved and can't be assigned to devices on a network

These are

1. Network address used to identify the network itself with all host bits zero.
   Example: 192.168.1.0
2. broadcast address used for broadcasting packets to all devices on the network with all host bits one
   Example: 192.168.1.255

So usable host with in a network calculated by 2n-2 (two is subtracted because these are reserved for the network and broadcast. where n is the number of bits used for the host portion of the address.

Class D and class E are also reserved addresses used for different purposes such as research.

Subnet mask (network mask)

A subnet mask or sub network mask is a 32 bit number which is used to identify which portion of the IP address identifies the network portion and which part indicates the host part or portion.

In subnet mask, all bits of the network ID portion are set to 1 and all bits of the host address portion are set to 0.Any address bits that have corresponding mask bits set to 1 represent the network ID, and any address bits that have corresponding mask bits set to 0 represent the node ID

For class full networks there are default mask

Class C -> 255.255.255.0

Class B-> 255.255.0.0

Class A-> 255.0.0.0

Subnneting

Subnetting is the process of breaking down an IP network into smaller sub-networks called “subnets.”

Each subnet is a non-physical description (or ID) for a physical sub-network (usually a switched network of host containing a single router in a multi-router network).

Sub netting a technique that allows a network administrator to divide one physical network into smaller logical network

There are many reasons in favor of sub netting, including the following benefits

- Reduced network traffic: we all appreciate less traffic of any kind. Networks are no different. Without trusty routers, packet traffic could grind the entire network down to a near standstill. With routers, most traffic will stay on the local network: only packets destined for other networks will pass through the router. Routers create broadcast domains. The more broadcast domains you create, the samller the broadcast domains and the less network traffic on each network segment.
- Organized network performance: this is a result of reduced network traffic
- Simplified management: it is easier to identify and isolate network problems in a group of smaller connected networks than with one gigantic network
- Facilitated spanning of large geographical distances: because WAN links are considerably slower and more expensive than LAN links, a single large network that spans long distances can create problems in every area previously listed, connecting multiple smaller networks makes the system more efficient.

Subnet Mask Notation

There are two forms of subnet notation, **standard notation** and **CIDR** (Classless Internet Domain Routing) notation. Both versions of notation use a base address (or network address) to define the network's starting point, such as 192.168.1.0. This means that the network begins at 192.168.1.0 and the first possible host IP address on this subnet would be 192.168.1.1.

In standard subnet masks notation, a four octet numeric value is used as with the base address, for example 255.255.255.0. The standard mask can be calculated by creating four binary values for each octet, assigning the binary digit of .1. to the network potion, and assigning the binary digit of .0. to the network potion. In the example above this value would be 11111111.11111111.11111111.00000000. In combination with the base address is a subnet definition. In this case the subnet in standard notation would be 192.168.1.0 / 255.255.255.0.

In CIDR notation, the number of 1.s in the mask's binary version is counted from the left and that number is appended to the end of the base address following a slash (/). In the example here, the subnet would be listed in CIDR notation as 192.168.1.0/24.

Subnneting steps

When you've chosen a possible subnet mask for your network and need to determine the number of subnets, valid hosts, and broadcast addresses of a subnet that the mask provides, all you need to do is answer five simple questions:

How many subnets does the chosen subnet mask produce?

How many valid hosts per subnet are available?

What are the valid subnets?

What's the broadcast address of each subnet?

What are the valid hosts in each subnet?

At this point it's important that you both understand and have memorized your powers of 2.

Answers to those five big questions:

1. How many subnets? 2^x = number of subnets. x is the number of masked bits, or the 1s. For example, in
   11000000, the number of ones gives us 22 subnets. In this example, there are 4 subnets.
2. How many hosts per subnet? $2^y – 2$ = number of hosts per subnet. y is the number of unmasked bits, or the 0s. For example, in 11000000, the number of zeros gives us $2^6 – 2$ hosts. In this example, there are 62 hosts per subnet. You need to subtract two for the subnet address and the broadcast address, which are not valid hosts.

3. *What are the valid subnets?* 256 – subnet mask = block size, or increment number. An example would be 256 – 192 = 64. The block size of a 192 mask is always 64. Start counting at zero in blocks of 64 until you reach the subnet mask value and these are your subnets. 0, 64, 128, 192. Easy, huh? Yes—that is, if you can count in the needed block size!
4. *What's the broadcast address for each subnet?* Now here's the really easy part… Since we counted our subnets in the last section as 0, 64, 128, and 192, the broadcast address is always the number right before the next subnet. For example, the 0 subnet has a broadcast address of 63 because the next subnet is 64. The 64 subnet has a broadcast address of 127 because the next subnet is 128, etc. And remember, the broadcast of the last subnet (the subnet with the same interesting octets as the mask) is always 255 for Class C.
5. *What are the valid hosts?* Valid hosts are the numbers between the subnets, omitting all the 0s and all 1s. For example, if 64 is the subnet number and 127 is the broadcast address, then 65–126 is the valid host range—it's *always* the numbers between the subnet address and the broadcast address.

I know this can truly seem confusing. But it really isn't as hard as it seems to be at first—just hang in there!

Why not try a few and see for yourself?

Practice Example #1C: 255.255.255.192 (/26)

Let's use the Class C subnet mask from the preceding example, 255.255.255.192, to see how much simpler this method is than writing out the binary numbers. We're going to subnet the network address 192.168.10.0 and subnet mask 255.255.255.192.

192.168.10.0 = Network address

255.255.255.192 = Subnet mask

Now, let's answer the big five:

3. *How many subnets?* Since 192 is 2 bits on (**11**000000), the answer would be 2^2.
4. *How many hosts per subnet?* We have 6 host bits off (11**000000**), so the equation would be 26 – 2 = 62 hosts.
5. *What are the valid subnets?* 256 – 192 = 64. Remember, we start at zero and count in our block size, so our subnets are 0, 64, 128, and 192.
6. *What's the broadcast address for each subnet?* The number right before the value of the next subnet is all host bits turned on and equals the broadcast address.

7. *What are the valid hosts?* These are the numbers between the subnet and broadcast address. The easiest way to find the hosts is to write out the subnet address and the broadcast address. This way, the valid hosts are obvious. The following table shows the 0, 64, 128, and 192 subnets, the valid host ranges of each, and the broadcast address of each subnet:

See? We really did come up with the same answers as when we did it the binary way, and this way is so much easier because you never have to do any binary-to-decimal conversions! About now, you might be thinking that it's not easier than the first method I showed you. And I'll admit, for the first subnet with only 2 subnet bits—you're right, it isn't that much easier. But remember, we're going after the gold: being able to subnet in your head. And to do that, you need one thing: practice!

Collision Domains vs. Broadcast Domains

These different types of domains mean different things and when designing a LAN both of these domains can harm the performance of your network. If you are not aware of the difference between these two, this tutorial should help you out.

If you have a small network at your home there is usually the router/modem that is connected via phone line or cable to the ISP that router/modem is then connected to a switch or they even have a switch built into the device. You connect a few cables turn on some devices and you now have an internet connection ready to go. In larger networks you have more choices that need to be taken like when to use a hub, a switch, or a router?

How much money do you want to spend usually the more money spent you get more ports, performance increases and more features are added. These are all types of components that need to be thought of when designing a LAN.

This tutorial is going to be focusing on two major things collision domains and broadcast domains. The definition of a collision domain is a set of LAN devices whose frames could collide with one another. This happens with hubs, bridges, repeaters and wireless access points as only one device can send and receive at a time. If more than one device tries sending or receiving, the information is lost and irrecoverable it will need to be resent. This can slow down network performance along with making it a security threat.

A hub is considered a layer one device of the OSI model; all it does is send packets out on all ports including the port in which the packet was received on. This causes a collision domain because only one device can transmit at time.

This also shares the bandwidth of all devices connected to that collision domain. These devices can inefficiently use that bandwidth because of the CSMA/CD and jamming signals that occur when a collision happens.

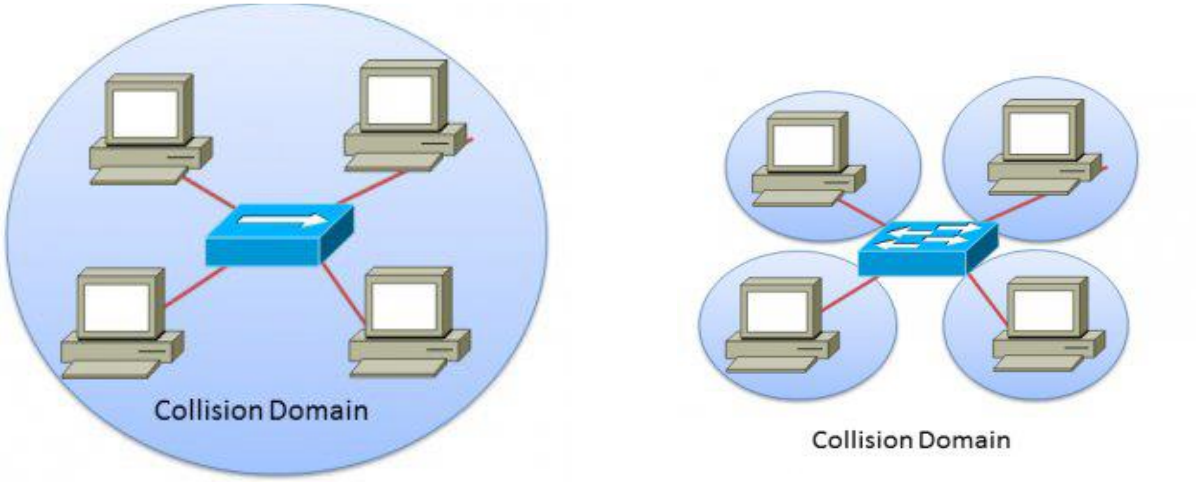


Figure 13.collision domain

A switch uses layer two of the OSI model, so the switch uses MAC addresses to send the packet to the correct device. Rather than sending it to all ports a switch only sends the packet out one port, if it has the MAC address in its MAC address table. If not the switch will send the packet on all ports except for the port in which the packet was received on. Switches provide separate collision domains on each port.

This provides dedicated bandwidth to that device. This also allows simultaneous conversations between devices on different ports. Each port can be operated at full-duplex so the device can send and receive information at

A broadcast domain is like a collision domain, the definition of a broadcast domain is a set of devices that if one device sends a broadcast frame all other devices will receive that frame in the same broadcast domain. So if devices are in the same IP network they will be able to receive a broadcast message. Having a smaller broadcast domain can improve network performance and improve against security attacks.

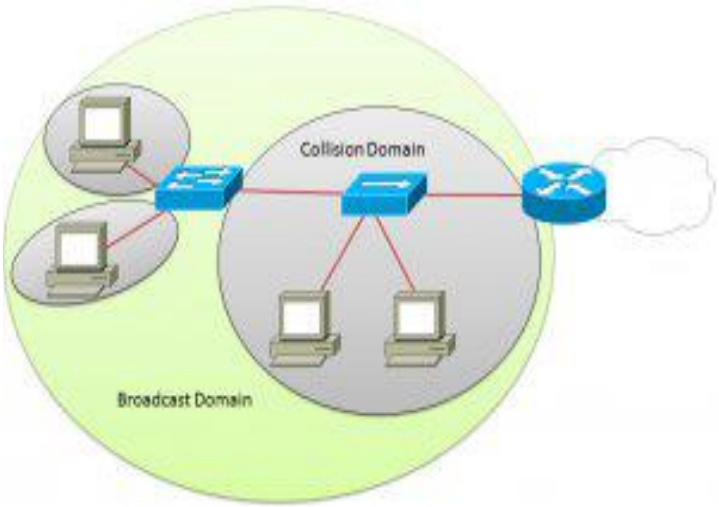


Figure 14. **Broadcast domain**

The more PCs and network devices connected to a single broadcast domain, the more broadcast messages you will have. Remember a broadcast message goes to every PC and network device. An example is when the router gets a packet that is destined to a host (192.168.1.124) on its Ethernet interface (192.168.1.0/24 network) the router will send an ARP request saying who is 192.168.1.124? That packet will go to every PC on the network, each PC has to look at the packet and then discard it if it is not 192.168.1.124. But only be processed by the PC that is 192.168.1.124. So a broadcast message can be just like a collision domain and affect network performance. The only devices that can block or not send broadcast messages are routers because they separate networks. Each interface on a router is a different network.

Introduction to IPV6

The current version of IP (known as Version 4 or IPv4) has not been substantially changed since RFC 791 was published in 1981. IPv4 has proven to be robust, easily implemented and interoperable, and has stood the test of scaling an internetwork to a global utility the size of today's Internet. This is a tribute to its initial design.

However, the initial design did not anticipate the following:

- The recent exponential growth of the Internet and the impending exhaustion of the IPv4 address space.

IPv4 addresses have become relatively scarce, forcing some organizations to use a Network Address Translator (NAT) to map multiple private addresses to a single public IP address.

While NATs promote reuse of the private address space, they do not support standards-based network layer security or the correct mapping of all higher layer protocols and can create problems when connecting two organizations that use the private address space.

Additionally, the rising prominence of Internet-connected devices and appliances ensures that the public IPv4 address space will eventually be depleted.

- The growth of the Internet and the ability of Internet backbone routers to maintain large routing tables.

  - Cables: are used to physically connect the computers on the network

  Normal /Straight through Cable: Connect Computer to Hub/switch [Different device].

  Cross-over Cable: Connect Hub to Hub or computer to computer [The same device].

Table 11. Cable arrangement summary

Cross over Cable		*Normal /Straight through Cable*	
End1	**End2**	**End1**	**End2**
White-Orange	White-Green	White-Orange	White-Orange
Orange	Green	Orange	Orange
White-Green	White-Orange	White-Green	White-Green
Blue	Blue	Blue	Blue
White-Blue	White-Blue	White-Blue	White-Blue
Green	Orange	Green	Green
White-Brown	White-Brown	White-Brown	White-Brown
Brown	Brown	Brown	Brown

Network connectivity device: Hub and Modem

Depending on the size of your network, you may also need a network hub to provide interconnection between PCs on the peer to peer network. Two PCs can connect using crossover cable but if you have three or more computers in your network you need buy a hub or multi-speed hub (called

Self-Check 1	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives. (1 point each)

1. In _____topology signals travel around the loop in one direction and pass through each computer, which can act as a repeater to boost the signal and send it on to the next computer.

A. Mesh B. Star C. Ring D. Bus E. B and C are correct

2. If there are 13 computers in Mesh topology, what is the total number of cables used in this topology design?

A. 123 B. 45 C. 92 D.78

3. The term terminator is used in _____topology.

A. Bus B. Ring C. Mesh D. Star

Part II: fill in the blank spaces.

1. _____refers to the arrangement or physical layout of computers, cables, and other components on the network.(**network topology**)(1%).

2. Write down the advantages of Bus topology. (4%).

_____

_____

_____

_____

_____

3. Write down the disadvantages of Ring topology. (3%).

Note: **Satisfactory rating 100%**

You can ask your teacher for the copy of the correct answers.

Score = _____

Information sheet 3.2. Analyzing features of the physical environment on network design

3.2. Analyzing features of the physical environment on network design

A traditional network planning methodology in the context of business decisions involves five layers of planning, namely:

- need assessment and resource assessment
- short-term network planning
- IT resource
- long-term and medium-term network planning
- Operations and maintenance**.**

Each of these layers incorporates plans for different time horizons, i.e. the business planning layer determines the planning that the operator must perform to ensure that the network will perform as required for its intended life-span. The Operations and Maintenance layer, however, examines how the network will run on a day-to-day basis.

The network planning process begins with the acquisition of external information. This includes:

- forecasts of how the new network/service will operate;
- The economic information concerning costs, and
- The technical details of the network's capabilities.

Planning a new network/service involves implementing the new system across the first four layers of the OSI Reference Model.

Network design

A company that manufactures custom-made bicycles has asked you to install an economical computer network that will bring it up-to-date in communication technology and be flexible enough to allow for future expansion.

The company's network goals are to:

- Network the existing computers so that they can share information and printers.
- Add two additional computers to the network: one for the Product Design Group and one for the Manufacturing Department.
- Allow for the possible addition of three computers at a later date.
- Provide an Internet connection for the Product Design Group.

The first decision we need to make for this new network is whether it should be a peer-to-peer or a server based network. The factors we need to examine include the:

- Size of the network.
- Level of security.
- Type of business.
- Level of administrative support available.
- Amount of network traffic.
- Needs of the network users.
- Network budget.

In a peer-to-peer network, all users on the network are equal. Each will have equal access to all other computers on the network, provided the owner of the computer has shared that resource with the network. In a small network or business, this "one for all and all for one" system often works well.

Often, in a small business, no individual is able to devote full-time attention to administering the network.

This brings another advantage of peer-to-peer networks to light. Here, responsibility for running the network is distributed to everyone, and users determine which information or resources on their computers will be shared.

Another down side of the peer-to-peer network is its limited performance. If another user is accessing the resources on your computer, that user will also be using processor time on your computer.

Therefore, regardless of how fast your computer's processor is or how much memory you have, the performance of your computer will slow down when someone else is drawing on its resources.

On a server-based network, resources are usually centralized. For example, one server manages all the printers, and another server manages all the files. Because servers are rarely turned off, resources will always be available. Server-based networks are also *scalable*. This means that their size can be easily adjusted to respond to changes in the load on the network.

Server-based networks are also more secure than peer-to-peer networks. With a peer-to-peer network, all resources are shared equally across the network. If the Accounting Department shares the directory that contains the salary files so that the Managing Director can access them, everyone else on the network can also access these files. On the other hand, server-based networks allow for the creation of accounts and permissions that provide for further security. For example, a server-based network can share individual files within a directory without making the directory itself available to everyone on the network.

As it grows, a server-based network can be segregated according to organizational needs. For example, one server might be designated for the Accounting Department and another server designated for the Sales Department. Should our bicycle company's network requirements reach this level, we will need to consider using a network that supports file-level sharing and user groups with shared rights to network resources.

At present, the better choice for our company is to use a peer-to-peer network. But in order to provide more flexibility and to prepare it for further expansion, another option exists: create a hybrid network. Thus, while our basic network will be peer-to-peer, we will install one computer as a file server. With this approach, access to the file server requires an account and permissions, while access to other computers on the network is shared equally.

So, after weighing these factors, we arrive at our network-design selection for this bicycle company: a hybrid peer-to-peer network, with one new computer to be installed and configured as a file server and used to centralize company information.

Taking Inventory

After deciding on the overall network design, our next step in creating a network is to take inventory to determine what hardware and software is already available and what needs to be acquired. As an illustration, we turn again to our bicycle company. It has a mixture of computers, ranging from a legacy 286 to a new Pentium III, as well as some older printers. Thus, some obvious updating will be required to get this network up and running. Taking inventory is an important step, because it sets the stage for future network expansion.

For example, if all your computers run Microsoft Windows 95 or Windows 98, you will be limited to using a peer-to-peer network. To upgrade to a server-based network in the future, you will have to upgrade one of the computers to run NetWare or Windows NT or add a new server with one of those network operating systems installed.

To take inventory, you'll need to survey four categories:

- Hardware
- Software
- Telecommunications equipment
- Network requirements

Hardware Survey

This is actually a simple process, but one that should not be taken lightly. Begin by recording the specifications of each computer; the details you gather at this stage can save time in the long run. As we will see later, in order to function effectively, networks often require that hardware and software meet certain minimum standards. If you know the specification details of the available equipment in advance, you can prevent many problems later on.

For each computer, you will need to gather information, including:

- Make and model.
- Processor manufacturer and speed.
- Amount of memory (RAM) installed.
- The size and manufacturer of each hard drive.
- Details of any other installed drives, such as compact-disc and removable disk drives.
- Monitor—make, model, and size.
- Video card—make, model, and amount of memory.

- Any installed peripherals.

- Type of bus—EISA, Micro Channel, ISA, or PCI—the computer uses and whether there are any free slots; you will need free slots to install network interface cards. (For more information on bus architecture, refer to make a list of the manufacturer and model number for any peripheral devices, such as printers, plotters, and scanners, whether they are installed or simply sitting on a shelf. For each of these, note whether you have the original disk with drivers.

Software Survey

Be aware of all the software currently in use throughout the potential network. For example, if you were to convert all the computers to Windows NT while you were installing the new network, you might find that some of the old standby programs, once used on a daily basis, now no longer run. Be especially careful when evaluating custom-designed and proprietary programs, such as accounting databases, which have been written especially for the company. You might need to contact the manufacturer for information about running proprietary programs on the network. Not all of these will run in a network environment; the product licensing arrangement might not allow network operations.

For each software program, gather the following information:

- Program name
- Program version number
- Availability of the original installation floppy disks or compact discs
- Any licensing information

As you carry out your survey of our bicycle company, also note any potential software incompatibilities within and among company departments. For example, the Accounting Department might be using WordPerfect, whereas the Sales Department is using Microsoft Office. If you are planning to upgrade some day, now is the time to make any changes needed to ensure that the same system is used company wide.

Telecommunications Equipment Survey

It might seem strange to review the existing telecommunications equipment when you are installing a LAN, but this is actually a very important element of your survey, especially if you intend to use Internet connections or some form of remote access server. Overlooking something as simple as the number of phone lines wired into each office can have a major impact later if you need modem and telephone connections at the same time.

For example, if the company has an automated telephone system, while telephone outlets might be located in every office, they might not be capable of a modem connection.

In that case, a separate telephone outlet might be required for voice and data communication. Also, if the company is using a high-speed digital telephone service, you might not be able to connect with standard modems.

Don't assume a standard RJ-11 telephone jack is going to be sufficient for you to connect a modem and start surfing the Web.

Requirements of the Network

After you have examined the existing facility and equipment, you need to define the requirements of your network. You'll then match these requirements to the existing hardware, software, and telecommunications features available and determine what steps need to be taken to develop the network. At a minimum, you should consider the following:

- The size of the facility (located on a single floor vs. multiple floors)
- The number of users
- Whether the LAN will be extended to several buildings
- The environment (office, manufacturing, out-of-doors)
- The current network media, if any
- The technical competence of users
- The amount of network traffic (initially, and anticipated for the future)
- The level of security

Building a Map

Now it's time to lay out the network. But before you begin to recommend a network plan for our bicycle company, you will first need to make a map of all the elements involved. During this step, you should consider two aspects of the network: the physical layout, including the location of each piece of hardware and how it relates to the others, and the physical and logical topology of the proposed network. The second step is to create a layout of the network topology. Don't forget to include printers and other peripherals, such as scanners and modems.

Choosing Network Media

The choice of which media to select should not be taken lightly. The cost of installation can be quite high, especially if you have to do it twice. The media you choose will usually be related to the geographic requirements of the site.

For example, if several of the workstations are located in a manufacturing environment in which a large amount of electrical noise is generated, fiber-optic cable might be required because it is unaffected by electrical signals.

On the other hand, in a small office, simple twisted-pair cable will usually be appropriate. The most important thing to keep in mind is not the cost today, but the cost in the future. Being overly cost-conscious now can limit the scalability, and thus the life span, of the network.

At our bicycle company, we might decide to install our network using CAT 3 UTP cable. This would give us a functional network with our seven workstations, but limit our network speed to 10 Mbps. Five years from now, when we might have as many as 30 to 50 workstations, a 10 Mbps network would be slow. However, by installing CAT 5 UTP now, we can upgrade our network to 100 Mbps at any time in the future without needing to rewire the building. And CAT 5 UTP cable costs only a few cents more per foot than CAT 3 UTP cable.

Factors That Affect a Network Design

Designing a network is more than merely planning to use the latest device in the market. A good network design takes into consideration many factors:

Size Matters

Designing a LAN for a small office with a few users is different from building one for a large company with two thousand users. In building a small LAN, a flat design is usually used, where all connecting devices may be connected to each other. For a large company, a hierarchical approach should be used.

Geographies

The geographical locations of the sites that need to be connected are important in a network design. The decision making process for selecting the right technology and equipment for remote

connections, especially those of cross-country nature, is different from that for a LAN. The tariffs, local expertise, quality of service from service providers, are some of the important criteria.

Politics

Politics in the office ultimately decides how a network should be partitioned. Department A may not want to share data with department B, while department C allows only department D to access its data.

At the network level, requirements such as these are usually done through filtering at the router so as to direct traffic flow in the correct manner. Business and security needs determine how information flows in a network and the right tool has to be chosen to carry this out.

Types of Application

The type of application deployed determines the bandwidth required. While a text-based transaction may require a few kbps of bandwidth, a multimedia help file with video explanations may require 1.5 Mbps of bandwidth. The performance requirement mainly depends on application need and the challenge of a good network is to be able to satisfy different application needs.

Strategy

One important factor is of course a networking strategy. Without a networking blueprint, one may end up with a multivendor, multiprotocol network that is both difficult to manage and expand. It has been estimated that 70% of the cost of owning a network is in maintaining it. Having a network strategy ensures that technology is deployed at the correct place and products chosen carefully. A network that is built upon a strategy ensures manageability and scalability.

Cost Constraints

The one major decision that makes or breaks a design is cost. Many a times, network managers have to forego a technically elegant solution for a less sophisticated design.

Standards

Choosing equipment that conforms to standards is an important rule to follow. A standard means having the ability to deploy an industry-recognized technology that is supported by the majority of vendors. This provides flexibility in choice of equipment, and allows network managers to choose the most cost effective solution. As more business and transactions are conducted through the network, the network infrastructure has become more important than ever. Network managers need to choose the right technologies, from the backbone to the desktops, and tie everything together to support the needs of their businesses. By now, it is obvious that designing a network is not just about raw speed. Adopting a balanced approach, weighing features against cost, and choosing the right technology that is based on open standards to meet the business requirement is a right way to begin.

The network planning process involves three main steps:

- **Topological design**: This stage involves determining where to place the components and how to connect them. The (topological) optimization methods that can be used in this stage come from an area of mathematics called Graph Theory. These methods involve determining the costs of transmission and the cost of switching, and thereby determining the optimum connection matrix and location of switches and concentrators

- **Network-synthesis**: This stage involves determining the size of the components used, subject to performance criteria such as the Grade of Service (GOS). The method used is known as "Nonlinear Optimization", and involves determining the topology, required GoS, cost of transmission, etc., and using this information to calculate a routing plan, and the size of the components.
- **Network realization**: This stage involves determining how to meet capacity requirements, and ensure reliability within the network. The method used is known as "Multicommodity Flow Optimization", and involves determining all information relating to demand, costs, and reliability, and then using this information to calculate an actual physical circuit plan.

The open system Interconnection (OSI) reference model

The OSI reference model represents the seven layers of the process by which data is packaged and transmitted from a sending application through the physical wires to the receiving application.

Network Communications

Network activity involves sending data from one computer to another. This complex process can be broken into discrete, sequential tasks. The sending computer must:

1. Recognize the data.
2. Divide the data into manageable chunks.
3. Add information to each chunk of data to determine the location of the data and to identify the receiver.
4. Add timing and error-checking information.
5. Put the data on the network and send it on its way.

With the rapid growth of networking hardware and software, a need arose for standard protocols that could allow hardware and software from different vendors to communicate. In response, two primary sets of standards were developed: the OSI reference model and a modification of that standard called Project 802 Acquiring a clear understanding of these models is an important first step in understanding the technical aspects of how a network functions. Throughout this lesson we refer to various protocols

In 1978, the International Organization for Standardization (ISO) released a set of specifications that described network architecture for connecting dissimilar devices. The original document applied to systems that were open to each other because they could all use the same protocols and standards to exchange information.

A Layered Architecture

The OSI reference model architecture divides network communication into seven layers. Each layer covers different network activities, equipment, or protocols. The OSI reference model defines how each layer communicates and works with the layers immediately above and below it. For example, the session layer communicates and works with the presentation and transport layers.

The seven layers of the OSI reference model from highest to lowest layers are:

7. Application layer
6. Presentation layer
5. Session layer

4. Transport layer
3. Network layer
2. Data link layer
1. Physical layer

Each layer provides some service or action that prepares the data for delivery over the network to another computer. The lowest layers—1 and 2—define the network's physical media and related tasks, such as putting data bits onto the network interface cards (NICs) and cable. The highest layers define how applications access communication services. The higher the layer, the more complex its task is.

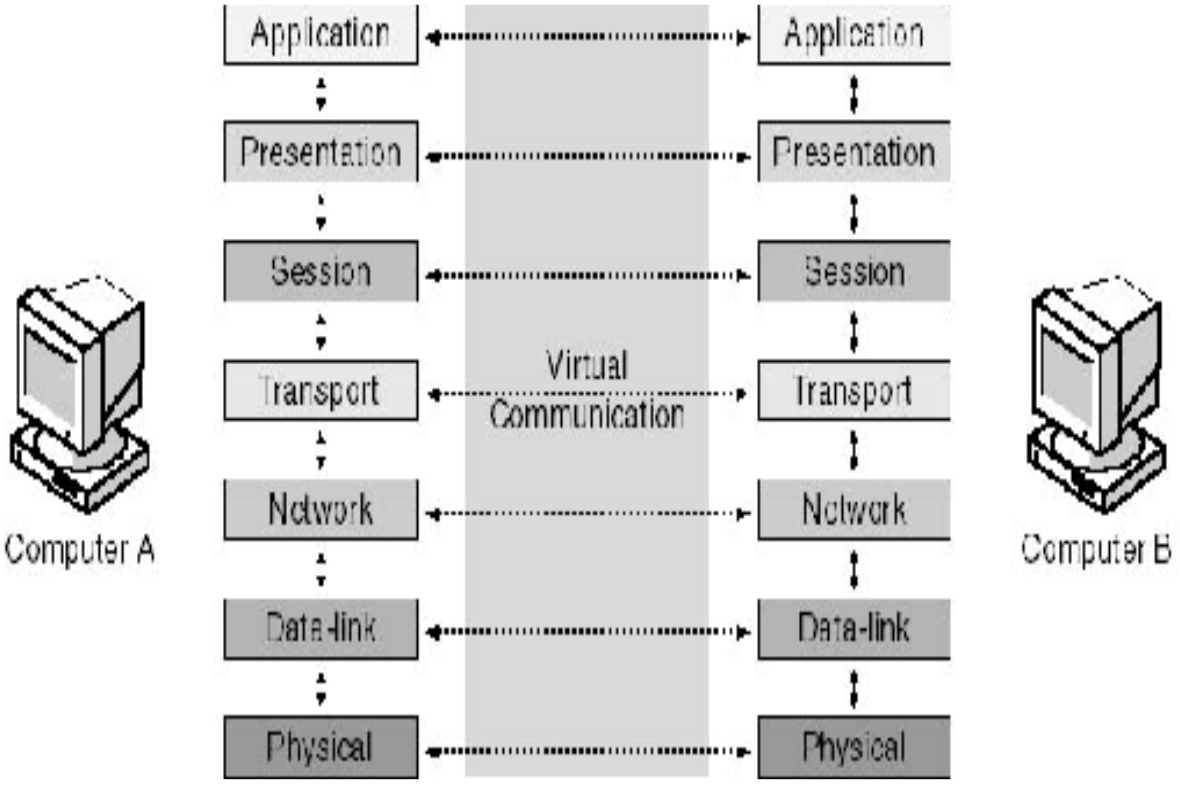


Figure 15. Relationships among OSI Reference Model Layers

Before data is passed from one layer to another, it is broken down into packets, or units of information, which are transmitted as a whole from one device to another on a network. The network passes a packet from one software layer to another in the same order as that of the layers. At each layer, the software adds additional formatting or addressing to the packet, which is needed for the packet to be successfully transmitted across the network.

With the exception of the lowest layer in the OSI networking model, no layer can pass information directly to its counterpart on another computer. Instead, information on the sending computer must be passed down through each successive layer until it reaches the physical layer. The information then moves across the networking cable to the receiving computer and up that computer's networking layers until it arrives at the corresponding layer. For example, when the network layer sends information from computer A, the information moves down through the data-link and physical layers on the sending side, over the cable, and up the physical and data-link layers on the receiving side to its final destination at the network layer on computer B.

Application Layer

- Layer 7, the topmost layer of the OSI reference model, is the *application layer*.
- This layer relates to the services that directly support user applications, such as software for file transfers, database access, and e-mail.
- A message to be sent across the network enters the OSI reference model at this point and exits the OSI reference model's application layer on the receiving computer.
- Application-layer protocols can be programs in themselves, such as File Transfer Protocol (FTP), or they can be used by other programs, such as Simple Mail Transfer Protocol (SMTP), used by most e-mail programs, to redirect data to the network.

Presentation Layer

- Layer 6, the *presentation layer*, defines the format used to exchange data among networked computers.
- When computers from dissimilar systems—such as IBM, Apple, and Sun—need to communicate, a certain amount of translation and byte reordering must be done.
- Within the sending computer, the presentation layer translates data from the format sent down from the application layer into a commonly recognized, intermediary format.
- At the receiving computer, this layer translates the intermediary format into a format that can be useful to that computer's application layer.
- Responsible for converting protocols, translating data, encryption and decryption , compression and decompression

Session Layer

- Layer 5, the *session layer*, allows two applications on different computers to open, use, and close a connection called a *session*.
- A session is a highly structured dialog between two workstations. The session layer is responsible for managing this dialog. It performs name-recognition and other functions, such as security, that are needed to allow two applications to communicate over the network.
- It synchronizes user tasks
- It implement dialog control between communicating process, such as regulating which side transmits, when and for how long

Transport Layer

- Layer 4, the *transport layer*, provides an additional connection level beneath the session layer.
- The transport layer ensures that packets are delivered error free, in sequence, and without losses or duplications.
- At the sending computer, this layer repackages messages, dividing long messages into several packets and collecting small packets together in one package.
- At the receiving computer, the transport layer opens the packets, reassembles the original messages, and, typically, sends an acknowledgment that the message was received.
- If a duplicate packet arrives, this layer will recognize the duplicate and discard it.
- The transport layer provides flow control and error handling, and participates in solving problems concerned with the transmission and reception of packets.
- Transmission Control Protocol (TCP) and Sequenced Packet Exchange (SPX) are examples of transport-layer protocols.

Network Layer

- Layer 3, the *network layer*, is responsible for addressing messages and translating logical addresses and names into physical addresses.
- This layer also determines the route from the source to the destination computer. It determines which path the data should take based on network conditions, priority of service, and other factors.

- If the network adapter on the router cannot transmit a data chunk as large as the source computer sends, the network layer on the router compensates by breaking the data into smaller units.
- Internet Protocol (IP) and Internetwork Packet Exchange (IPX) are examples of network-layer protocols.

Data-Link Layer

- Layer 2, the *data-link layer*, sends data frames from the network layer to the physical layer. It controls the electrical impulses that enter and leave the network cable.
- On the receiving end, the data-link layer packages raw bits from the physical layer into data frames. (A data frame is an organized, logical structure in which data can be placed. The electrical representation of the data (bit patterns, encoding methods, and tokens) is known to this layer only.
- The data-link layer is responsible for providing error-free transfer of these frames from one computer to another through the physical layer.

The bellow Figure shows a simple data frame. In this example, the sender ID represents the address of the computer that is sending the information; the destination ID represents the address of the computer to which the information is being sent. The control information is used for frame type, routing, and segmentation information. The data is the information itself. The cyclical redundancy check (CRC) provides error correction and verification information to ensure that the data frame is received correctly.

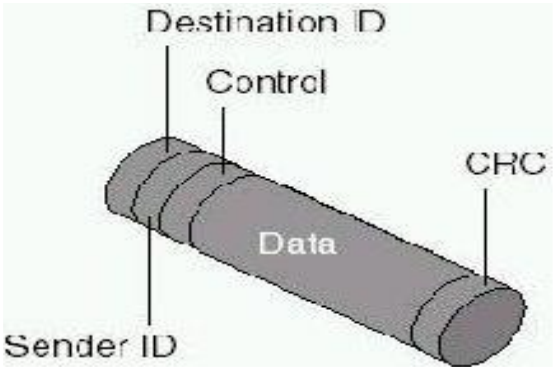


Figure 16. Relation between sender and receiver in data link layer

Physical Layer

- Layer 1, the bottom layer of the OSI reference model, is the *physical layer.*
- This layer transmits the unstructured, raw bit stream over a physical medium (such as the network cable).
- The physical layer is totally hardware-oriented and deals with all aspects of establishing and maintaining a physical link between communicating computers. The physical layer also carries the signals that transmit data generated by each of the higher layers.
- This layer defines how the cable is attached to the NIC. For example, it defines how many pins the connector has and the function of each. It also defines which transmission technique will be used to send data over the network cable.
- The physical layer is responsible for transmitting bits (zeros and ones) from one computer to another, ensuring that when a transmitting host sends a 1 bit, it is received as a 1 bit, not a 0 bit
- It defines how each bit is translated into the appropriate electrical or optical impulse for the network cable.

This layer is often referred to as the "hardware layer." Although the rest of the layers can be implemented as firmware (chip-level functions on the NIC), rather than actual software, the other layers are software in relation to this first layer.

- **LLC—**The LLC sub layer, which is defined by the IEEE 802.2 standard, controls the access of the media, enabling multiple high-level protocols to use a single network link.
- **MAC—**The MAC sub layer manages and controls access to the network media for the protocols trying to use it. The MAC address is defined at this sub layer.

Data Packets and the OSI Reference Model

Data packets are assembled and disassembled according to the OSI reference model. The packet-creation process begins at the application layer of the OSI reference model, where the data is generated. Information to be sent across the network starts at the application layer and descends through all seven layers.

At each layer, information relevant to that layer is added to the data. This information is for the use of the corresponding layer in the receiving computer. The data-link layer in the receiving computer, for instance, will read information added at the data-link layer in the sending computer.

At the transport layer, the original block of data is broken into the actual packets. The protocol defines the structure of the packets used by the two computers.

When the packet reaches the transport layer, sequence information is added that guides the receiving computer in reassembling the data from packets.

When the packets finally pass through the physical layer on their way to the cable, they contain information from each of the other six layers.

The Function of Network Protocols

Protocols are rules and procedures for communicating. The term "protocol" is used in a variety of contexts.

For example, diplomats from one country adhere to rules of protocol designed to help them interact smoothly with diplomats from other countries. Rules of protocol apply in the same way in the computer environment.

TCP/IP protocol

Transmission Control Protocol/Internet Protocol (TCP/IP) is an industry-standard suite of protocols that provide communications in a heterogeneous (made up of dissimilar elements) environment. In addition,

TCP/IP provides a routable, enterprise networking protocol and access to the Internet and its resources.

Because of its popularity, TCP/IP has become the de facto standard for what's known as *internetworking*, the intercommunication in a network that's composed of smaller networks. This lesson examines the TCP/IP protocol and its relationship to the OSI reference model.

Introduction to TCP/IP

TCP/IP has become the standard protocol used for interoperability among many different types of computers. This interoperability is a primary advantage of TCP/IP. Most networks support TCP/IP as a protocol. TCP/IP also supports routing and is commonly used as an internetworking protocol.

Other protocols written specifically for the TCP/IP suite include:

- **SMTP (Simple Mail Transfer Protocol)** E-mail.
- **FTP (File Transfer Protocol)** For exchanging files among computers running TCP/IP.

- **SNMP (Simple Network Management Protocol)** For network management.

Designed to be routable, robust, and functionally efficient, TCP/IP was developed by the United States Department of Defense as a set of wide area network (WAN) protocols. Its purpose was to maintain communication links between sites in the event of nuclear war. The responsibility for TCP/IP development now resides with the Internet community as a whole. TCP/IP requires significant knowledge and experience on the user's part to install and configure.

TCP/IP and OSI

The TCP/IP protocol does not exactly match the OSI reference model. Instead of seven layers, it uses only four. Commonly referred to as the Internet Protocol Suite, TCP/IP is broken into the following four layers:

- Network interface layer
- Internet layer
- Transport layer
- Application layer

Each of these layers corresponds to one or more layers of the OSI reference model.

Network Interface Layer

The *network interface layer,* corresponding to the physical and data-link layers of the OSI reference model, communicates directly with the network. It provides the interface between the network architecture (such as token ring, Ethernet) and the Internet layer.

Internet Layer

The *Internet layer*, corresponding to the network layer of the OSI reference model, uses several protocols for routing and delivering packets. Routers "Elements of Network Connectivity," are protocol dependent. They function at this layer of the model and are used to forward packets from one network or segment to another.

Several protocols work within the Internet layer.

Internet Protocol (IP)

Internet Protocol (IP) is a packet-switched protocol that performs addressing and route selection. As a packet is transmitted, this protocol appends a header to the packet so that it can be routed through the network using dynamic routing tables. IP is a connectionless protocol and sends packets without expecting the receiving host to acknowledge receipt. In addition, IP is responsible for packet assembly and disassembly as required by the physical and data-link layers of the OSI reference model. Each IP packet is made up of a source and a destination address, protocol identifier, checksum (a calculated value), and a TTL (which stands for "time to live"). The TTL tells each router on the network between the source and the destination how long the packet has to remain on the network. It works like a countdown counter or clock. As the packet passes through the router, the router deducts the larger of one unit (one second) or the time that the packet was queued for delivery. For example, if a packet has a TTL of 128, it can stay on the network for 128 seconds or 128 hops (each stop, or router, along the way), or any combination of the two. The purpose of the TTL is to prevent lost or damaged data packets (such as missing e-mail messages) from endlessly wandering the network. When the TTL counts down to zero, the packet is eliminated from the network.

Another method used by the IP to increase the speed of transmission is known as "*ANDing.*" The purpose of ANDing is to determine whether the address is a local or a remote site. If the address is local, IP will ask the Address Resolution Protocol (ARP), discussed in the next section, for the hardware address of the destination machine. If the address is remote, the IP checks its local routing table for a route to the destination. If a route exists, the packet is sent on its way. If no route exists, the packet is sent to the local default gateway and then on its way.

Address Resolution Protocol (ARP)

Before an IP packet can be forwarded to another host, the hardware address of the receiving machine must be known. The *ARP* determines hardware address (MAC addresses) that correspond to an IP address. If ARP does not contain the address in its own cache, it broadcasts a request for the address. All hosts on the network process the request and, if they contain a map to that address, pass the address back to the requestor. The packet is then sent on its way, and the new information address is stored in the router's cache.

Reverse Address Resolution Protocol (RARP)

A RARP server maintains a database of machine numbers in the form of an ARP table (or cache) which is created by the system administrator. In contrast to ARP, the RARP protocol provides an IP number to a requesting hardware address. When the RARP server receives a request for an IP number from a node on the network, it responds by checking its routing table for the machine number of the requesting node and sending the appropriate IP number back to the requesting node.

Internet Control Message Protocol (ICMP)

The *ICMP* is used by IP and higher-level protocols to send and receive status reports about information being transmitted. Routers commonly use ICMP to control the flow, or speed, of data between themselves. If the flow of data is too fast for a router, it requests that other routers slow down. The two basic categories of ICMP messages are reporting errors and sending queries.

Transport Layer

The *transport layer*, corresponding to the transport layer of the OSI reference model, is responsible for establishing and maintaining end-to-end communication between two hosts. The transport layer provides acknowledgment of receipt, flow control, and sequencing of packets. It also handles retransmissions of packets. The transport layer can use either TCP or User Datagram Protocol (UDP) protocols depending on the requirements of the transmission.

Transmission Control Protocol (TCP)

The TCP is responsible for the reliable transmission of data from one node to another. It is a connection based protocol and establishes a connection (also known as a session, virtual circuit, or link), between two machines before any data is transferred. To establish a reliable connection, TCP uses what is known as a "three-way handshake." This establishes the port number and beginning sequence numbers from both sides of the transmission. The handshake contains three steps:

1. The requestor sends a packet specifying the port number it plans to use and its initial sequence number (ISN) to the server.
2. The server acknowledges with its ISN, which consists of the requestor's ISN, plus 1.
3. The requestor acknowledges the acknowledgement with the server's ISN, plus 1.

In order to maintain a reliable connection, each packet must contain:

- A source and destination TCP port number.
- A sequence number for messages that must be broken into smaller pieces.

- A checksum to ensure that information is sent without error.
- An acknowledgement number that tells the sending machine which pieces of the message have arrived.
- TCP Sliding Windows.

User Datagram Protocol (UDP)

A connectionless protocol, the *UDP*, is responsible for end-to-end transmission of data. Unlike TCP, however, UDP does not establish a connection. It attempts to send the data and to verify that the destination host actually receives the data. UDP is best used to send small amounts of data for which guaranteed delivery is not required. While UDP uses ports, they are different from TCP ports; therefore, they can use the same numbers without interference.

Application Layer

Corresponding to the session, presentation, and application layers of the OSI reference model, the *application layer* connects applications to the network. Two application programming interfaces (APIs) provide access to the TCP/IP transport protocols—Windows Sockets and NetBIOS.

Table 12. OSI Layer summary

OSI Layer	Major Functions
Application	• Provides access to the network for applications and certain end-user functions • Displays incoming information and prepares outgoing information for network access
Presentation	• Converts data from the application layer into a format that can be sent over the network • Converts data from the session layer into a format that can be understood by the application layer • Handles encryption and decryption of data; provides compression and decompression functionality
Session	• Synchronizes on separate devices • Handles error detection and notification to the peer layer on the other device
Transport	• Establishes, maintains, and breaks connections between two devices • Determines the ordering and priorities of data • Performs error checking and verification and handles retransmissions if necessary
Network	• Provides mechanisms for the routing of data between devices

	across single or multiple network segments • Handles the discovery of destination systems and addressing
Data link	• Has two distinct sub layers: LLC and MAC • Performs error detection and handling for the transmitted signals • Defines the method by which the media is accessed • Defines hardware addressing through the MAC sub layer
Physical	• Defines the physical structure of the network • Defines voltage/signal rates and the physical connection methods • Defines the physical topology

The Layers at Which Devices Operate

Network devices are said to operate at certain layers of the OSI model based on their functions and roles in the network.

Table 13. The Layers at Which Devices Operate

Device	**OSI Layer at Which the Device Operates**
Hub	Physical (Layer 1)
Switch	Data link (Layer 2)
Bridge	Data link (Layer 2)
Router	Network (Layer 3)
NIC	Data link (Layer 2)
AP	Data link (Layer 2)

TCP/IP Protocol Suite Summary

Each of these protocols maps to the OSI model. Knowing what the protocol does helps to identify where it fits within the OSI model.

Table.14 **TCP/IP Protocol Suite Summary**

Protocol	**Full Name**	**Description**	**OSI Layer**
IP	Internet Protocol	Connectionless protocol used for moving data around a network.	Network Layer (3)
TCP	Transmission Control Protocol	Connection-oriented protocol that offers flow control, sequencing, and retransmission of dropped packets.	Transport Layer (4)
UDP	User Datagram	Connectionless alternative to TCP	Transport Layer (4)

	Protocol	used for applications that do not require the functions offered by TCP.	
FTP	File Transfer Protocol	Protocol for uploading and downloading files to and from a remote host; also accommodates basic file management tasks.	Application Layer (7)
SFTP	Secure File Transfer Protocol	Protocol for securely uploading and downloading files to and from a remote host. Based on SSH security.	Application Layer (7)
TFTP	Trivial File Transfer Protocol	File transfer protocol that does not have the security or error checking of FTP. TFTP uses UDP as a transport protocol and is therefore connectionless.	Application Layer (7)
SMTP	Simple Mail Transfer Protocol	Mechanism for transporting email across networks.	Application Layer (7)
HTTP	Hypertext Transfer Protocol	Protocol for retrieving files from a web server.	Application Layer (7)
HTTPS	Hypertext Transfer Protocol Secure	Secure protocol for retrieving files from a web server.	Application Layer (7)
POPv3/ IMAPv4	Post Office Protocol version 3/ Internet Message Access Protocol version 4	Used for retrieving email from a server on which the email is stored. Can be used only to retrieve mail. IMAP and POP cannot be used to send mail.	Application Layer (7)
Telnet	Telnet	Enables sessions to be opened on a remote host.	Application Layer (7)
SSH	Secure Shell	Enables secure sessions to be opened on a remote host.	Application Layer (7)
ICMP	Internet Control	Used on IP-based networks for error	Network Layer (3)

	Message Protocol	reporting, flow control, and route testing.	
ARP	Address Resolution Protocol	Resolves IP addresses to MAC addresses to enable communication between devices.	Data Link Layer (2)
RARP	Reverse Address Resolution Protocol	Resolves MAC addresses to IP addresses.	Data Link Layer (2)
NTP	Network Time Protocol	Used to communicate time synchronization information between devices.	Application Layer (7)
NNTP	Network News Transport Protocol	Facilitates the access and downloading of messages from newsgroup servers.	Application Layer (7)
SCP	Secure Copy Protocol	Enables files to be copied securely between two systems. Uses Secure Shell (SSH) technology to provide encryption services.	Application Layer (7)
LDAP	Lightweight Directory Access Protocol	Protocol used to access and query directory services systems, such as Novell Directory Services and Microsoft Active Directory.	Application Layer (7)
IGMP	Internet Group Management Protocol	Provides a mechanism for systems within the same multicast group to register and communicate with each other.	Network Layer (3)
DNS	Domain Name System	Resolves hostnames to IP addresses.	Application Layer (7)
DHCP	Dynamic Host Configuration Protocol	Automatically assigns TCP/IP information.	Application Layer (7)
SNMP	Simple Network Management	Enables network devices to communicate information about their	Application Layer (7)

	Protocol	state to a central system. It also enables the central system to pass configuration parameters to the devices.	
TLS	Transport Layer Security	A security protocol designed to ensure privacy between communicating client/server applications.	Application Layer (7)
SIP	Session Initiation Protocol	An application-layer protocol designed to establish and maintain multimedia sessions such as Internet telephony calls.	Application Layer (7)
RTP	Real-time Transport Protocol	The Internet-standard protocol for the transport of real-time data.	Application Layer (7)

Self-Check 2	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives. (1 point each)

1. _____is responsible for establishing and maintaining end-to-end communication between two hosts.

A. Physical layer B. Presentation layer C. Session layer D. Transport layer

2. Internet explorer is found in _____ layer of the OSI

A. Physical layer B. Presentation layer C. Session layer D. Application layer

3. Makes to application to open, use and close a connection

A. Application layer B. Network layer C. Session layer D. Data link layer

4. Hub is operated in the _____of OSI reference model.

A. Presentation layer B. Physical C. Transport layer D. Network layer

5. The set of rule and procedures which govern communication between computers

A. OSI B. Topology C. Protocol D. IP

6. The protocol which enables computer to send and receive e mail

A. FTP B. SNMP C. SMTP D. HTTP

7. Which of the following is connection oriented protocol?

A. TCP B. UDP C. SMTP D. All

Part II: Fill in the blank spaces

1. Data link layer has two distinct sub layers called :(2%).

_____

_____

_____

3. The _____layer is the top most layer of the OSI reference model.

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Score = _____

Information sheet 3.3. Conducting costing process for possible topology

3.3. Conducting costing process for possible topology

The primary reason for conducting **cost analysis** is generally to determine the true (full) **costs** of each of the programs under **analysis** (services and/or products). You can then utilize this knowledge to: Identify and prioritize **cost**-saving opportunities.

A cost-benefit analysis is a process businesses use to analyze decisions. The business or analyst sums the benefits of a situation or action and then subtracts the costs associated with taking that action. Some consultants or analysts also build models to assign a dollar value on intangible items, such as the benefits and costs associated with living in a certain town.

The major steps in a cost-benefit analysis

- Step 1: Specify the set of options. ...
- Step 2: Decide whose costs and benefits count. ...
- Step 3: Identify the impacts and select measurement indicators. ...
- Step 4: Predict the impacts over the life of the proposed regulation. ...
- Step 5: Monetize (place dollar values on) impacts.

COST BENEFIT ANALYSIS “Cost is always a factor when considering any type of training” (Lee, Mamone, & Roadman, 1995, p. 14). Thus, an organization should perform the cost-benefit analysis of **a network-based training system** in an analytic manner. The objective is to compare the values of outcomes, costs, and revenues of the proposed system to help in the decision-making process. The intent of this analysis is to provide a framework to evaluate the impact of establishing the system in the organization. Unless an organization carries out a cost analysis, decision-makers cannot make reliable, well-planned, and carefully considered decisions.

As the results of various studies that network-based instruction can be as effective as traditional instruction. Consequently, the major assumption in the analysis is that both traditional and online training have identical benefits,

meaning that they have the same amount of output in terms of learning. Accordingly, the basis for analysis will only be the costs emerging in the development and delivery processes.

Estimated Costs: This section analyzes the potential costs of investing and establishing a network-based training system in the organization. According to Horton (2000), Web-based training is “so diverse that cost estimating is more a matter of wishful thinking than scientific method” (p. 43). The author hypothesizes that there are several (various) key elements that have costs in need of identification in a majority of Web-based training projects. The following are the estimated costs associated with a network-based training system.

Hardware Resources: One of the key elements that contribute to server/network hardware costs is the estimated number of the trainees that will access the course. Based on the estimated number of trainees and level of the interactivity designed into the course will determine the server capacity and performance requirements. The higher capacity means the more cost.

> **Server**: In the proposed system, the assumption is that the purchase of a server is necessary to offer an online course. The estimated total cost of a server is $5,000. This is a start-up cost as well as a time-independent cost, which means that the cost does not increase over time. •Computers: Since personnel have their own personal computers that have sufficient specifications for accessing the online training system, the assumption is that that the organization does not have new computer needs, and thus there is no associated cost.

Software Resources: Several vendors offer a variety of online distance-learning software products. The organization can acquire software either by obtaining a hosting service from an application service provider (ASP) by paying annual license fee or by purchasing the application by paying a one-time perpetual use license fee. Software costs may be both time-dependent and time-independent costs.

Network-Infrastructure: Since the organization has its own Intranet network, the author assumes that there is no network infrastructure cost.

Salaries and Wages: the organization needs at least one course developer at the outset. An issue taken into consideration is whether to hire a full-time or outsource the service to a contractor or a third party. For the phase where a prototype course is developed, it may be a right decision to outsource the job. For developing courses, the organization may want to hire a full-time employee. Salaries and wages are time-dependent costs.

Miscellaneous Costs: the organization should have a budget to maintain and update the system during its lifecycle. Another cost that should also be factored into the analysis is the cost of training users and instructors. Maintenance costs are assumed 10% of initial equipment and courseware costs per year.

Regulations require the government to pay expense allowances for government employees while they are on official business travel. Travel expenses include the cost of travel, meals, and employee accommodations. Accordingly, when assigned to training in a place other than their place of work employees obtain reimbursement for their expenses. According to Becker (as cited in Horton, 2000, p. 20), as much as 40% of the cost of corporate training is for travel. In a traditional system, the high cost of transporting personnel from their place of work to training facilities is indispensable. On the other hand, an online system does not have travelling expenses.

Self-Check	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Fill in the blank spaces

1. **What is Cost benefit analysis in computer networking?**

_____

_____

2. **What are the major steps in a cost-benefit analysis?**

_____

_____

_____

_____

_____

_____

Note: **Satisfactory rating 100%**

You can ask you teacher for the copy of the correct answers.

Score = _____

Information sheet3.4. Selecting and documenting appropriate network topology

3.4. Selecting and documenting appropriate network topology

Consideration for cable selection

Which cabling you select will depend on the needs of a particular site:

The cabling you purchase to set up a LAN for a small business has different requirements from those of a larger organization, such as a major banking institution.

Installation Logistics

How easy is the cable to install and work with? In a small installation where distances are short and security isn't a major issue, it does not make sense to choose thick, cumbersome, and expensive cable.

Shielding

The level of shielding required will affect cable cost. Almost every network uses some form of shielded cable. The noisier the area in which the cable is run, the more shielding will be required. The same shielding in a plenum-grade cable will be more expensive as well.

Crosstalk

Crosstalk and noise can cause serious problems in large networks where data integrity is crucial. Inexpensive cabling has low resistance to outside electrical fields generated by power lines, motors, relays, and radio transmitters. This makes it susceptible to both noise and crosstalk.

Transmission Rates

Transmission rates are measured in megabits per second. A standard reference point for current LAN transmission over copper cable is 100 Mbps. Fiber-optic cable transmits at more than 1 Gbps.

Cost

Higher grades of cables can carry data securely over long distances, but they are relatively expensive; lower grade cables, which provide less data security over shorter distances, are relatively inexpensive.

Table. 15 Summary of cable Characteristics

Characteristics	**Thinnet coaxial (10Base2) Cable**	**Thicknet coaxial (10Base5) Cable**	**Twisted-pair (10BaseT) Cable1**	**Fiber-optic Cable**
Cable cost	More than UTP	More than thinnet	▪ UTP: Least expensive ▪ STP: More than thinnet	▪ More than thinnet, but less than thicknet
Usable cable Length	185 meters (about 607 feet)	500 meters (about 1640 feet)	UTP and STP: ▪ 100 meters (about 328 feet)	2 kilometers (6562 feet)
Transmission Rates	4-100 Mbps	4-100 Mbps	▪ UTP: 4-100 Mbps ▪ STP: 16-500 Mbps	100 Mbps or more (> 1Gbps)
Flexibility	Fairly flexible	Less flexible than Thinnet	▪ UTP: Most flexible ▪ STP: Less flexible than UTP	Less flexible than thicknet
Ease of Installation	Easy to install	Moderately easy to Install	▪ UTP: Very easy; often preinstalled ▪ STP: Moderately easy	Difficult to install
Susceptibility to interference	Good resistance to Interference	Good resistance to Interference	▪ UTP: Very susceptible ▪ STP: Good resistance	Not susceptible to Interference

Special features	Electronic support components are less expensive than twisted-pair cable	Electronic support components are less expensive than twisted-pair cable	▪ UTP: Same as telephone wire; often preinstalled in buildings ▪ STP: Supports higher transmission rates than UTP	Supports voice, data, and video
Preferred uses	Medium to large sites with high security needs	Linking thinnet Networks	▪ UTP: smaller sites on budget. ▪ STP: Token Ring in any size	Any size installation requiring speed and high data security and integrity

Unguided (wireless transmission) media

Wireless LANs use the following techniques for transmitting data:

1. Infrared transmission
2. Laser transmission

Infrared Transmission All infrared wireless networks operate by using an infrared light beam to carry the data between devices. These systems need to generate very strong signals because weak transmission signals are susceptible to interference from light sources such as windows. Many of the high-end printers sold today are preconfigured to accept infrared signals. This method can transmit signals at high rates because of infrared light's high bandwidth. An infrared network can normally broadcast at 10 Mbps. Infrared transmission mostly used to remote control system.

In infrared transmission the communicating bodies should be

- In direct line of sight
- If there is any body in between the communicating bodies will be unable to communicate
- Can not be used outdoors

Terrestrial Microwave

- Typically used where laying a cable is not practical
- Parabolic dish shaped antenna for directional and bar-like antenna for omni directional transmission
- transmits/receives electromagnetic waves in the 2-40 GHz range
- Travels in a straight line (line-of-sight propagation)
- High data rates: 100's Mbps
- Repeaters spaced 10 - 100 km apart
- Applications : telephone and data transmission- wireless LANs

Satellite Microwave

- Uses satellite in geostationary (geosynchronous) 36,000 km ~orbit
- Source transmits signal to satellite which amplifies or repeats it, and retransmits down to destinations
- Optimum transmission in 1 - 10 GHz range;
- Bandwidth of 100's MHz
- 270ms Significant propagation delay about
- VSAT (Very small Aperture Terminal) :- High speed data transmission using satellite

Characteristics and relative strengths and weakness of LAN Network

Characteristics of Local Area Network

- LANs are private owned-network, can be extended up to a few kilometers.
- LANs operate at relatively high speed as compared to the typical WAN
- It connects computers within a single office, building, block or campus, i.e. they work in a relatively small geographical area.

Advantages of LAN

1. **Resource Sharing:** LAN provides resource sharing such as computer resources like printers, scanners, modems, DVD-ROM drives, and hard disks can be shared within the connected devices. This reduces cost and hardware purchases.
2. **Software Applications Sharing:** In a Local Area Network, it is easy to use the same software in a number of computers connected to a network instead of purchasing the separately licensed software for each client a network.
3. **Easy and Cheap Communication:** Data and messages can easily be shared with the other computer connected to the network.
4. **Centralized Data:** The data of all network users can be stored on a hard disk of the central/server computer. This help user to use any computer in a network to access the required data.
5. **Data Security:** Since data is stored on the server computer, it will be easy to manage data at only one place and the data will be more secure too.
6. **Internet Sharing:** Local Area Network provides the facility to share a single internet connection among all the LAN users. In school labs and internet Cafes, single internet connection is used to provide internet to all connected computers.
7. Data is easy to backup as all the data is stored on the file server.

Disadvantages of LAN

1. **High Setup Cost:** The initial setup costs of installing Local Area Networks is high because there is special software required to make a server. Also, communication devices like an Ethernet cable, switches, hubs, routers, cables are costly.
2. **Privacy Violations:** The LAN administrator can see and check personal data files of each and every LAN user. Moreover, he can view the computer and internet history of the LAN user.
3. **Data Security Threat:** Unauthorized users can access important data of an office or campus if a server hard disk is not properly secured by the LAN administrator.
4. **LAN Maintenance Job:** ***Local Area Network requires a LAN Administrator*** because there are problems such as software installations, program faults or hardware failures or cable disturbances in Local Area Network. A LAN Administrator is required to maintain these issues.

5. **Covers Limited Area:** LANs are restricted in size they cover a small area like a single office, single building or a group of nearby buildings.
6. Managing a large network is complicated, requires training and a network manager usually needs to be employed.
7. Viruses can spread to other computers throughout a computer network.
8. There is a danger of hacking, particularly with wide area networks. Security procedures are needed to prevent such abuse, eg a firewall.

Hacker: A computer hacker is a person who finds out weaknesses in the computer and exploits it. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge

Workstation: PC connected to a network

Network Transmission media

Transmission Medium is the physical path between transmitter and receiver in a data communication system. The characteristics and quality of data transmission are determined both by the characteristics of the medium and characteristics of the signal.

Media of data transmission:

1. Guided Transmission media- Data transmission is through solid medium (wired system).
2. Unguided Transmission media– Data transmission through air /space (i.e. wireless system)

Guided transmission media (Cable)

Transmission capacity of guided media is described with respect to:

- Data rate or bandwidth
- Distance the media can run

Commonly Types of Cables

- Twisted pair
- Coaxial cable
- Optical fiber

Coaxial Cable

In its simplest form, coaxial cable consists of a core of copper wire surrounded by insulation, a braided metal shielding, and an outer cover. The term *shielding* refers to the woven or stranded metal mesh (or other material) that surrounds some types of cabling. Shielding protects transmitted data by absorbing stray electronic signals, called *noise*, so that they do not get onto the cable and distort the data.

The core of a coaxial cable carries the electronic signals that make up the data. This wire core can be either solid or stranded. If the core is solid, it is usually copper.

Surrounding the core is a dielectric insulating layer that separates it from the wire mesh. The braided wire mesh acts as a ground and protects the core from electrical noise and crosstalk.

A no conducting outer shield—usually made of rubber, Teflon, or plastic—surrounds the entire cable.

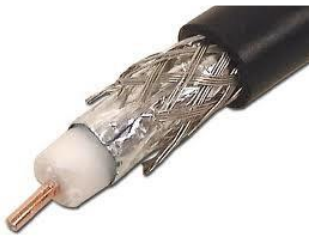


Figure 17. Image of coaxial cable

Coaxial cable is more resistant to interference and attenuation than twisted-pair cabling

Types of Coaxial Cable

There are two types of coaxial cable:

- Thin (thinnet) cable
- Thick (thicknet) cable

Which type of coaxial cable you select depends on the needs of your particular network.

Thinnet Cable

- *Thinnet* cable is a flexible coaxial cable about 0.64 centimeters (0.25 inches) thick. Because this type of coaxial cable is flexible and easy to work with, it can be used in almost any type of network installation.
- Thinnet coaxial cable can carry a signal for a distance of up to approximately **185** meters (about 607 feet) before the signal starts to suffer from attenuation

Thicknet Cable

- *Thicknet* cable is a relatively rigid coaxial cable about 1.27 centimeters (0.5 inches) in diameter.

- Thicknet cable is sometimes referred to as Standard Ethernet because it was the first type of cable used with the popular network architecture Ethernet.
- Thicknet cable's copper core is thicker than a thinnet cable core. The thicker the copper core, the farther the cable can carry signals. This means that thicknet can carry signals farther than thinnet cable.
- Thicknet cable can carry a signal for 500 meters (about 1640 feet). Therefore, because of thicknet's ability to support data transfer over longer distances, it is sometimes used as a backbone to connect several smaller thinnet-based networks.

Coaxial-Cable Connection Hardware

Both thinnet and thicknet cable use a connection component, known as a *BNC connector*, to make the connections between the cable and the computers

Figure 18. Twisted-Pair Cable

In its simplest form, *twisted-pair cable* consists of two insulated strands of copper wire twisted around each other

A number of twisted-pair wires are often grouped together and enclosed in a protective sheath to form a cable. The total number of pairs in a cable varies. The twisting cancels out electrical noise from adjacent pairs and from other sources such as motors, relays, and transformers.

Two types of twisted pair cable

- Unshielded twisted pair cable(UTP)
- Shielded twisted pair cable (STP)

Unshielded Twisted-Pair (UTP) Cable

UTP, using the 10BaseT specification, is the most popular type of twisted-pair cable and is fast becoming the most popular LAN cabling. The maximum cable length segment is 100 meters, about 328 feet

There are five categories of UTP

- **Category 1** This refers to traditional UTP telephone cable that can carry voice but not data transmissions. Most telephone cable prior to 1983 was Category 1 cable.
- **Category 2** This category certifies UTP cable for data transmissions up to 4 megabits per second (Mbps). It consists of four twisted pairs of copper wire.
- **Category 3** This category certifies UTP cable for data transmissions up to 16 Mbps. It consists of four twisted pairs of copper wire with three twists per foot.
- **Category 4** This category certifies UTP cable for data transmissions up to 20 Mbps. It consists of four twisted pairs of copper wire.
- **Category 5** This category certifies UTP cable for data transmissions up to 100 Mbps. It consists of four twisted pairs of copper wire.

Shielded Twisted-Pair (STP) Cable

STP cable uses a woven copper-braid jacket that is more protective and of a higher quality than the jacket used by UTP. STP also uses a foil wrap around each of the wire pairs. This gives STP excellent shielding to protect the transmitted data from outside interference, which in turn allows it to support higher transmission rates over longer distances than UTP.

Figure 19. STP cable

Connection hardware Twisted-pair cabling uses RJ-45 telephone connectors to connect to a computer.

These are similar to RJ-11 telephone connectors. Although RJ-11 and RJ-45 connectors look alike at first glance, there are crucial differences between them.

The RJ-45 connector is slightly larger and will not fit into the RJ-11 telephone jack. The RJ-45 connector houses eight cable connections, while the RJ-11 houses only four.

Figure 20. RJ-45 connector

Fiber-Optic Cable

In *fiber-optic cable*, optical fibers carry digital data signals in the form of modulated pulses of light. This is a relatively safe way to send data because, unlike copper-based cables that carry data in the form of electronic signals, no electrical impulses are carried over the fiber-optic cable. This means that fiberoptic cable cannot be tapped, and its data cannot be stolen.

Fiber-optic cable is good for very high-speed, high-capacity data transmission because of the purity of the signal and lack of signal attenuation.

Fiber-optic cable transmissions are not subject to electrical interference and are extremely fast, currently transmitting about 100 Mbps with demonstrated rates of up to 1 gigabit per second (Gbps). They can carry a signal—the light pulse—for many miles.

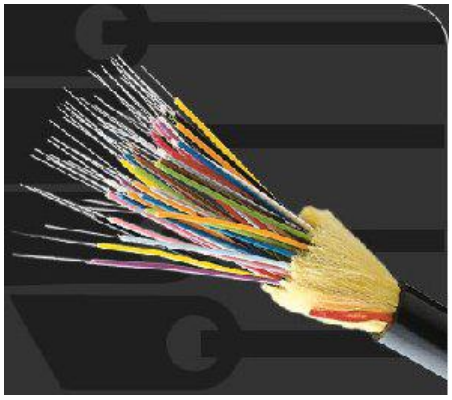


Figure 21. Fiber-Optic Cabling Considerations

Use fiber-optic cable if you:

- Need to transmit data at very high speeds over long distances in very secure media.

Do not use fiber-optic cable if you:

- Are under a tight budget.
- Do not have the expertise available to properly install it and connect devices to it.

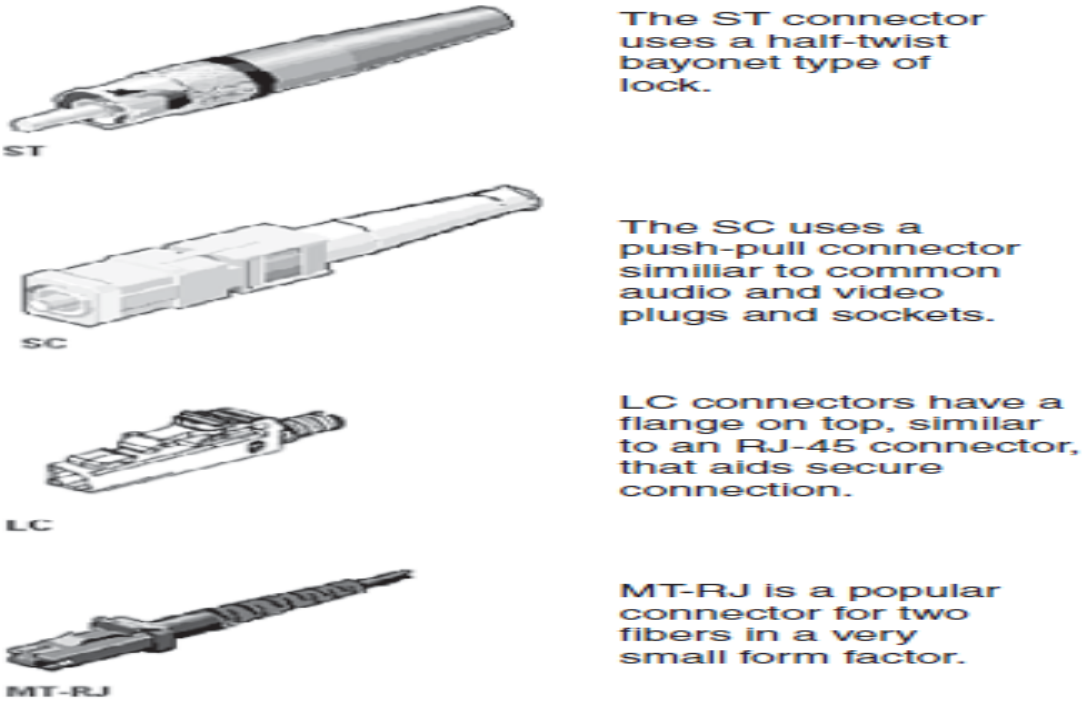


Figure 22. Fiber connectors.

Table 16. Cable characteristics summary

Media	Resistance to Attenuation	Resistance to EMI/Cross Talk	Cost of Implementation	Difficulty of Implementation
UTP	Low	Low	Low	Low
STP	Moderate	Moderate	Moderate	Low
Thin coax	Moderate	Moderate	Low	Low
Fiber-optic	Very high	Perfect	Very high	Moderate

IEEE 1394 (FireWire)

The IEEE 1394 interface, also known as FireWire, is more commonly associated with the attachment of peripheral devices such as digital cameras or printers than network connections. However, it is possible to create small networks with IEEE 1394 cables.

The IEEE 1394 interface comes in a 4- or 6-pin version, both of which are shown in the following Figure

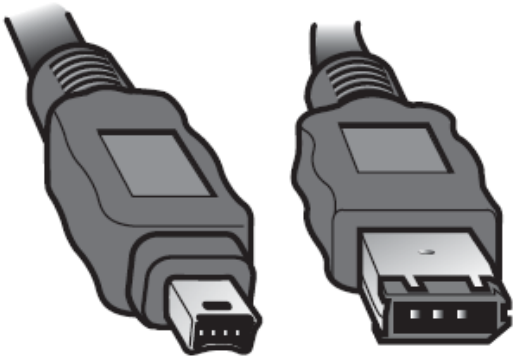


Figure 23. 4-pin (left) and 6-pin (right) IEEE 1394 (FireWire) connectors.

Universal Serial Bus Connectors (USB)

Universal Serial Bus (USB) ports are now a common sight on both desktop and laptop computer systems. Like IEEE 1394, USB is associated more with connecting consumer peripherals such as MP3 players and digital cameras than with networking. However, many manufacturers now make wireless network cards that plug directly into a USB port.

Most desktop and laptop computers have between two and four USB ports, but USB hubs are available that provide additional ports if required.

A number of connectors are associated with USB ports, but the two most popular are Type A and Type B. Type A connectors are the more common of the two and are the type used on PCs. Although many peripheral devices also use a Type A connector, an increasing number now use a Type B. Figure 1.25 shows a Type A connector and a Type B connector.

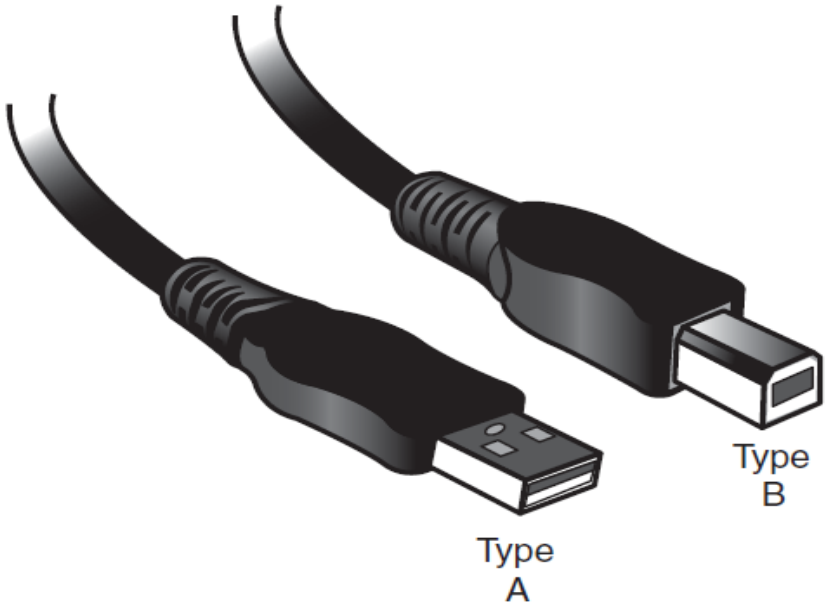


Figure 24. Type A and Type B USB connectors.

Mode of transmission

The term transmission mode defines the direction of data flow between two linked devices. The manner or way in which data is transmitted from one place to another is called Data Transmission Mode. There are three ways for transmitting data from one location to another. These are:

- Simplex mode
- Half-Duplex mode
- Full-Duplex mode

1. Simplex Mode

The most basic form of data or information transmission is called *simplex*. This means that data is sent in one direction only, from sender to receiver.

Examples of simplex transmission are radio and television. With simplex transmission, problems encountered during the transmission are not detected and corrected. Senders

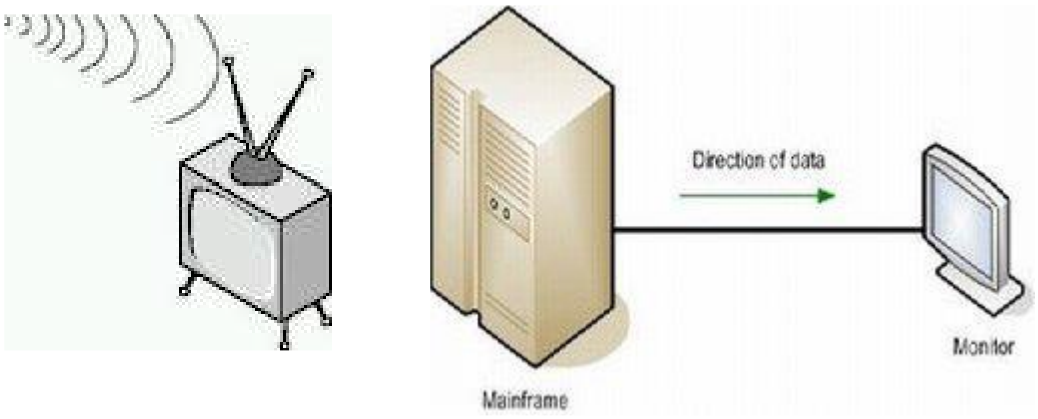


Figure 25. Simplex mode

2. Half duplex mode

In Half-duplex mode, the communication can take place in both directions, but only in one direction at a time. In this mode, data is sent and received alternatively. It is like a one-lane bridge where two-way traffic must give way in order to cross the other. In half-duplex mode, at a time only one end transmits data while other end receives. In addition, it is possible to perform error detection and request the sender to re-transmit information. The Internet browsing is an example of half duplex. When we issue a request to download a web document, then that document is downloaded and displayed before we issue another request.

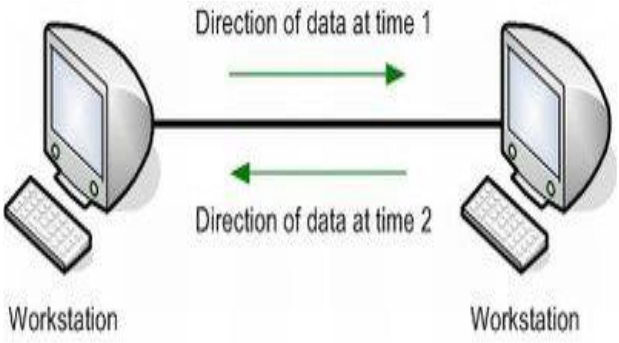


Figure 26. Half-duplex mode

Full duplex mode

In Full-duplex mode, the communication can take place in both directions simultaneously, i.e. at the same time on the same channel. It is the fastest directional mode of communication. Example of this mode is conversation of the persons through telephone. This type of communication is similar to automobile traffic on a two-lane road. The telephone communication system is an example of full duplex communication mode.

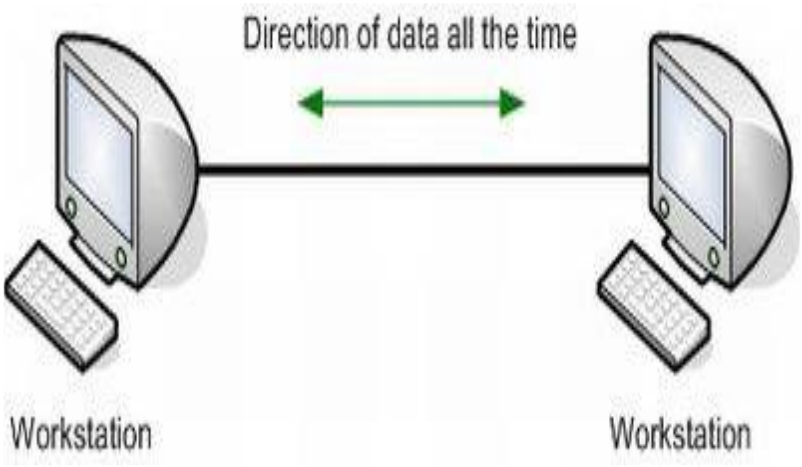


Figure 27. Full-duplex mode

Parallel vs. serial transmission

There are two types of data transmission modes. These are:

1. Parallel Transmission
2. Serial Transmission

1. Parallel Transmission

In parallel transmission, bits of data flow concurrently through separate communication lines. The automobile traffic on a multi-lane highway is an example of parallel transmission. Inside the computer binary data flows from one unit to another using parallel mode. If the computer uses 32-bits internal structure, all the 32-bits of data are transferred simultaneously on 32-lane connections. Similarly, parallel transmission is commonly used to transfer data from computer to printer. The printer is connected to the parallel port of computer and parallel cable that has many wires is used to connect the printer to computer. It is very fast data transmission mode.

2. Serial Transmission

In serial data transmission, bits of data flow in sequential order through single communication line. The flow of traffic on one-lane residential street is an example of serial data transmission mode. Serial transmission is typically slower than parallel transmission, because data is sent sequentially in a bit-by-bit fashion. Serial mouse uses serial transmission mode in computer.

Synchronous & Asynchronous Transmissions

1. Synchronous Transmission

In synchronous transmission, large volumes of information can be transmitted at a time. In this type of transmission, data is transmitted block-by-block or word-byword simultaneously. Each block may contain several bytes of data. In synchronous transmission, a special communication device known as synchronized clock' is required to schedule the transmission of information. This special communication device or equipment is expensive.

2. Asynchronous Transmission

In asynchronous transmission, data is transmitted one byte at a 'time'. This type of transmission is most commonly used by microcomputers. The data is transmitted character-by-character as the user types it on a keyboard. An asynchronous line that is idle (not being used) is identified with a value 1, also known as 'Mark' state.

This value is used by the communication devices to find whether the line is idle or disconnected. When a character (or byte) 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 character is coming.

Data transfer methods

In a complex system where a number of senders, receivers and many ways to move the data between two communicating parties where the transmission system is made of a number of nodes interconnected with a transmission medium, two typical methods are employed to ensure data transfer. These are:

1. **Circuit switching**
2. **Packet switching**

Circuit Switching

Circuit switching was designed in 1878 in order to send telephone calls down a dedicated channel. This channel remained open and in use throughout the whole call and could not be used by any other data or phone calls.

- There are three phases in circuit switching:
  - ✓ Establish
  - ✓ Transfer
  - ✓ Disconnect
- The telephone message is sent in one go, it is not broken up. The message arrives in the same order that it was originally sent.
- In modern circuit-switched networks, electronic signals pass through several switches before a connection is established.
- During a call, no other network traffic can use those switches.
- The resources remain dedicated to the circuit during the entire data transfer and the entire message follows the same path.
- Circuit switching can be analogue or digital
- With the expanded use of the Internet for voice and video, analysts predict a gradual shift away from circuit-switched networks.
- A circuit-switched network is excellent for data that needs a constant link from end-to-end. For example real-time video.

Advantages

- Circuit is dedicated to the call – no interference, no sharing
- Guaranteed the full bandwidth for the duration of the call
- Guaranteed Quality of Service

Disadvantages

- Inefficient – the equipment may be unused for a lot of the call, if no data is being sent, the dedicated line still remains open
- Takes a relatively long time to set up the circuit
- During a crisis or disaster, the network may become unstable or unavailable.

It was primarily developed for voice traffic rather than data traffic

Packet switching

- In packet-based networks, the message gets broken into small data packets. These packets are sent out from the computer and they travel around the network seeking out the most efficient route to travel as circuits become available. This does not necessarily mean that they seek out the shortest route.
- Each packet may go a different route from the others.
- Each packet is sent with a 'header address'. This tells it where its final destination is, so it knows where to go.
- The header address also describes the sequence for reassembly at the destination computer so that the packets are put back into the correct order.
- One packet also contains details of how many packets should be arriving so that the recipient computer knows if one packet has failed to turn up.

If a packet fails to arrive, the recipient computer sends a message back to the computer which originally sent the data, asking for the missing packet to be resent

Advantages of packet switching

- Security
- Bandwidth used to full potential
- Devices of different speeds can communicate
- Not affected by line failure (rediverts signal)
- Availability – do not have to wait for a direct connection to become available
- During a crisis or disaster, when the public telephone network might stop working, emails and texts can still be sent via packet switching

Disadvantages

- Under heavy use there can be a delay
- Data packets can get lost or become corrupted
- Protocols are needed for a reliable transfer
- Not so good for some types data streams e.g real-time video streams can lose frames due to the way packets arrive out of sequence.

Self-Check 4	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives. (1 point each)

1. Which of the following is not a criteria in selecting and documenting an appropriate network topology?
   A. Cost B. Shielding C. Transmission rate D. Crosstalk E. None of the above
2. Which one of the following is odd among the given one?
   A. ST B. LC C. MT-RJ D.RJ-45 E. SC
3. The maximum length of UTP cable is _____Meter.
   A. 100 B.25 C. 75 D. 175

Part II: Fill in the blank spaces

3. The three phases of circuit switching's: (3%)

   _____
   _____
   _____
   _____

2. The three types of mode of data transmissions are: (3%)
   a. _____
   b. _____
   c. _____

3. What are the two most popular USB connectors? (2%)

   _____
   _____
   _____

4. List the common types of Guided Medias. (3%)

_____
_____
_____
_____

5. _____is a person who finds out weaknesses in the computer and exploits it. (1%)

Note: **Satisfactory rating 100%**
You can ask you teacher for the copy of the correct answers.

Score = _____

References

Best fit topology

- Child, J. (1972). *Organizational structure, environment and performance: The role of strategic choice*. sociology, 6(1), 1-22.

- James D.Mcabe Network Analysis, Architecture, and Design 3rd Edition
- Priscilla Oppenheimer Top Down Approach 3rd Edition,
- www.syngrress.com

Answer Key Module Title: Best fit topology

LO #1- Identify key information sources	
Self-Check 1	**Written Test**

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives. (Each 2 point)

1. D. Wisdom
2. B. Repository
3. A. Tertiary

Part II: Fill the blank spaces

1. When information is entered and stored in a computer, it is generally referred to as **Data.**
2. List sources of information.
   - Primary sources
   - Secondary sources
   - Tertiary sources
3. Write down at least 4 examples of primary sources of information.
   - Original written works
   - Poems
   - Diaries
   - Court records

Self-Check 2	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives. (1 point each).

1. All are correct
2. All of the above.

Part II: fill in the blank spaces.

1. The four kinds of documentation are:-

   _____

   - ❖ learning-oriented tutorials
   - ❖ goal-oriented how-to guides
   - ❖ understanding-oriented discussions
   - ❖ information-oriented reference material

2. What is documentation?

   Answer: Documentation is any communicable material that is used to describe, explain or instruct regarding some attributes of an object, system or procedure, such as its parts, assembly, installation, maintenance and use.

Self-Check 3	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives. (1 point each).

1. B. Open-ended
2. A. Close-ended

Part II: Fill in the blank spaces

1. Write down at least 3 examples of closed ended questions.
   - ❖ How old are you?
   - ❖ Are you a student?
   - ❖ What is your name?

2. Write down at least 3 examples of open-ended questions.
   - ❖ What is the use of computer?
   - ❖ What is information?
   - ❖ What is your hobby?

Self-Check 4	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives. (1 point each).

1. A. True
2. C. All of the above
3. E. None of the above
4. D. None of the above

Part II: fill in the blank spaces

1. _____is a technique that enables the analyst to view how processes and activities are being done in the context of the business.
   Answer: Observation
2. An_____ is a planned meeting during which you obtain information from another person.
   Answer: Interview
3. The most common steps that take place during the interviewing process are:
   a. Determining the people to interview
   b. Establishing objectives of the interview
   c. Developing the interview questions
   d. Preparing for the interview
   e. Conducting the interview
   f. Documenting the interview
   g. Evaluating the interview

LO #2- Determine User needs	
Self-Check 1	**Written Test**

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives. (1 points each).

1. **A**. MAN
2. D. sharing of power
3. D. All of the above
4. A. Media
5. B. Virtual Private network

Part II: Fill the blank spaces

1. What is the main difference between LAN, MAN and WAN?
   - **LAN:** Is a local area network that covers a small geographical coverage such as in a single building or groups of buildings.
   - **MAN:** A large network that usually spans several buildings in the same city or town.
   - **WAN:** a network that covers all over the country or the world.

     Example: Network among news agency offices in different regions of Ethiopia.
2. Write down the advantages of server based network.

- Centralized resources
  - Easier to backup files
  - Easier to find files
- Efficient
- Security
  - One machine can secure entire network
  - One central login
- Scalability

Self-Check 2	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives. (1 points each).

1. E. All of the above
2. E. All of the above

Part II: fill in the blank spaces.

1. A _____is a combination of hardware and software.
   Answer: Network analyzer
2. _____ is the term that is used to describe the random variation of signal timing (e.g., electromagnetic interference and crosstalk with other signals).
   Answer: Jitter
3. _____is a command-line network sniffer that is included with the Sun Solaris OS. **Answer:** Snoop
4. _____involves splitting the larger network into smaller network segments can be accomplished through firewalls, virtual local area networks, and other separation techniques.
   Answer: Network segmentation

Self-Check 3	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Fill in the blank spaces.

1. _____refers to the amount of data moving across a network at a given point of time.

   Answer: Network traffic or data traffic

2. _____is used to measure the efficiency of a communications network.

   Answer: Network traffic simulation

3. _____is the main component for network traffic measurement, network traffic control and simulation.

   Answer: Network traffic

LO #3- Develop best topology	
Self-Check 1	**Written Test**

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer (Each 1 point)

1. C. Ring
2. D. 87
3. A. Bus

Part II: fill in the blank spaces.

1. _____refers to the arrangement or physical layout of computers, cables, and other components on the network.

Answer: Network topology

2. Write down the advantages of Bus topology.

- Use of cable is economical.
- Media is inexpensive and easy to work with.
- System is simple and reliable.
- Bus is easy to extend.

3. Write down the disadvantages of Ring topology. (3%).

- Failure of one computer can impact the rest of the network.
- Problems are hard to isolate.
- Network reconfiguration disrupts operation.

Self-Check 2	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives. (1 point each)

1. D**.** Transport layer
2. D. Application layer
3. A. application layer
4. B. Physical layer
5. C. protocol
6. C. SMTP
7. A.TCP

Part II: Fill in the blank spaces

1. Data link layer has two distinct sub layers called:

Answer:

- LLC (Logical Link Control) and
- MAC(Media Access Control)

2. The _____layer is the top most layer of the OSI reference model.

Answer: Application layer

Self-Check 3	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Fill in the blank spaces

1. **What is Cost benefit analysis in computer networking?**

   Answer: It can be explained as a procedure for estimating all **costs** involved and possible profits to be derived from a business opportunity or proposal. Most economists also account for opportunity **costs** of the investment in the project to get the **costs** involved.

2. **What are the major steps in a cost-benefit analysis?**

Answer:

- Step 1: Specify the set of options. ...
- Step 2: Decide whose costs and benefits count. ...
- Step 3: Identify the impacts and select measurement indicators. ...
- Step 4: Predict the impacts over the life of the proposed regulation. ...
- Step 5: Monetize (place dollar values on) impacts.

Self-Check 4	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Choose the best answer from the given alternatives. (1 point each)

1. E. None f the above
2. D. RJ-45
3. A. 100

Part II: Fill in the blank spaces

1. The three phases of circuit switching's are :
   - Establish
   - Transfer
   - Disconnect
2. The three types of mode of data transmissions are:
   - Simplex mode
   - Half-Duplex mode
   - Full-Duplex mode
3. What are the two most popular USB connectors?
   - Type A and
   - Type B
4. List the common types of Guided Medias.
   - Twisted pair
   - Coaxial and
   - Fiber optic
4. _____is a person who finds out weaknesses in the computer and exploits it.

   Answer: Hacker

AKNOWLEDGEMENT

We wish to extend thanks and appreciation to the many representatives of TVET instructors who donated their time and expertise to the development of this TTLM.

We would like also to express our appreciation to Federal Technical and Vocational Education and Training Agency (FTVET), Oromia TVET Bureau, TVET College/ Institutes, who made the development of this TTLM with required standards and quality possible.

This TTLM is developed on December 2020 at Bishoftu Bin International hotel.

he trainers who developed the TTLM

No	Name of Trainer	College Name	Edu. Background	Address	
				Mob.	Email
1	Abebe Mintefa	Ambo TVET College	MSc.	0929352458	tolabula@gmail.com
2	Frew Atkilt	Bishoftu Polytechnic College	MSc.	0911787374	frew.frikii@gmail.com
3	Tewodiros Girma	Sheno TVET College	MSc.	0912068479	tedimutd@gmail.com
4	Tsedale Mengiste	Dukem TVET College	MSc.	0912076643	tmmeng2005@gmail.com
5	Zerihun Abate	Sebeta Polytechnic College	MSc.	0911858358	zedoabata2017@gmail.com