Chapter 1

INTRODUCTION

Here are some ideas of projects in the Networking area. Some of these are new, and some are ideas that have run before but could be run again. Note that, unlike the normal project ideas, these ideas do not have a contact listed against them. They are there to give you ideas of the sort of things that could be done. If a project idea seems interesting, and you would like to pursue it further, then you should discuss it with one of the lecturers who are experienced in the Networking area: Bill Buchanan, Gordon Russell, Ahmed Al-Dubai, Imed Romdhani, Jim Jackson, Robert Ludwiniak or Neil Urquhart. They may not be able to help you directly, but will at least be able to point you to somebody better placed, perhaps because their specialist knowledge is in the area of the project.

This introduces the underlying concepts behind networking using the Internet and its protocols as examples. There are two goals:
(1) to give you an understanding of how networks, especially the Internet, work,
(2) to teach you network programming.
We will cover the first five chapters of Kurose in detail, working our way down the network stack from the application layer to the data-link layer. Concurrent with the lectures, you (in groups of two) will be building a functional TCP/IP stack and a small web server that will run on it. What you build will be "real" – your code will interoperate with other TCP/IP stacks and you'll be able to talk to your web server using any browser on any TCP/IP stack.
This is a learn-by-doing kind of class. You will get your hands dirty by examining parts of our Internet infrastructure and building other parts. It will be a lot of work, but it will also be a lot of fun, provided you enjoy this sort of thing. We will assume that you do and that you will make a good faith effort. We don't want to have to spend too much time measuring your performance. If you care about what we're teaching, you'll do a better job of that yourself, and if you don't care, then you should take some course that you do care about.

The goal of the networking project is to enable you to do the following:

- Build implementations of the Internet protocols
- Generalize this knowledge to other networking protocols.
- Be a competent network and systems programmer.
- Think like a networking practitioner
- Read and judge articles on networking in trade magazines
- Begin to read and judge research and technical articles on networking

? Create simplicity and reliability out of complexity and unreliability
? Structure and design software systems to achieve that simplicity and Reliability

Chapter 2
Project Specification

2.1 Hardware Specification

CPU Speed :2GHz recommended or higher
Processor :Pentium Processor or above
Memory/RAM: 1GB minimum,2GB recommended or higher
Display Properties: Greater than 256 color depth
Size of Hard Disk:60GBminimum
NIC Card

2.2 Software Specification

Software Used: Packet Tracer 5.3.2
Operating System: Microsoft Windows XP,Vista,7

2.2.1Packet Tracer

Packet Tracer is a Cisco router simulator that can be utilized in training and education, but also in research for simple computer network simulations. The tool is created by Cisco Systems and provided for free distribution to faculty, students, and alumni who are or have participated in the Cisco Networking Academy. The purpose of Packet Tracer is to offer students and teachers a tool to learn the principles of networking as well as develop Cisco technology specific skills.

Features

The current version of Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP,OSPF, and EIGRP, to the extent required by the current CCNA curriculum. While Packet Tracer aims to provide a realistic simulation of functional networks, the application itself utilizes only a small number of features found within the actual hardware running a current CiscoIOS version. Thus, Packet Tracer is unsuitable for modeling production networks. With the introduction of version 5.3, several new features were

added, including BGP. BGP is not part of the CCNA curriculum, but part of the CCNP curriculum.

2.3PROJECT DETAIL

2.3.1Description:

Here we have 8 branches of a company in a Campus Network design, they are accessing internet through ISP.

2.3.2DEVICES USED

- 8 SERIAL CABLES
- 28 COPPER CROSS OVER
- 8 COPPER STRAIGHT THROUGH
- 8 ROUTERS
- 16 SWITCHES(LAYER 2)
- 1 MULTY LAYER SWITCH
- 28 PCs
- 16 CONSOLE CABLES

2.3.3 PROTOCOLS USED

- EIGRP 100
- VTP(VLAN TRUNKING PROTOCOL) at all SWITCHES
- INTER VLAN SWITCHING

- DHCP on MULTI-LAYER SWITCH
- SUBNET MASKING
- WILD CARD MASKING
- STP(SPANNING TREE PROTOCOL)
- NAT(NETWORK ADDRESS TRANSLATION)

Chapter 3

SYSTEM DESIGN

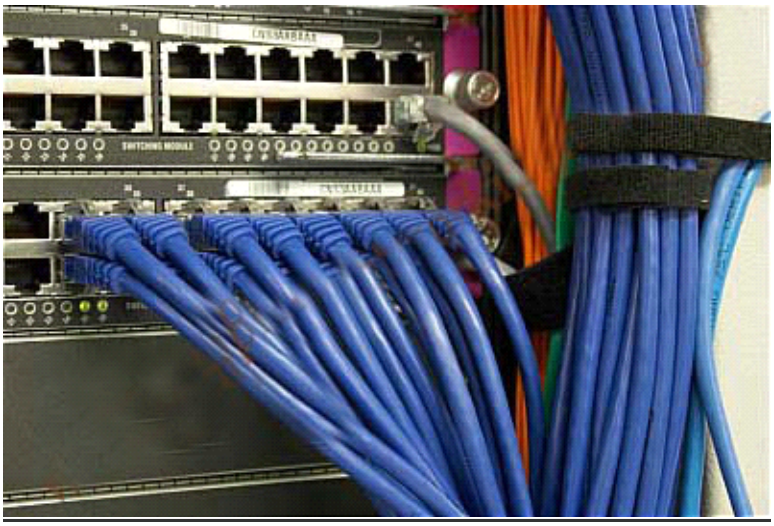
(TECHNOLOGY AND TOOLS USED)

3.1Networking Technologies

Networks using a Star topology require a central point for the devices to connect. Originally this device was called a concentrator since it consolidated the cable runs from all network devices. The basic form of concentrator is the hub.

As shown in Figure; the hub is a hardware device that contains multiple, independent ports that match the cable type of the network. Most common hubs interconnect Category 3 or 5 twisted-pair cable with RJ-45 ends, although Coax BNC and Fiber Optic BNC hubs also exist. The hub is considered the least common denominator in device concentrators. Hubs offer an inexpensive option for transporting data between devices, but hubs don't offer any form of intelligence. Hubs can be active or passive.

3.2SWITCHES



Switches are a special type of hub that offers an additional layer of intelligence to basic, physical-layer repeater hubs. A switch must be able to read the MAC address of each frame it receives. This information allows switches to repeat incoming data frames only to the computer or computers to which a frame is addressed. This speeds up the network and reduces congestion.

Switches operate at both the physical layer and the data link layer of the OSI Model.

3.3BRIDGES

A **bridge** is used to join two network segments together, it allows computers on either segment to access resources on the other. They can also be used to divide large networks into smaller segments. Bridges have all the features of repeaters, but can have more nodes, and since the network is divided, there is fewer computers competing for resources on each segment thus improving network performance.

3.4ROUTERS

Routers Are networking devices used to extend or segment networks by forwarding packets from one logical network to another. Routers are most often used in large internetworks that use the TCP/IP protocol suite and for connecting TCP/IP hosts and local area networks (LANs) to the Internet using dedicated leased lines.

Routers work at the network layer (layer 3) of the Open Systems Interconnection (OSI) reference model for networking to move packets between networks using their logical addresses (which, in the case of TCP/IP, are the IP addresses of destination hosts on the network). Because routers operate at a higher OSI level than bridges do, they have better packet-routing and filtering capabilities and greater processing power, which results in routers costing more than bridges.

3.4.1Routing tables

Routers contain internal tables of information called routing tables that keep track of all known network addresses and possible paths throughout the internetwork, along with cost of reaching

each network. Routers route packets based on the available paths and their costs, thus taking advantage of redundant paths that can exist in a mesh topology network.

Because routers use destination network addresses of packets, they work only if the configured network protocol is a routable protocol such as TCP/IP or IPX/SPX. This is different from bridges, which are protocol independent. The routing tables are the heart of a router; without them, there's no way for the router to know where to send the packets it receives.

Unlike bridges and switches, routers cannot compile routing tables from the information in the data packets they process. This is because the routing table contains more detailed information than is found in a data packet, and also because the router needs the information in the table to process the first packets it receives after being activated. A router can't forward a packet to all possible destinations in the way that a bridge can.

Static routers: These must have their routing tables configured manually with all network addresses and paths in the internetwork.

Dynamic routers: These automatically create their routing tables by listening to network traffic.

Routing tables are the means by which a router selects the fastest or nearest path to the next "hop" on the way to a data packet's final destination. This process is done through the use of routing metrics.

Routing metrics which are the means of determining how much distance or time a packet will require to reach the final destination. Routing metrics are provided in different forms.

hop is simply a router that the packet must travel through.

Ticks measure the time it takes to traverse a link. Each tick is 1/18 of a second. When the router selects a route based on tick and hop metrics, it chooses the one with the lowest number of ticks first.

You can use routers, to segment a large network, and to connect local area segments to a single network backbone that uses a different physical layer and data link layer standard. They can also be used to connect LAN's to a WAN's.

3.5GATEWAYS

A gateway is a device used to connect networks using different protocols. Gateways operate at the network layer of the OSI model. In order to communicate with a host on another network, an IP host must be configured with a route to the destination network. If a configuration route is not found, the host uses the gateway (default IP router) to transmit the traffic to the destination host. The default t gateway is where the IP sends packets that are destined for remote networks. If no default gateway is specified, communication is limited to the local network. Gateways receive data from a network using one type of protocol stack, removes that protocol stack and repackages it with the protocol stack that the other network can use.

Examples

- E-mail gateways-for example, a gateway that receives Simple Mail Transfer Protocol (SMTP) e-mail, translates it into a standard X.400 format, and forwards it to its destination
- Gateway Service for NetWare (GSNW), which enables a machine running Microsoft Windows NT Server or Windows Server to be a gateway for Windows clients so that they can access file and print resources on a NetWare server
- Gateways between a Systems Network Architecture (SNA) host and computers on a TCP/IP network, such as the one provided by Microsoft SNA Server

- A packet assembler/disassembler (PAD) that provides connectivity between a local area network (LAN) and an X.25 packet-switching network

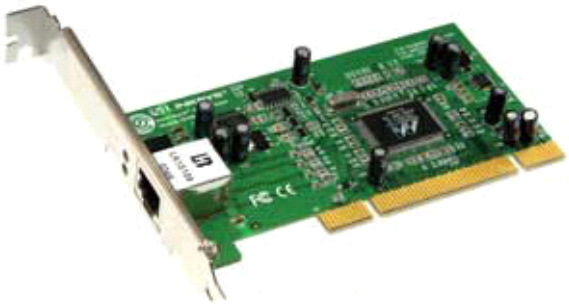
3.6NICs (Network Interface Card)

Network Interface Card, or NIC is a hardware card installed in a computer so it can communicate on a network. The network adapter provides one or more ports for the network cable to connect to, and it transmits and receives data onto the network cable.

Wireless Lan card

Every networked computer must also have a network adapter driver, which controls the network adapter. Each network adapter driver is configured to run with a certain type of network adapter.

3.6.1Network card



3.6.2Adapter Functions Network Interface

Network interface adapters perform a variety of functions that are crucial to getting data to and from the computer over the network.

These functions are as follows:

3.6.2.1Data encapsulation

The network interface adapter and its driver are responsible for building the frame around the data generated by the network layer protocol, in preparation for transmission. The network interface adapter also reads the contents of incoming frames and passes the data to the appropriate network layer protocol.

3.6.2.2Signal encoding and decoding

The network interface adapter implements the physical layer encoding scheme that converts the binary data generated by the network layer-now encapsulated in the frame-into electrical voltages, light pulses, or whatever other signal type the network medium uses, and converts received signals to binary data for use by the network layer.

3.6.2.3Transmission and reception

The primary function of the network interface adapter is to generate and transmit signals of the appropriate type over the network and to receive incoming signals. The nature of the signals depends on the network medium and the data-link layer protocol. On a typical LAN, every computer receives all of the packets transmitted over the network, and the network interface adapter examines the destination address in each packet, to see if it is intended for that computer.

3.6.2.4Data buffering

Network interface adapters transmit and receive data one frame at a time, so they have built-in buffers that enable them to store data arriving either from the computer or from the network until a frame is complete and ready for processing.

3.6.2.5Serial/parallel conversion

The communication between the computer and the network interface adapter runs in parallel, that is, either 16 or 32 bits at a time, depending on the bus the adapter uses. Network communications, however, are serial (running one bit at a time), so the network interface adapter is responsible for performing the conversion between the two types of transmissions.

3.6.2.6Media access control

The network interface adapter also implements the MAC mechanism that the data-link layer protocol uses to regulate access to the network medium. The nature of the MAC mechanism depends on the protocol used.

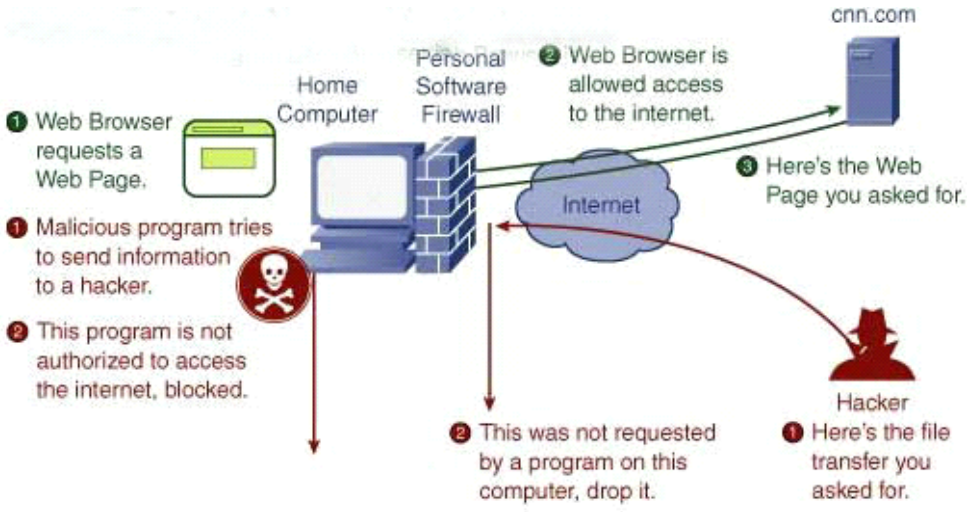
3.7MODEMS

A modem is a device that makes it possible for computers to communicate over telephone lines. The word modem comes from Modulate and Demodulate. Because standard telephone lines use analog signals, and computers digital signals, a sending modem must modulate its digital signals into analog signals. The computers modem on the receiving end must then demodulate the analog signals into digital signals.

Modems can be external, connected to the computers serial port by an RS-232 cable or internal in one of the computers expansion slots. Modems connect to the phone line using standard telephone RJ-11 connectors.

3.8FIREWALLS

In computing, a firewall is a piece of hardware and/or software which functions in a networked environment to prevent some communications forbidden by the security policy, analogous to the function of firewalls in building construction.



A firewall has the basic task of controlling traffic between different zones of trust. Typical zones of trust include the Internet (a zone with no trust) and an internal network (a zone with high trust). The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.

There are three basic types of firewalls depending on:

- whether the communication is being done between a single node and the network, or between two or more networks
- whether the communication is intercepted at the network layer, or at the application layer
- whether the communication state is being tracked at the firewall or not

3.9Network protocols

A networked computer must also have one or more protocol drivers (sometimes called a transport protocol or just a protocol). The protocol driver works between the upper-level network software and the network adapter to package data to be sent on the network.

In most cases, for two computers to communicate on a network, they must use identical protocols. Sometimes, a computer is configured to use multiple protocols. In this case, two computers need only one protocol in common to communicate. For example, a computer running File and Printer Sharing for Microsoft Networks that uses both NetBEUI and TCP/IP can communicate with computers using only NetBEUI or TCP/IP.

In this project we are using three protocols:-

- RIPV2
- OSPF
- EIGRP

3.9.1 RIPV2

The **Routing Information Protocol** (**RIP**) is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and used to deprecate inaccessible, inoperable, or otherwise undesirable routes in the selection process.
RIP version 2 (RIPv2) was developed in 1993 and last standardized in 1998. It included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remained. RIPv2 has facilities to fully interoperate with the earlier specification if all Must Be Zero protocol fields in the RIPv1 messages are properly specified. In addition, a compatibility switch feature allows fine-grained interoperability adjustments.
In an effort to avoid unnecessary load on hosts that do not participate in routing, RIPv2 multicasts the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast. Unicast addressing is still allowed for special applications.

3.9.2 OSPF

Open Shortest Path First (**OSPF**) is a link-state routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). It is defined as OSPF Version 2 in (1998) for IPv4 The updates for IPv6 are specified as OSPF Version 3

OSPF is perhaps the most0 widely used interior gateway protocol (IGP) in large enterprise networks. IS-IS, another link-state dynamic routing protocol, is more common in large service provider networks. The most widely used exterior gateway protocol is the Border Gateway Protocol (BGP), the principal routing protocol between autonomous systems on the Internet

.OSPF is an interior gateway protocol that routes Internet Protocol (IP) packets solely within a single routing domain (autonomous system). It gathers link state information from available routers and constructs a topology map of the network. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets. OSPF was designed to support variable-length subnet masking (VLSM) or Classless Inter-Domain Routing (CIDR) addressing models.

OSPF detects changes in the topology, such as link failures, and converges on a new loop-free routing structure within seconds. It computes the shortest path tree for each route using a method based on Dijkstra's algorithm, a shortest path first algorithm.

The OSPF routing policies to construct a route table are governed by link cost factors (external metrics) associated with each routing interface. Cost factors may be the distance of a router (round-trip time), network throughput of a link, or link availability and reliability, expressed as simple unitless numbers. This provides a dynamic process of traffic load balancing between routes of equal cost.

An OSPF network may be structured, or subdivided, into routing areas to simplify administration and optimize traffic and resource utilization. Areas are identified by 32-bit numbers, expressed either simply in decimal, or often in octet-based dot-decimal notation, familiar from IPv4 address notation.

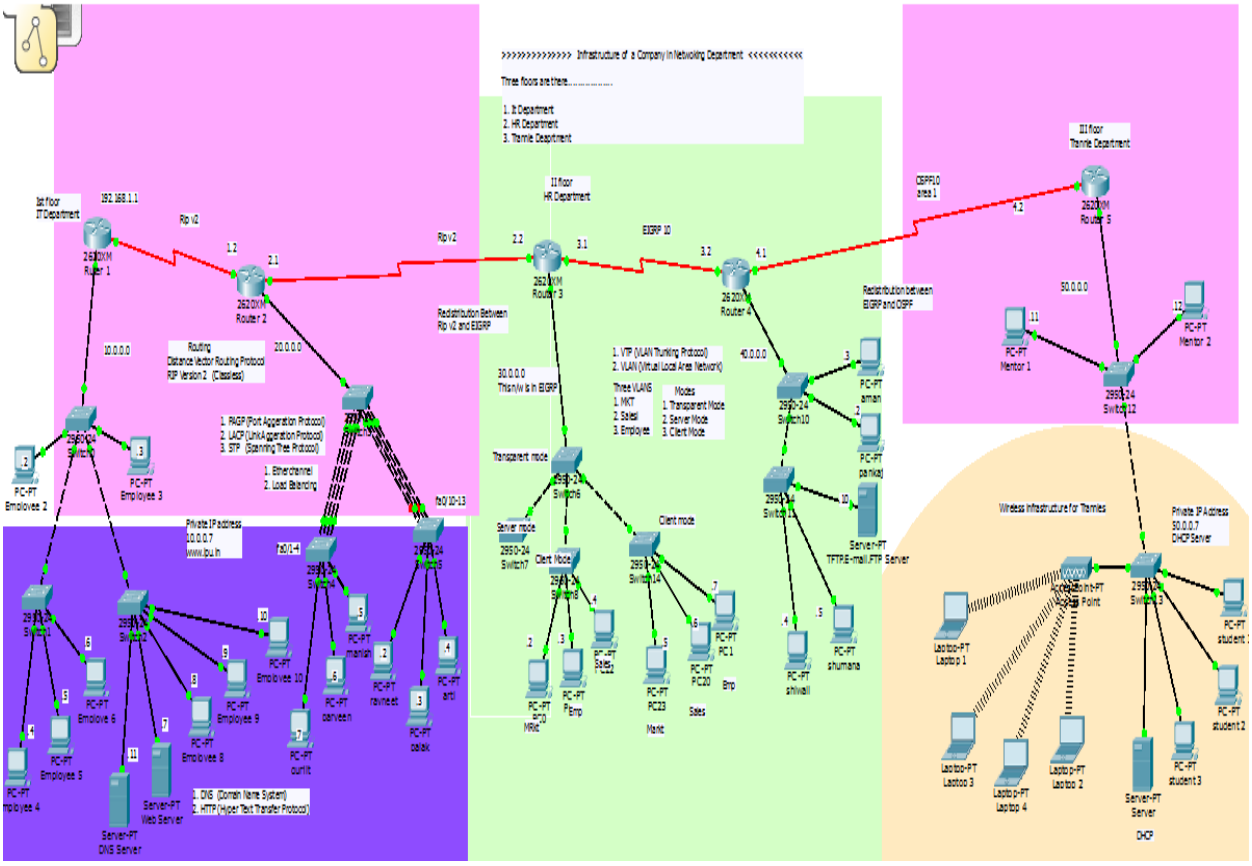
3.9.3 EIGRP

Enhanced Interior Gateway Routing Protocol - (**EIGRP**) is an open routing protocol loosely based on their original IGRP created by Cisco. EIGRP is an advanced distance-vector routing protocol, with optimizations to minimize both the routing instability incurred after topology changes, as well as the use of bandwidth and processing power in the router. Routers that support EIGRP will automatically redistribute route information to IGRP neighbors by converting the 32 bit EIGRP metric Update Algorithm (DUAL) work from SRI, which guarantees loop-free operation and provides a mechanism for fast convergence

CHAPTER 4

SNAPSHOTS

4.1PROJECT SCENARIO



REFERENCES

- www.google.com
- www.cbtnuggets.com