KASNEB

CICT

PART 2

SECTION 4

Data Communication and Computer Networks

Practical

Contents

TOPIC 1

DATA COMMUNICATION CONCEPTS

Introduction

When we communicate, we are sharing information. This sharing can be local or remote. between individuals, local communication usually occurs face to face, while remote communication takes place over distance.

The term **Telecommunication**, which includes Telephony, Telegraphy, and television, means communication at a distance.
The data refers to facts, concepts and instruction presented in whatever form is agreed upon by the parties creating and using the data. In the context of computer information system, data represented by binary information units produced and consumed in the form of 0s and 1s.

Data Communications is the transfer of data or information between a source and a receiver. The source transmits the data and the receiver receives it. The actual generation of the information is

not part of Data Communications nor is the resulting action of the information at the receiver. Data Communication is interested in the transfer of data, the method of transfer and the preservation of the data during the transfer process.

The purpose of Data Communications is to provide the rules and regulations that allow computers with different disk operating systems, languages, cabling and locations to share resources. The rules and regulations are called protocols and standards in Data Communications.

For data communication to occur, the communicating devices must be part of a communication system made up of a combination of hardware and software. The effectiveness of a data communication system depends on the three fundamental characteristics:
1. Delivery: The System must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user
2. Accuracy: The system must deliver data accurately. Data that have been altered in transmission and left uncorrected are rustles
3. Timeliness: The system must deliver data in a timely manner. Data delivered late are useless. In the case of video, audio, and voice data, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. this kind of delivery id called real-time transmission.

Data Communication Terminologies

Here you will learn about some common data communication terminologies such as:

Data Channel - A channel is basically a medium that is used to carry information or data from one point to another.

Baud - Baud is basically the unit of measurement for the information carrying capacity of communication channel.

The baud is synonymous with bps (stands for bits per second), which is another unit of measuring data transfer rates.

TOPIC 3

DATA SIGNAL ANALYSIS

Introduction

Signal - In electronics, a signal is an electric current or electromagnetic field used to convey data from one place to another. The simplest form of signal is a direct current (DC) that is switched on and off; this is the principle by which the early telegraph worked. More complex signals consist of an alternating-current (AC) or electromagnetic carrier that contains one or more data streams.

What are Analog and Digital Signals?

Signals - In electrical engineering, the fundamental quantity of representing some information is called a signal. It does not matter what the information is i-e: Analog or digital information. In mathematics, a signal is a function that conveys some information. In fact any quantity measurable through time over space or any higher dimension can be taken as a signal. A signal could be of any dimension and could be of any form.

Analog signals

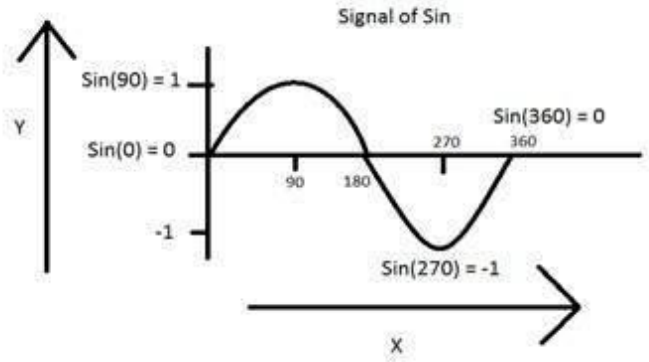
A signal could be an analog quantity that means it is defined with respect to the time. It is a continuous signal. These signals are defined over continuous independent variables. They are difficult to analyze, as they carry a huge number of values. They are very much accurate due to a large sample of values. In order to store these signals , you require an infinite memory because it can achieve infinite values on a real line. Analog signals are denoted by sin waves.

For example:

Human voice is an example of analog signals. When you speak, the voice that is produced travel through air in the form of pressure waves and thus belongs to a mathematical function, having independent variables of space and time and a value corresponding to air pressure.

Another example is of sin wave which is shown in the figure below.

Y = sin(x) where x is independent



Digital signals

As compared to analog signals, digital signals are very easy to analyze. They are discontinuous signals. They are the appropriation of analog signals.

The word digital stands for discrete values and hence it means that they use specific values to represent any information. In digital signal, only two values are used to represent something i-e: 1 and 0 (binary values). Digital signals are less accurate then analog signals because they are the discrete samples of an analog signal taken over some period of time. However digital signals are not subject to noise. So they last long and are easy to interpret. Digital signals are denoted by square waves.

For example:

Computer keyboard: Whenever a key is pressed from the keyboard, the appropriate electrical signal is sent to keyboard controller containing the ASCII value that particular key. For example the electrical signal that is generated when keyboard key a is pressed, carry information of digit 97 in the form of 0 and 1, which is the ASCII value of character a.

Difference between analog and digital signals

Comparison element	Analog signal	Digital signal
Analysis	Difficult	Possible to analyze
Representation	Continuous	Discontinuous
Accuracy	More accurate	Less accurate
Storage	Infinite memory	Easily stored
Subject to Noise	Yes	No
Recording Technique	Original signal is preserved	Samples of the signal are taken and preserved
Examples	Human voice, Thermometer, Analog phones e.t.c	Computers, Digital Phones, Digital pens, e.t.c

Systems

A system is a defined by the type of input and output it deals with. Since we are dealing with signals, so in our case, our system would be a mathematical model, a piece of code/software, or a physical device, or a black box whose input is a signal and it performs some processing on that signal, and the output is a signal. The input is known as excitation and the output is known as response.

In the above figure a system has been shown whose input and output both are signals but the input is an analog signal. And the output is an digital signal. It means our system is actually a conversion system that converts analog signals to digital signals.

Conversion of analog to digital signals

Since there are lot of concepts related to this analog to digital conversion and vice-versa. We will only discuss those which are related to digital image processing.There are two main concepts that are involved in the coversion.

- Sampling
- Quantization

Sampling

Sampling as its name suggests can be defined as take samples. Take samples of a digital signal over x axis. Sampling is done on an independent variable. In case of this mathematical equation:

Sampling is done on the x variable. We can also say that the conversion of x axis (infinite values) to digital is done under sampling.

Sampling is further divide into up sampling and down sampling. If the range of values on x-axis are less then we will increase the sample of values. This is known as up sampling and its vice versa is known as down sampling.

Quantization

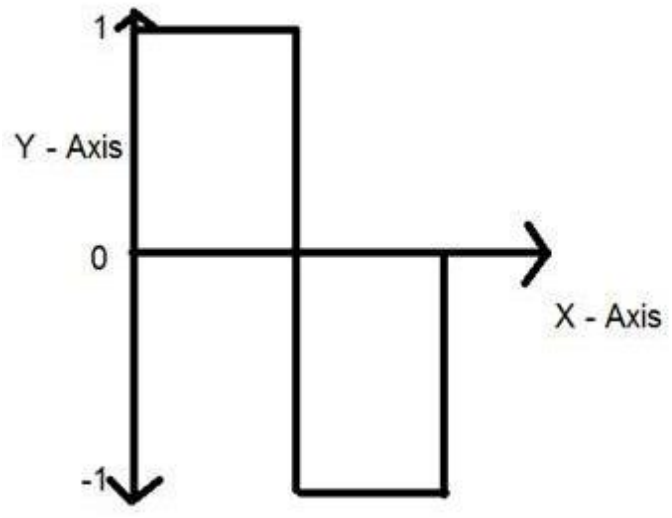
Quantization as its name suggest can be defined as dividing into quanta (partitions). Quantization is done on dependent variable. It is opposite to sampling.

In case of this mathematical equation y = sin(x)

Quantization is done on the Y variable. It is done on the y axis. The conversion of y axis infinite values to 1, 0, -1 (or any other level) is known as Quantization.

These are the two basics steps that are involved while converting an analog signal to a digital signal.

The quantization of a signal has been shown in the figure below.



Why do we need to convert an analog signal to digital signal.

The first and obvious reason is that digital image processing deals with digital images, that are digital signals. So when ever the image is captured, it is converted into digital format and then it is processed.

The second and important reason is, that in order to perform operations on an analog signal with a digital computer, you have to store that analog signal in the computer. And in order to store an analog signal, infinite memory is required to store it. And since thats not possible, so thats why we convert that signal into digital format and then store it in digital computer and then performs operations on it.

Continuous systems vs discrete systems

Continuous systems The type of systems whose input and output both are continuous signals or analog signals are called continuous systems.

Discrete systems The type of systems whose input and output both are discrete signals or digital signals are called digital systems.

Modulation And Demodulation

TOPIC 5

ADMINSTERING USER ACCOUNTS

User accounts are one of the basic tools for managing a Windows server. As a network administrator, you'll spend a large percentage of your time dealing with user accounts — creating new ones, deleting expired ones, resetting passwords for forgetful users, granting new access rights, and so on. Before getting into the specific procedures of creating and managing user accounts, this section presents an overview of user accounts and how they work.

Local accounts versus domain accounts

A *local account* is a user account that's stored on a particular computer and applies only to that computer. Typically, each computer on your network will have a local account for each person who uses that computer.

In contrast, a *domain account* is a user account that's stored by Active Directory and can be accessed from any computer that's a part of the domain. Domain accounts are centrally managed. This chapter deals primarily with setting up and maintaining domain accounts.

User account properties

Every user account has a number of important *account properties* that specify the characteristics of the account. The three most important account properties are

- **Username:** A unique name that identifies the account. The user must enter the username when logging on to the network. The username is public information. In other words, other network users can (and often should) find out your username.
- **Password:** A secret word that must be entered in order to gain access to the account. You can set up Windows so that it enforces password policies, such as the minimum length of the password, whether the password must contain a mixture of letters and numerals, and how long the password remains current before the user must change it.
- **Group membership:** The group or groups to which the user account belongs. Group memberships are the key to granting access rights to users so that they can access various network resources, such as file shares or printers or to perform certain network tasks, such as creating new user accounts or backing up the server.

Many other account properties record information about the user, such as the user's contact information, whether the user is allowed to access the system only at certain times or from certain computers, and so on..

Printer setup

A **network printer** is one attached to a **server** (possibly internal, possibly a windows server) which handles job queuing and caching, security, etc. for multiple users. The server makes the printer available on the network as a network printer (more than just a shared printer) and a client PC connects to the server to use the network printer.

A network-connected **local printer** is a printer that simply connects to a PC through the network, instead of USB or parallel interfaces. The protocol allows many PCs to be connected to this printer as their local printer, each with the same setup with a tcp/ip port created for the printer. It's not necessary for any PC to share such a printer out because each PC can be configured to talk directly to it.

Think of local in this instance as meaning a printer that is locally (i.e. on this PC) configured and controlled, rather than handing that off to a server and printing to that server.

The **existing ports** are other local interfaces such as serial, parallel, and possibly others. You need to create a new local tcp/ip port for a local network-connected printer because the PC has no idea what IP address and other settings the printer might need, wheras it knows how to talk to a printer on a parallel port, for example. USB printers never need any of this because it's all done automatically.

How to Configure a Printer in Windows

In most cases, setting up and configuring a printer in Windows 7 or Vista is straightforward. Follow the instructions that came with your printer's software on an installation CD, or download that information from the printer manufacturer's Website. If you can't find the information there, follow this guide to set up a printer manually on your PC. We show the steps to add a local and network printer in Windows 7. The process is very similar in Windows Vista.

Step by Step: Configuring a Printer in Windows 7

Step 1 Click *Start, Devices and Printers*.

Step 2 In the window that pops up, click the *Add a Printer* button on the toolbar near the top.

TOPIC 9

MONITORING NETWORK RESOURSE

Network monitoring is the information collection function of network management.

Network monitoring is the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, SMS or other alarms) in case of outages or other trouble. Network monitoring is part of network management.

Details

While an intrusion detection system monitors a network for threats from the outside, a network monitoring system monitors the network for problems caused by overloaded or crashed servers, network connections or other devices.

For example, to determine the status of a web server, monitoring software may periodically send an HTTP request to fetch a page. For email servers, a test message might be sent through SMTP and retrieved by IMAP or POP3.

Commonly measured metrics are response time, availability and uptime, although both consistency and reliability metrics are starting to gain popularity. The widespread addition of WAN optimization devices is having an adverse effect on most network monitoring tools, especially when it comes to measuring accurate end-to-end response time because they limit round trip visibility.

Status request failures, such as when a connection cannot be established, it times-out, or the document or message cannot be retrieved, usually produce an action from the monitoring system. These actions vary; An alarm may be sent (via SMS, email, etc.) to the resident sysadmin, automatic failover systems may be activated to remove the troubled server from duty until it can be repaired, etc.

Monitoring the performance of a network uplink is also known as network traffic measurement.

Network tomography is an important area of network measurement, which deals with monitoring the health of various links in a network using end-to-end probes sent by agents located at vantage points in the network/Internet.

Route analytics is another important area of network measurement. It includes the methods, systems, algorithms and tools to monitor the routing posture of networks. Incorrect routing or routing issues cause undesirable performance degradation or downtime.

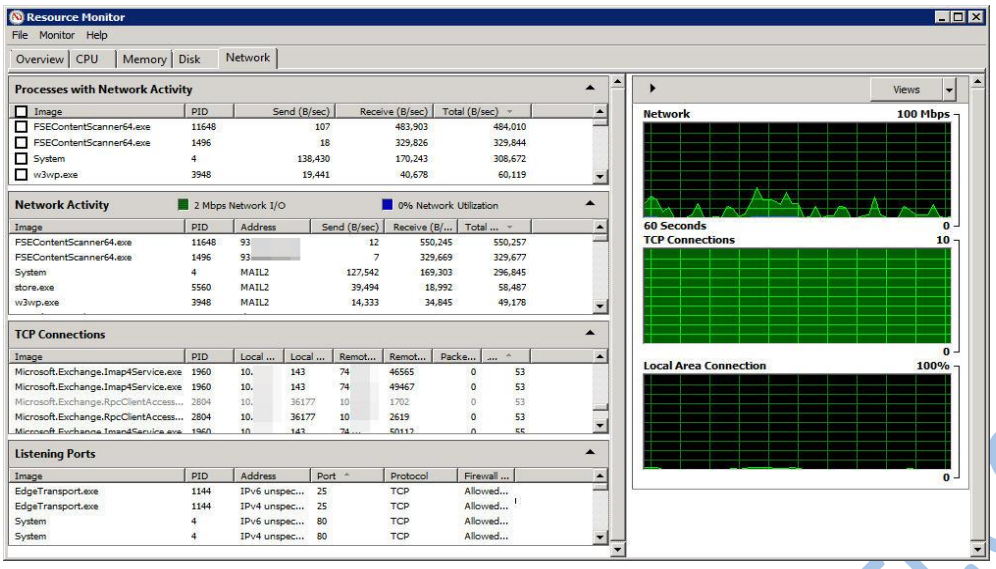
Various types of protocols

Website monitoring service can check HTTP pages, HTTPS, SNMP, FTP, SMTP, POP3, IMAP, DNS, SSH, TELNET, SSL, TCP, ICMP, SIP, UDP, Media Streaming and a range of other ports with a variety of check intervals ranging from every four hours to every one minute. Typically, most network monitoring services test your server anywhere between once-per-hour to once-per-minute.

Use Resource Monitor to monitor network performance

By use of Microsoft's Resource Monitor tool, There are ways by which you can receive real-time performance metrics related to storage performance and CPU utilization. In this installment of my four-part series, I'll discuss the various network-related metrics that you can view with Resource Monitor, explain the graphs you see in the tool, and provide some context around each metric.

For the purposes of this post, we'll use the screenshot in **Figure A**. This figure shows a Resource Monitor view from a production server running Windows Server 2008 R2 and Exchange Server 2010 with all Exchange roles installed. As such, this server has significant need for network resources that operate within acceptable boundaries. (**Note:** Like all of our other servers, this server is running as a virtual machine under VMware vSphere 4.1.) **Figure A**



A look at Resource Monitor in Windows Server 2008 R2 (Click the image to enlarge.)

Let's start with an overall look at the console. Occupying most of the window is the statistics area, which I'll be explaining in depth. At the right side of the window are a number of graphs, each depicting a key network-based performance metric.

In the sections below, I provide details for each metric. I don't repeat metrics; if one type of metric appears in multiple areas, I only list it once.

Processes with Network Activity

This section of the Resource Monitor window shows a list of all of the running processes that are using disk resources. You see the name of the executable and a number of performance statistics.

- **Image.** Process executable file name. This is the name of the process that is actively using the disk.
- **PID.** The ID number associated with the process. This is useful if you want to use other utilities to manage processes, or you want to easily match up processes with Task Manager.
- **Send (B/sec).** Average number of bytes per second that the process has sent over the network in the past minute.
- **Receive (B/sec).** Average number of bytes per second that the process has received from the network in the past minute.
- **Total (B/sec).** Average total network activity (in bytes) that the process has generated in the past minute.

The information in this section isn't particularly useful for troubleshooting except to show you which processes are consuming the most network resources. In Figure A, you can see that the processes named FSEContentScanner64.exe are receiving quite a bit of information from the network.

Network Activity

This section of the Resource Monitor window provides more useful troubleshooting information. In particular, the two boxes next to the heading offer the most impactful, immediately useful metrics.

- **Network I/O.** This box shows the current total network utilization in Mbps (megabits per second). This is a useful data point, but the metric next to it is the one that provides you with really good information.
- **Network Utilization.** This metric wraps up all total utilization into a single, easily accessible metric that can help you determine exactly how loaded your network really is. If this number is approaching 100% and stays there on a regular basis, you likely have network congestion issues and should add more network capacity.

Below this header information, you will find the following new metric:

- **Address.** This is the name or IP address with which the process is communicating.

The remaining metrics in this section repeat the information from the previous section.

TCP Connections

- **Local Address.** Many servers have multiple network adapters, and each network adapter can have multiple IP addresses assigned to it. In order to better determine which network adapter and IP address may have congestion issues, this sections adds more granular IP address information to the list of metrics.
- **Local Port.** Likewise, you may have services that run services using a multitude of TCP ports. If you'd like to determine on which ports communication is happening, you can see that here.
- **Remote Address.** Every local connection requires some kind of communication with a remote system. In this column, you will see the remote address that makes up the other half of the communication stream.
- **Remote Port.** Here you will find the remote port that makes up the other end of the communication.

TOPIC 11

INTERNET OF THINGS (IOT)

The **Internet of things** (**IoT**) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data

Elements: Below are elements compositions of the Internet of Things:

- **Internet of Things:** A network of internet-connected objects able to collect and exchange data using embedded sensors.
- **Internet of Things device:** Any stand-alone internet-connected device that can be monitored and/or controlled from a remote location.
- **Internet of Things ecosystem:** All the components that enable businesses, governments, and consumers to connect to their IoT devices, including remotes, dashboards, networks, gateways, analytics, data storage, and security.
- **Entity:** Includes businesses, governments, and consumers.
- **Physical layer:** The hardware that makes an IoT device, including sensors and networking gear.
- **Network layer:** Responsible for transmitting the data collected by the physical layer to different devices.
- **Application layer:** This includes the protocols and interfaces that devices use to identify and communicate with each other.
- **Remotes:** Enable entities that utilize IoT devices to connect with and control them using a dashboard, such as a mobile application. They include smartphones, tablets, PCs, smartwatches, connected TVs, and nontraditional remotes.
- **Dashboard:** Displays information about the IoT ecosystem to users and enables them to control their IoT ecosystem. It is generally housed on a remote.
- **Analytics:** Software systems that analyze the data generated by IoT devices. The analysis can be used for a variety of scenarios, such as predictive maintenance.
- **Data storage:** Where data from IoT devices is stored.
- **Networks:** The internet communication layer that enables the entity to communicate with their device, and sometimes enables devices to communicate with each other.
- **Localization**: Location awareness, providing ability to identify the location of sensor, machine, vehicle, and wearable device,

- **Radio-Frequency Identification (RFID)** is a communication method used for tracking and identifying objects wirelessly.

Note

Tags: The tags are the end points in an RFID system. They store identity information along with other information as required by the purpose of the tag. There are two types of tags:

- **Active Tags:** These tags have an on-board power source of some sort, usually a battery, which means they can transmit stronger signals and therefore have more range. This type of tag can periodically transmit a signal irrespective of a reader.
- **Passive Tags:** These tags do not have any internal power source and get activated in the vicinity of a reader. Your metro or bus pass is generally a passive tag, which gets activated when you touch it to the reader. These tags harvest the radio energy transmitted by the reader.

Readers: Readers have a similar construction to an RFID tag. They have an antenna to receive and transmit signals to/from the tags. They might be either battery powered or plugged in to a wall outlet, as a reader requires strong RF signals to activate the tag (for passive) when it comes in the vicinity of the reader. The reader is connected to a reader controller, which manages the information read by the reader. The reader may also write or update a tag depending on the application. For example, the reader in subway stations is at the entry point. When the rider places a card (tag) on the reader, it reads the available money in the card and grants the user entry. At the passenger's exit, it calculates the fare and updates the amount on the card.

RFID tags can have three main components:

- An Integrated Circuit (IC) for storing identity information, processing it and modulating/demodulating the RF signals
- An antenna to receive and send the radio signals
- A power source (battery) if an active tag

Applications of the Internet of Things

1. **Smart Home:** The smart home is likely the most popular IoT application at the moment because it is the one that is most affordable and readily available to consumers. From the Amazon Echo to the Nest Thermostat, there are hundreds of products on the market that users can control with their voices to make their lives more connected than ever.
2. **Wearables:** Watches are no longer just for telling time. The Apple Watch and other smart-watches on the market have turned our wrists into smartphone holsters by enabling text messaging, phone calls, and more. And devices such as Fitbit and Jawbone have helped revolutionize the fitness world by giving people more data about their workouts.
3. **Smart Cities:** The IoT has the potential to transform entire cities by solving real problems citizens face each day. With the proper connections and data, the Internet of Things can solve traffic congestion issues and reduce noise, crime, and pollution.

4. **Connected Car:** These vehicles are equipped with Internet access and can share that access with others, just like connecting to a wireless network in a home or office. More vehicles are starting to come equipped with this functionality, so prepare to see more apps included in future cars.

Internet of Things Devices & Examples

1. **Amazon Echo - Smart Home:** The Amazon Echo works through its voice assistant, Alexa, which users can talk to in order to perform a variety of functions. Users can tell Alexa to play music, provide a weather report, get sports scores, order an Uber, and more.
2. **Fitbit One - Wearables:** The Fitbit One tracks your steps, floors climbed, calories burned, and sleep quality. The device also wirelessly syncs with computers and smartphones in order to transmit your fitness data in understandable charts to monitor your progress.
3. **Barcelona - Smart Cities:** The Spanish city is one of the foremost smart cities in the world after it implemented several IoT initiatives that have helped enhance smart parking and the environment.
4. **AT&T - Connected Car:** AT&T added 1.3 million cars to its network in the second quarter of 2016, bringing the total number of cars it connects to 9.5 million. Drivers don't have to subscribe or pay a monthly fee for data in order for AT&T to count them as subscribers.

If you're interested in learning more about the Internet of Things, then check out the in-depth report from **BI Intelligence**, Business Insider's premium research service. To get your copy of this invaluable guide to the IoT universe, choose one of these options:

1. Subscribe to an ALL-ACCESS Membership with BI Intelligence and gain immediate access to this report AND over 100 other expertly researched deep-dive reports, subscriptions to all of our daily newsletters, and much more.
2. Purchase the report and download it immediately from our research store.